THĒMIS

Revista de Derecho

Derecho y Tecnología
1965 - 2021

THĒMIS
desde 1965

79

© Asociación Civil THĒMIS, 2021
Facultad de Derecho
Pontificia Universidad Católica del Perú
editor@themis.pe
themisconsejoeditorial@gmail.com
cceethemis@gmail.com
www.themis.pe
www.revistas.pucp.edu.pe/themis

Editor: Chiara Lucía Jacob Camaiora
Coordinadores: José Miguel Porto y Diego Fernández
Diseño y diagramación: Mario Popuche Llontop

El contenido de los artículos publicados en **THĒMIS-Revista de Derecho**, así como las opiniones y posturas vertidas en ellos, son de responsabilidad exclusiva de los autores.

THĒMIS autoriza la reproducción parcial o total del contenido de esta publicación, siempre que se cite la fuente y utilice para fines académicos.

Primera edición: Noviembre 2021
Hecho el Depósito Legal en la Biblioteca Nacional del Perú: 2000-0958
ISSN: 1810-9934 (Impreso)
ISSN: 2410-9592 (En línea)
Registro de Proyecto Editorial: 31501142100623
THĒMIS-Revista de Derecho 79. ISSN: 1810-9934 (Impreso)
Año LVII - Número 79

Editado por:
Asociación Civil THĒMIS, 2021
Av. Universitaria 1801, Lima 32, Perú
Domicilio legal: Calle Santa Honorata 384, Piso 3, Lima 01, Perú
Teléfono: 626-2000, anexo 5391

Impreso por:
Tarea Asociación Gráfica Educativa
Pasaje María Auxiliadora 156 Breña
tareagrafica@tareagrafica.com
Lima - Perú

PRESENTACIÓN

THĒMIS-Revista de Derecho tiene como misión la promoción y difusión de la cultura jurídica a nivel nacional e internacional. Para ello, las diversas generaciones del Consejo Ejecutivo, encargadas de la edición y producción de la revista, han logrado escoger temáticas que impulsen la investigación y el desarrollo de conocimiento jurídico. De este modo, con cada entrega de THĒMIS-Revista de Derecho se ha retado a diversos profesionales y estudiosos del medio a escribir sobre temas de vanguardia, de gran relevancia y trascendencia para nuestra disciplina. Ello, sumado al arduo esfuerzo y dedicación invertido por los estudiantes detrás de cada edición, ha consolidado nuestra publicación como un producto de excelente calidad académica.

En línea con esta tradición, nos complace entregar la edición 79 de THĒMIS-Revista de Derecho, dedicada a la compleja relación entre el Derecho y la Tecnología. En efecto, debido a los rápidos desarrollos tecnológicos de los últimos años, acelerados a causa de la pandemia del COVID-19, hoy vivimos inmersos en un mundo en constante renovación en el que el Derecho no siempre puede mantenerse al día. Por lo tanto, es importante que desde espacios académicos como el nuestro se impulsen la reflexión y el planteamiento de propuestas para la regulación y el uso adecuado de estas nuevas tecnologías.

La edición 79 logra esto y mucho más al abordar temas de gran vigencia desde un abanico de ángulos que proveen una variedad de reflexiones y propuestas. En las páginas siguientes, nuestros lectores encontrarán artículos que analizan temas que van desde los avances tecnológicos y los derechos fundamentales; pasando por el gobierno electrónico y las oportunidades de regulación; la modernización de la función jurisdiccional; la optimización digital y los desafíos para el derecho mercantil; hasta los retos del derecho laboral frente a las nuevas tecnologías. Verdaderamente, es una edición de corte innovador que empuja al Derecho a adaptarse, actualizarse y adelantarse a los desafíos de esta nueva era digital.

Estamos orgullosos de presentar un número que refleje la calidad y excelencia característica de nuestra revista y, así, reafirmar el compromiso de THĒMIS-Revista de Derecho con su objetivo original. Dicho logro no hubiera sido posible sin el esfuerzo constante de los miembros del Consejo Ejecutivo conformado por los estudiantes editores de la revista, así como de nuestros coordinadores, asesor temático, árbitros y autores quienes aportaron su tan apreciado trabajo, consejos y conocimientos.

Finalmente, manifestamos nuestro más sincero deseo de que las futuras generaciones encargadas de la elaboración de THĒMIS-Revista de Derecho continúen y mejoren nuestra labor, siempre siendo fieles al lema: **Innovar es nuestra tradición**.

Lima, noviembre de 2021

EL CONSEJO EJECUTIVO

Reseña sobre la Pintura

THĒMIS-Revista de Derecho tiene el agrado de presentar como portada de su edición 79 el óleo “El afilador de cuchillos”, c. 1912-1913, de Kazimir Malévich (1879-1935). Con gran influencia en los ismos que irrumpieron la escena artística tradicional a inicios del siglo XX en Rusia, el pintor se inmiscuyó en el frondoso camino de encontrar su estilo, partiendo desde la pintura impresionista hasta encontrar su esencia en el arte del futurismo y cubismo de la época. Realizado entre 1912 y 1913, este lienzo captura con objetividad la realidad en movimiento, la cual, a través de composiciones estáticas y sólidas, aspira construir una nueva visión del mundo y desvelar la sensibilidad humana en la vida cotidiana. Inmerso en figuras geométricas cuya abstracción y tonos lúgubres difuminan su silueta, el afilador de cuchillos dirige sus manos con vehemencia a la acción, flexionando su cuerpo con rigidez y enfocando la totalidad de su atención en el resultado. Aunque cuestionada por la crítica inicialmente, no es sino hasta tiempo después que se advierte la trascendencia que la obra alcanza en el tiempo y espacio, siendo considerada una de las pinturas más icónicas del cubo-futurismo ruso.

THĒMIS

Revista de Derecho

Publicación semestral editada por alumnos de la Facultad de Derecho de la Pontificia Universidad Católica del Perú

2020-2

CONSEJO DIRECTIVO

Cristina Gonzales Camarena (Actualidad Jurídica)
Luis Felipe Cornejo Arenas (Administración)
Luz Andrea Caycho Cáceres (Contenido)
Mariana Isabel Gálvez Zárate (Cursos & Capacitaciones)
Denisse Paucar Laurencio (Desarrollo Social)
Joyce Vivas Huaccho (Imagen Institucional)
Rodrigo Roman Olarte (Publicaciones)
Nicole Cristina Velazco Velazco (Recursos Humanos)
Alessandra Rocca Rodríguez (Seminarios)

MIEMBROS ACTIVOS

Actualidad Jurídica
Fanny Herrera Cevasco
Adriana Chávez Copa
Daniel Rodríguez Tamo
Kathia Martínez Tarazona
Valeria Aguado Arauco
Piero Vivar Pajuelo
César Eduardo Véliz Nuñez

Administración
Sebastián Morello Montes
Diana Salazar Pérez
Alexis Salinas Temoche
Rodrigo Falla Valdez

Contenido
Lucia Beatriz López Gallardo
Sol María Guevara Ratto
Santiago Garnica Franco
Lilian Raquel Cánepa Yufra
Joaquín Alejandro Mejía Cacho
Chiara Lucía Jacob Camaiora

Cursos & Capacitaciones
Miguel Rosas Ramírez
María José Erausquin Herrada
Alexia Gaitán Meléndez
Vivian Bustamante Yabar
Gonzalo Milton Noriega Chuquiray

Desarrollo Social
Aixa Cristoval Solorzano
Rubiela Gaspar Clavo
Sebastián Pepper Smith
Alessandra Jaramillo Rojas
Alvaro Peña Villanueva
Cristina Phicihua Aliaga

Financiamiento
Valeria Murrieta Noly
Steven Hu Huang

Imagen Institucional
Ariana Armacanqui Paredes
Romina Alarcón Bonilla
Gabriela Alexandra Herbozo Villayzán
María Fernanda Villanueva Ruete
Ángel Sebastián Bravo Morales
Angie Yman Palomino

Publicaciones
Johanna Mosqueira Gonzáles
Ariana Novoa Suarez
Karla Soria Valeriano
Rosa Sobrados Burgos

Recursos Humanos
Ana Calderón Torres
Katherine Lisseth Ortiz Cornejo
Hector Gianfranco Míñope Ferro
María José Escobar Castillo

Seminarios
Andreé Castro Arequipeño
Angela Romero Carranza
Alexandra Aguirre Sumarriva
Melady Chávez Macuado
Carlos Osorio Alza

CONSEJO CONSULTIVO

Alfredo Bullard González (PUCP)
Guido Calabresi (U. de Yale)
Robert D. Cooter (U. de California, Berkeley)
Javier de Belaúnde López de Romaña (PUCP)
Fernando de Trazegnies Granda (PUCP)
Carlos Fernández Sessarego † (UNMSM)
Baldo Kresalja Roselló (PUCP)
César Landa Arroyo (PUCP)
Javier Neves Mujica (PUCP) †
Javier Pazos Hayashida (PUCP)
Richard A. Posner (U. de Chicago)
George L. Priest (U. de Yale)
José Daniel Amado Vargas (PUCP)

Asociación Civil THĒMIS
Facultad de Derecho de la Pontificia Universidad Católica del Perú
Teléfono: 626-2000 anexo 5391
Correo electrónico: themisconsejoeditorial@gmail.com
www.themis.pe

THĒMIS - Revista de Derecho 79

Editor General
Chiara Lucía Jacob Camaiora, Pontificia Universidad Católica del Perú, Perú

Consejo Editorial de THĒMIS-Revista de Derecho
Elvira Méndez Chang, Pontificia Universidad Católica del Perú, Perú
Ana Teresa Revilla Vergara, Pontificia Universidad Católica del Perú, Perú
Fernando Cantuarias Salaverry, Universidad del Pacífico, Perú
Cecilia O'Neill de la Fuente, Universidad del Pacífico, Perú
Carlos Zelada Acuña, Universidad del Pacífico, Perú
José Manuel Álvarez Zárate, Universidad Externado de Colombia, Colombia
Rémy Cabrillac, Université de Montpellier, Francia
Michele Taruffo, Università degli Studi di Pavia, Italia
Carlos Moreiro González, Universidad Carlos III de Madrid, España
Daniel Francisco Mitidiero, Universidade Federal do Rio Grande do Sul, Brasil
Antonio Saccoccio, Università degli Studi di Brescia, Italia
René Provost, McGill University, Canadá
Manuel Atienza Rodríguez, Universidad de Alicante, España
Luiz Guilherme Marinoni, Universidade Federal do Paraná, Brasil

Consejo Consultivo de THĒMIS-Revista de Derecho
Alfredo Bullard González, Pontificia Universidad Católica del Perú, Perú
Guido Calabresi, Universidad de Yale, Estados Unidos
Robert D. Cooter, Universidad de California - Berkeley, Estados Unidos
Javier de Belaúnde López de Romaña, Pontificia Universidad Católica del Perú, Perú
Fernando de Trazegnies Granda, Pontificia Universidad Católica del Perú, Perú
Carlos Fernández Sessarego†, Universidad Nacional Mayor de San Marcos, Perú
Baldo Kresalja Roselló, Pontificia Universidad Católica del Perú, Perú
César Landa Arroyo, Pontificia Universidad Católica del Perú, Perú
Javier Neves Mujica†, Pontificia Universidad Católica del Perú, Perú
Javier Pazos Hayashida, Pontificia Universidad Católica del Perú, Perú
Richard A. Posner, Universidad de Chicago, Estados Unidos
George L. Priest, Universidad de Yale, Estados Unidos
José Daniel Amado Vargas, Pontificia Universidad Católica del Perú, Perú

Consejo Ejecutivo de THĒMIS-Revista de Derecho
Lilian Raquel Cánepa Yufra, Pontificia Universidad Católica del Perú, Perú
Santiago Garnica Franco, Pontificia Universidad Católica del Perú, Perú
Joyce Alexandra Uriol Quiroz, Pontificia Universidad Católica del Perú, Perú
Franco Arce Saldarriaga, Pontificia Universidad Católica del Perú, Perú
Maria Fernanda Sanabria Gamboa, Pontificia Universidad Católica del Perú, Perú
Katherine Nicole Larios Pulido, Pontificia Universidad Católica del Perú, Perú

THĒMIS-Revista de Derecho es una publicación semestral, editada y publicada, en formato impreso y electrónico, por la Asociación Civil THĒMIS, conformada enteramente por estudiantes de la Facultad de Derecho de la Pontificia Universidad Católica del Perú. La revista fue fundada en 1965 y viene siendo publicada de manera ininterrumpida desde 1984. El contenido de la revista versa sobre temas relacionados al Derecho y la cultura jurídica en general, estando dirigida a un público de académicos, abogados y estudiantes de Derecho. Los artículos publicados en THĒMIS-Revista de Derecho constituyen una fuente de consulta tanto para profesionales como estudiantes, siendo una fuente importante de doctrina jurídica en el ámbito nacional. THĒMIS-Revista de Derecho es una Revista arbitrada que se encuentra oficialmente indizada en Latindex y Clase, Directory of Open Access Journals (DOAJ), sistemas de información de la Universidad Nacional Autónoma de México (UNAM), y en Dialnet, catálogo de la Universidad de La Rioja, España. Asimismo, THĒMIS-Revista de Derecho puede ser ubicada en el Repositorio digital de la Biblioteca de la Pontificia Universidad Católica del Perú, y en los agregadores Ebsco y vLex. De igual forma, THĒMIS-Revista de Derecho se encuentra anexada a los portales web internacionales de recepción de artículos ExpressO y Scholastica. Los estándares académicos y calidad editorial de nuestra revista se encuentran certificados internacionalmente. THĒMIS-Revista de Derecho, se encuentra en constante convocatoria abierta para recepción de artículos relativos al tema central que el Consejo Ejecutivo elija o a cualquier otro tema relacionado a la disciplina del Derecho.

ÍNDICE 79

TEMA CENTRAL: Derecho y tecnología

Avances tecnológicos y derechos fundamentales

Juan Carlos Díaz Colchado y Andreé Castro Arequipeño 15
Los derechos fundamentales y las nuevas tecnologías de la información y comunicación: una aproximación
Fundamental Rights and New Information and Communication Technologies: An Approach

César Landa Arroyo 37
Constitución, derechos fundamentales, inteligencia artificial y algoritmos
Constitution, Fundamental Rights, Artificial Intelligence and Algorithms

Omar Alvarado Escobar 51
Neutralidad de Red y libertad de expresión: una relación en debate
Net Neutrality and Freedom of Speech: A Disputed Relationship

Lidia Moreno Blesa 73
La retirada de contenidos ilícitos por los prestadores de servicios en línea
The Removal of Illegal Content by Online Service Providers

Antonio Robles Vargas y Jacqueline St. Laurent del Castillo 87
El virus más letal: la necesidad de una adecuada regulación peruana sobre las *fake news* en el Perú
The Most Lethal Virus: The Need for an Adequate Fake News Regulation in Peru

Ariel Vercelli 111
El extractivismo de grandes datos (personales) y las tensiones jurídico-políticas y tecnológicas vinculadas al voto secreto
(Personal) Big Data Extractivism and the Political-Legal and Technological Tensions Related to the Secret Vote

Juan Flaquer Riutort 127
La función publicitaria de las *cookies*: mecanismos de prevención y cautela en el Derecho español
The Advertising Function of Cookies: Prevention and Precautionary Mechanisms in Spanish Law

Gobierno electrónico y oportunidades de regulación

Dana Masumura Ynami y Valeria Acosta Chia 141
Atando los nodos sueltos: *blockchain* para la reducción de corrupción en las licitaciones públicas de ProInversión
Tying Up the Loose Ends: Blockchain to Reduce Corruption in ProInversión Public Bidding

María del Rosario Quiroga y Luis Fernando Roca 155
La Red Dorsal y los 'costos jurídicos' de mantener un proyecto que ya no es viable
The Dorsal Network and the 'Legal Costs' of Maintaining a Project that is No Longer Viable

Carmen Ruíz Hidalgo y Mónica Siota Álvarez 175
La colaboración de las plataformas digitales en la aplicación y en la recaudación de los tributos
The Collaboration of Digital Platforms in the Application and Collection of Taxes

Martín La Rosa Almenara 193
Tributación de criptomonedas y otros criptoactivos: análisis comparado
Taxation of Cryptocurrencies and Other Cryptoassets: Comparative Analysis

Tamara Rezqallah Arón 215
Innovando en la arenera: una aproximación a las *FinTech* y a la importancia de la implementación de un *sandbox* regulatorio en Perú
Innovating in the Sandbox: An Approach to FinTech and the Importance of the Implementation of a Regulatory Sandbox in Peru

José Villafuerte Mendoza 235
¿Podemos regular a la *FinTech*? Desafíos y propuestas
Can We Regulate FinTech? Challenges and Approaches

José Alonzo Jiménez Alemán 251
Fundamentos de la regulación del *crowdfunding*: a propósito del Decreto de Urgencia 013-2020 que establece el régimen jurídico del financiamiento participativo financiero
The Regulation of Crowdfunding: Regarding Emergency Decree 013-2020 Which Establishes the Legal Regime for Financial Crowdfunding

Modernización de la función jurisdiccional

Pere Simón Castellano 283
Inteligencia artificial y valoración de la prueba: las garantías jurídico-constitucionales del órgano de control
Artificial Intelligence and The Assessment of Evidence: The Legal-Constitutional Guarantees of the Supervising Body

Gonzalo Hierro Viétiez 299
Introducción al *blockchain*, los contratos inteligentes y su relación con el arbitraje
Introduction to Blockchain, Smart Contracts and their Relationship to Arbitration

Christian Valero Quispe 311
Derecho e inteligencia artificial en el mundo de hoy: escenarios internacionales y los desafíos que representan para el Perú
Law and Artificial Intelligence in Today's World: International Scenarios and the Challenges that they Represent for Peru

Optimización digital y desafíos para el Derecho Mercantil

H. Andrés Izquierdo 323
Minería de textos y datos e inteligencia artificial: nuevas excepciones al derecho de autor
Text and Data Mining and Artificial Intelligence: New Exceptions to Copyright

María del Carmen Alvarado Bayo y Daniela Supo Calderón 345
Blockchain y propiedad intelectual: aplicando una tecnología innovadora en la gestión de derechos intangibles
Blockchain and Intellectual Property: Applying a New Technology in the Management of Intangible Rights

Andrea Von Chrismar Medina y Benjamín Grebe Lira 359
Plataformas digitales y riesgos de conglomerado: desafíos para las autoridades de competencia en Iberoamérica en el análisis de operaciones de concentración
Digital Platforms and Conglomerate Risks: Challenges for Competition Authorities in Ibero-America in the Analysis of Concentration Operations

Isabella Monsante Moy, Ariana Novoa Suárez y Alejandra Quintanilla 373
Smart contracts como solución eficiente a los nuevos problemas del consumidor en el *e-commerce*
Smart Contracts as an Efficient Solution to the Consumer's Distrust of E-Commerce

Fiorella Senno Vassallo 393
¿Desea recibir comunicaciones promocionales? Un análisis desde las reglas de protección al consumidor y de datos personales
Would You Like to Receive Ads? An Analysis of Consumer and Data Protection Law

José Miguel Porto Urrutia 409
Gobierno corporativo en tiempos de *venture capital*
Corporate Governance in Times of Venture Capital

Derecho Laboral frente a las nuevas tecnologías

Cecilia Calderón Paredes 419
Las plataformas digitales y la particularidad de su papel en el mercado: su actividad económica y las implicancias laborales que se generan como consecuencia de su incorrecta implementación
Digital Platforms and the Particularity of Their Role in The Market: Their Economic Activity and the Labor Implications that are Generated as a Consequence of their Incorrect Implementation

Iván Blume Moore 435
Las nuevas tecnologías y la protección de datos en el entorno laboral: retos y perspectivas legales
New Technologies and Data Protection in the Workplace: Challenges and Legal Perspectives

Lucía Aragüez Valenzuela 451
Debates emergentes en materia laboral y de privacidad: sistemas de videovigilancia, algoritmos digitales e identificación biométrica de la persona trabajadora
Emerging Debates on Labor and Privacy Matters: Video Surveillance Systems, Digital Algorithms and Biometric Identification of the Worker

Raúl Feijóo Cambiaso 467
Hacia una adecuada protección del derecho fundamental al secreto e inviolabilidad de las comunicaciones en la relación laboral: análisis constitucional a la luz de las nuevas tecnologías
Towards an Adequate Protection of the Fundamental Right to Secret and Inviolable Communications in the Labor Relationship: Constitutional Analysis in Light of New Technologies

Coordinadores Generales

José Miguel Porto

Abogado por la Pontificia Universidad Católica del Perú (PUCP). Máster en Derecho por la Universidad de Chicago. Socio fundador de Porto Legal (antes Montezuma y Porto) desde el 2014, firma que lidera a la fecha y que se ha posicionado como líder en las prácticas de capital de riesgo, telecomunicaciones, *FinTech* y Protección de Datos.

Hasta el año 2009, se desempeñó como Gerente Legal de Nextel del Perú. Posteriormente, ocupó el cargo de Director y Senior Commercial Counsel para NII Holdings, Inc. (casa matriz de Nextel del Perú), empresa listada en el Fortune 500 y con base en Reston, Virginia. En esta posición lideró importantes transacciones tecnológicas en México, Brasil, Perú, Chile y Argentina para la compra de infraestructura, *hardware*, *software*, dispositivos y servicios para el despliegue de redes 3G de Nextel; para el desarrollo, integración, prueba, implementación y entrenamiento en nuevos sistemas informáticos; para la adquisición de *software* a medida, configuración e instalación; acuerdos para almacenamiento y desarrollo de portales; *built-to-suit*, venta y *leaseback* de torres de telecomunicaciones, acuerdos de compartición de infraestructura; procesos de tercerización, entre otros. También lideró transacciones para compra de entidades y activos, así como financiamientos sindicados, financiamiento de exportaciones y financiamientos de fabricantes y proveedores para las operaciones de Nextel en Latinoamérica.

Lawyer by the Pontifical Catholic University of Peru (PUCP). Has a Master's degree in Law from the University of Chicago. Founding Partner at Porto Legal (formerly Montezuma y Porto) since 2014, a firm he currently leads and which has positioned itself as a leader in the venture capital, telecommunications, FinTech and data protection practices.

He served as Chief Commercial Counsel of Nextel del Peru until 2009. Later, he served as Director - Senior Commercial Counsel for NII Holdings, Inc. (parent company of Nextel del Peru), a Fortune 500 company and based in Reston, Virginia. In this position he led important technology transactions in Mexico, Brazil, Peru, Chile and Argentina for the purchase of infrastructure, hardware, software, devices and services for the deployment of Nextel's 3G networks; for the development, integration, testing, implementation and training in new computer systems; for the acquisition of customized software, configuration and installation; agreements for storage and development of webportals; built-to-suit, sale and leaseback of telecommunications towers, infrastructure sharing agreements; outsourcing processes, among others. He also led transactions to purchase entities and assets, as well as syndicated financing, export financing and financing from manufacturers and suppliers for Nextel's operations in Latin America.

Diego Fernández

Abogado por la Pontificia Universidad Católica Argentina. Socio del área de Propiedad Intelectual, Tecnología de la Información y Privacidad de Marval O'Farrell Mairal. Experto en tecnología, con dieciocho años de experiencia en privacidad y protección de datos, privacidad en investigaciones internas y en el trabajo, *RegTech*, licencias de *software*, acuerdos de tecnología de la información, ciberseguridad y legislación penal en relación con delitos informáticos.

Asimismo, es miembro del Comité Ejecutivo de ITechLaw y presidente de su Comité Latinoamericano. También, es copresidente del Capítulo Argentino de la International Association of Privacy Professionals (IAPP), miembro del Comité de Datos Personales de la International Trademark Asssociation (INTA) y miembro del Comité de Tecnología del IBA. Además, es presidente del Comité de Privacidad y M&A de la Asociación Latinoamericana de Privacidad (ALAP) y miembro de la Junta Editorial de la publicación Global Privacy Law Review.

En el plano académico, Fernández es Director de Educación Legal Ejecutiva de la Universidad Torcuato Di Tella en su curso de Protección de Datos Personales. A su vez, es profesor invitado del curso *online* sobre privacidad de datos del The John Marshal Law School.

Lawyer by the Pontifical Catholic University of Argentina. Partner in the intellectual property, information technology and privacy practice group at Marval O'Farrell Mairal. He is a technology expert, with eighteen years of experience in privacy & data protection, privacy compliance, privacy in internal investigations and at the workplace, RegTech, software licensing, IT agreements, IT compliance, cyber security, and criminal law in connection with technology.

Additionally, he is a member of the Executive Committee of ITechLaw (and Chair of the Latin America Committee). He is also Co-Chair of the IAPP's Argentine Chapter, member of the Data Protection Committee of INTA, member of the Technology Committee of IBA. Furthermore, he is the President of the Privacy & M&A Committee of the Latin America Privacy Association (ALAP) and Editorial Board Member of the Global Privacy Law Review.

In the academic field, Fernández is a professor on the Privacy & Data Protection Legal Education Executive Program at Universidad Di Tella. He is also a guest professor at The John Marshall Law School, Chicago (United States) in its online course on Global Privacy.

Asesor Temático

Miguel Morachimo

Abogado por la Pontificia Universidad Católica del Perú (PUCP). Máster en Derecho, Ciencia y Tecnología por la Universidad de Stanford, California. Candidato a Máster en Administración de Empresas (MBA) de la Universidad de Toronto. Fundador y actual Director Ejecutivo de la organización sin fines de lucro Hiperderecho. Actual coorganizador del capítulo local de Legal Hackers Lima y uno de los líderes del capítulo peruano de Creative Commons. Profesor a tiempo parcial en las facultades de Derecho de la Universidad del Pacífico y la Pontificia Universidad Católica del Perú.

Anteriormente, ha sido miembro de la Comisión de Derecho y Tecnología del Colegio de Abogados del Lima (2017-2019). Ha brindado testimonio y contribuido a más de una docena de procesos de política pública en el Congreso y el Poder Ejecutivo. Su trabajo se centra en entender la relación entre la innovación tecnológica y el ejercicio de derechos individuales y colectivos, con énfasis particular en controles de información, vigilancia gubernamental y explotación corporativa de datos personales.

Lawyer by the Pontifical Catholic University of Peru (PUCP). Has a Master's degree in Law, Science and Technology by Stanford University. MBA candidate at University of Toronto. Founder and Executive Director of the nonprofit Hiperderecho. He is the current co-organizer of Legal Hackers Lima and one of the leaders of the Peruvian Creative Commons chapter. Part-time teacher at the Law Schools of Pacifico University and Pontifical Catholic University of Peru (PUCP).

Previously, he has been a member of the Law and Technology Commission of the Lima Bar Association (2017-2019). He has also acted as an expert witness and contributed to over a dozen public policy projects from both Congress and the Executive Branch. His work centers around understanding the relationship between technological innovation and the exercise of individual and collective rights, particularly in regards to information controls, government surveillance and corporate exploitation of personal data.

DERECHO Y TECNOLOGÍA

10.18800/themis.202101.001

LOS DERECHOS FUNDAMENTALES Y LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN: UNA APROXIMACIÓN

FUNDAMENTAL RIGHTS AND NEW INFORMATION AND COMMUNICATION TECHNOLOGIES: AN APPROACH

Juan Carlos Díaz Colchado*
Pontificia Universidad Católica del Perú

Andreé Castro Arequipeño**
Exmiembro de THĒMIS
Pontificia Universidad Católica del Perú

The use of new information and communication technologies in different areas of society is increasing. On one hand, there is no doubt that technology has a positive impact on society. However, on the other, its application cannot be unrestricted, but rather, based on a harmonious reading of the Constitution, it must be limited on the basis of material criteria such as fundamental rights.

In this article, the authors analyze the irruption of new technologies –such as big data and algorithms– in the general theory of fundamental rights, delimiting their concepts, foundations, contents, among others. In addition, the authors explore the impact on certain fundamental rights such as personal freedom and privacy. Finally, from a critical point of view, they distinguish when the use of these new technologies in specific situations becomes constitutional or, failing that, unconstitutional.

Keywords: New technologies; fundamental rights; internet; big data; algorithms; artificial intelligence.

El uso de las nuevas tecnologías de la información y comunicación en los diferentes ámbitos de la sociedad cada vez es mayor. Por un lado, es indudable que la tecnología genera un impacto positivo en la sociedad. Empero, por otro lado, su aplicación no puede ser irrestricta, sino que, a partir de una lectura armónica de la Constitución, debe limitarse sobre la base de criterios materiales como lo son los derechos fundamentales.

En el presente artículo, en primer lugar, los autores analizan la irrupción de las nuevas tecnologías –como el big data *y los algoritmos– en la teoría general de los derechos fundamentales, delimitando sus conceptos, fundamentos, contenidos, entre otros. Sumado a ello, en segundo lugar, los autores exploran la incidencia que se produce sobre determinados derechos fundamentales como la libertad personal y la privacidad. Finalmente, desde una mirada crítica, los autores distinguen cuándo el uso de estas nuevas tecnologías en situaciones concretas deviene en constitucional o, en su defecto, en inconstitucional.*

Palabras clave: Nuevas tecnologías; derechos fundamentales; internet; big data*; algoritmos; inteligencia artificial.*

* Abogado. Magíster en Derecho Constitucional e Investigación Jurídica por la Pontificia Universidad Católica del Perú (PUCP). Docente de Derecho Constitucional de la PUCP y de la Universidad Nacional Mayor de San Marcos (UNMSM) (Lima, Perú). Contacto: jdiazc@pucp.edu.pe

** Estudiante de décimo ciclo de Derecho de la Pontificia Universidad Católica del Perú (PUCP). Asistente de docencia del curso de Sistema de Justicia y Fundamentos Constitucionales del Proceso, y Derechos Fundamentales en la PUCP. Practicante en Miranda & Amado (Lima, Perú). Contacto: acastroa@pucp.edu.pe

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 28 de enero de 2021, y aceptado por el mismo el 17 de abril de 2021.

"La tecnología nueva no es buena o mala.
Tiene que ver con cómo las personas eligen usarla".
David Wong

I. INTRODUCCIÓN

El siglo XXI se caracteriza por la penetración intensa de las tecnologías de la información y comunicación, calificadas como 'nuevas tecnologías', en la vida diaria de las personas. Todos los días, desde que despertamos hasta que culmina el día, nuestras actividades están atravesadas por la presencia de la tecnología, siendo hoy su faz más visible el aparato de telefonía móvil.

Con este aparato, no solo nos comunicamos a través de mensajería de voz, sino también con videollamadas, lo que se ha intensificado por las medidas de confinamiento adoptadas para hacer frente a la pandemia del COVID-19, de modo que no solo nos comunicamos, sino que también desarrollamos nuestras labores (trabajo remoto) o nos capacitamos (educación virtual). Siendo que el internet, la herramienta tecnológica que lo hace posible, se convierte en una gran fuente de recursos asociados con la gestión de la información, tanto la que por mutuo propio generamos como las que generan otros, para los más diversos fines, incluyendo el ocio y el esparcimiento. Incluso, en algunos países, la tecnología de la información se ha empleado como una herramienta para velar por la salud pública a través del monitoreo de los contagios que se producían durante la pandemia del COVID-19 y que aún se mantienen.

La irrupción de estas nuevas tecnologías si bien ha recibido una profunda atención de parte de los hacedores de política pública para posibilitar su desarrollo y regulación administrativa, no es menos cierto que también es posible tener una perspectiva de análisis a partir de los derechos fundamentales, tanto desde la perspectiva de su teoría general, como desde algunos derechos específicos, con relación a la incidencia que las nuevas tecnológicas representan para estas instituciones constitucionales, tanto en sus aspectos positivos (en tanto permiten optimizar su ejercicio) como desde sus desafíos (en tanto supongan un riesgo a su ejercicio).

En dicho contexto, el presente trabajo persigue presentar, de modo descriptivo, a partir de una aproximación conceptual a las nuevas tecnologías (numeral II), la incidencia que tienen en distintos aspectos de la teoría general de los derechos fundamentales (numeral III) y de aspectos específicos de algunos de ellos (numeral IV), destacando su impacto positivo y los desafíos que representan estas nuevas tecnologías en lo que al contenido de los derechos fundamentales se refiere; así como su incidencia en el surgimiento de nuevos derechos (numeral V).

II. APROXIMACIÓN AL CONCEPTO DE 'NUEVAS TECNOLOGÍAS' DE LA INFORMACIÓN DE LA INFORMACIÓN Y COMUNICACIÓN

Para analizar la incidencia de las 'nuevas tecnologías' de la información y comunicación en los derechos fundamentales es necesario realizar algunas aproximaciones conceptuales en torno a lo que se debe entender por 'nuevas tecnologías' de la información y comunicación, y cuáles, para efectos del presente trabajo, reciben tal consideración. En dicho sentido, debido a su presencia cada vez más intensa en la vida cotidiana de las personas y a los retos que representan para el derecho, se debe comprender dentro de esta categoría al internet, el *big data,* los algoritmos y la inteligencia artificial. Esto no significa que no existan otras (realidad virtual, por ejemplo), pero esas no serán objeto de tratamiento en el presente trabajo.

A. Aproximación conceptual a las nuevas tecnologías de la información y comunicación

El mundo está en constante cambio y evolución, por ello día a día aparecen nuevas innovaciones tecnológicas que ayudan y facilitan ciertas actividades humanas. Por tanto, debemos considerar que las nuevas tecnologías son aquellas innovaciones que realiza el ser humano con la finalidad de que algunas actividades sean realizadas de manera más eficiente, pero, sobre todo, con menos esfuerzo y riesgo.

Sin embargo, ¿qué son las 'nuevas tecnologías' de la información y comunicación? Al respecto, Díaz Revorio agrupa diversos instrumentos que combinan tecnologías de las telecomunicaciones, de la informática y la radiodifusión, que en conjunto posibilitan la transmisión y recepción de información y comunicación como la telefonía fija, móvil, televisión, radio, *Global Positioning System* (GPS), los ordenadores, fax, videoconferencias, *Short Message Service* (SMS), el correo electrónico, el chat y otros servicios de mensajería instantánea, siendo el internet la que tiene un indudable protagonismo (2010, pp. 35-36). Por otro lado, para Raúl Oroño construir un concepto exacto sobre qué son las nuevas tecnologías puede ser problemático y complejo, no obstante, indica que la característica de 'nueva' se refiere a que antes ya existían tecnologías, las cuales se van renovando constantemente. Es por ello que cobra sentido el ser nuevas, puesto que siempre existirá una más moderna que otra, en tanto que por tecnología entiende el uso de materiales, instrumentos, técnicas y fuentes de

energía a fin de facilitar la vida y hacer más productivo el desarrollo del trabajo (2007, p. 237).

Lo cierto es que pueden establecerse conceptos más amplios o restringidos, pero que, como la propia experiencia demuestra, debido a la innovación permanente del sector, siempre habrá 'nuevas tecnologías' que surgirán para actualizar a las que ya existen o simplemente para reemplazarlas progresivamente, como ha sucedido con el ordenador de escritorio, reemplazado por las laptops y ahora estas por los teléfonos móviles.

Es así que, para el desarrollo de estas 'nuevas tecnologías' de la información y comunicación, el ser humano creó vías que faciliten la implementación de estas en todo el mundo. Como muestra de ello, se desarrolló el internet a nivel mundial, puesto que los gobiernos comprendieron y asimilaron las ventajas que otorga esta tecnología a la sociedad. Del mismo modo, podemos apreciar como los Estados están predispuestos a apostar por las innovaciones tecnológicas, tanto así que, incluso, en algunos países estas innovaciones son consideradas como parte de sus políticas públicas.

Ello en la medida que en el mundo existen múltiples países que se encuentran en constante competencia, no solo cultural, económica o social, sino también dentro una carrera tecnológica, factor que 'juega' en la geopolítica mundial (recordemos el caso de la compañía china Huawei y las acusaciones de espionaje que desde el gobierno de Trump se le hicieron). De ahí que, en la actualidad, esta carrera resulta una de la más importantes. Así, herramientas como el *big data* o la inteligencia artificial (IA) pueden solucionar problemas de manera célere y eficiente, así como ser factores de desequilibrio en las relaciones internacionales.

En relación con las políticas nacionales, con el fin de implementar el acceso a las nuevas tecnologías, desde el año 2012, en el Perú se ha implementado una política pública para propiciar la conectividad a nivel nacional mediante redes de fibra óptica para facilitar el acceso al internet. Se hace referencia a la Ley de Promoción de la Banda Ancha y construcción de la Red Dorsal Nacional de Fibra Óptica, publicada el 20 de julio de 2012, cuyo propósito fue

> […] impulsar el desarrollo, utilización y masificación de la Banda Ancha en todo el territorio nacional, tanto en la oferta como en la demanda por este servicio, promoviendo el despliegue de infraestructura, servicios, contenidos, aplicaciones y habilidades digitales como medio que favorece y facilita la inclusión social, el desarrollo socioeconómico, la competitividad, la seguridad del país y la transformación organizacional hacia una sociedad de la información y el conocimiento (Ley 29904, 2012, art. 1).

El objetivo era interconectar las capitales de las regiones (lo que se ha logrado), y desde ahí, a las distintas capitales de provincia y los distritos, especialmente los más alejados; y dentro de ellos a los colegios y centros de salud. Lamentablemente, el proyecto, que aún sigue en desarrollo, no ha tenido los resultados esperados (Campodónico, 2019). Pero lo avanzado ciertamente debe ser mejorado.

A pesar de esta experiencia nacional, las nuevas tecnologías de la información y comunicación, dado su carácter dinámico, siguen creándose y mejorando, y así tenemos herramientas como el internet, al que ya hicimos referencia, pero también al *big data*, los algoritmos y la inteligencia artificial, las que de forma estipulativa se consideran las nuevas tecnologías de la información y comunicación para el análisis que se desarrollará en el presente trabajo. Por ello, abordaremos brevemente sus conceptos, para con ellos efectuar el análisis de su incidencia en la teoría de los derechos fundamentales y en algunos de ellos.

B. Aproximación conceptual al internet

Hace aproximadamente treinta años se logró orquestar una red de conexión entre diversos ordenadores a nivel mundial, en la cual se podía compartir recursos, imágenes, entre otros y entablar una conversación con otra persona, ubicada en otro hemisferio, de manera instantánea. A este descubrimiento, se le llamó internet. Sin imaginarlo, este ha sido de gran utilidad para muchas generaciones desde 1990 hasta la actualidad. Según Elena de la Cuadra, es a través del internet que las personas, hoy en día, logran comunicarse inmediatamente con cualquier parte del mundo, con la intención de obtener información sobre algún tema que es de interés, conseguir un juego, incluso, observar los fondos de alguna institución pública estadounidense (1996, p. 35).

En ese mismo sentido, Marco Zamora Lucio indica que el internet es una gran red compuesta por miles de redes y computadoras que están conectadas entre sí mediante el uso de cables y sistemas que tienen en común el mismo uso de tecnología (2014, p. 4). También se ha señalado que en internet es posible distinguir tres estratos interrelacionados: (i) el estrato físico constituido por la propia red y las conexiones físicas; (ii) el estrato lógico constituido por la interfaz, esto es la conexión física y funcional entre los dispositivos y redes, que es posible por el *software*, los estándares técnicos, así como los protocolos de comunicación diseñados especialmente para ello; y (iii) el estrato de los

servicios y contenidos, compuesto por múltiples fuentes de información, así como los servicios que se presta en línea y que se ponen a disposición de los usuarios por distintos proveedores (públicos y privados) (Barrio Andrés, 2017, pp. 36-37).

A partir de lo señalado, se puede entender al internet como una macrored que, compuesto por los estratos antes indicados, permite a las personas, así como a los ordenadores, intercambiar información de manera célere e inmediata, mediante el uso de un dispositivo móvil o fijo, tales como los celulares, tabletas, computadoras de mesa, laptops, entre otros.

Es a partir de este invento que los humanos pueden enviar y recibir correos electrónicos, a través del uso del correo electrónico; compartir links, mediante el uso de una red social o vía mensajería instantánea; usar Whatsapp, Facebook, Twitter y las demás redes sociales presentes en la actualidad; así como navegar en los buscadores, tales como Google Chrome, Internet Explorer, Mozilla Firefox, entre otros.

Tras conceptualizar y describir los beneficios que le otorga a la sociedad el internet, podemos indicar que esta macrored es el punto de partida de las llamadas 'nuevas tecnologías', puesto que, sin una red que posibilite el intercambio de información a larga distancia, las aplicaciones, la inteligencia artificial, el *big data*, los algoritmos, estas no podrían operar de manera independiente y adecuada. Es decir, el internet sirve como una vía de comunicación y un canal común para el desarrollo de las funcionalidades de las nuevas tecnologías.

Realizando una comparación, el internet sería como una carretera que conecta miles de kilómetros para que las personas y los vehículos se puedan conectar entre ciudades, países e, incluso, en algunos casos, continentes. Sin embargo, el internet cuenta con una peculiaridad, ya que logra esta conexión de manera instantánea, en cuestión de segundos o de milésimas de estos.

Ahora, la pregunta que surge es, ¿cuál es la relevancia del internet y las nuevas tecnologías para el Derecho? La respuesta puede resultar sencilla, pero a la vez compleja, ya que puede indicarse que hay una relación bilateral. Ello debido a que, podemos entender a la relación entre las tecnologías y el Derecho, en una primera acepción, como que el Derecho regula el uso de las nuevas tecnologías por las personas; y en una segunda, como que el Derecho aprovecha la irrupción de las nuevas tecnologías, y además de regularlas, se aprovecha de estas para optimizar el ejercicio del derecho y de los derechos fundamentales (y legales) en el mundo.

En el presente trabajo se asume esta segunda concepción, ya que, a raíz de la pandemia ocasionada por el COVID-19, el uso de nuevas tecnologías se ha incrementado de manera exponencial, por lo que a nivel mundial los gobiernos, para mitigar y reducir el índice de contagios diarios, optaron por suspender derechos fundamentales, ordenar el confinamiento y la paralización de las actividades cotidianas, tales como el trabajo y los servicios educativos. Es entonces, cuando el uso de las nuevas tecnologías se torna cada vez más necesario, ya que, para reemplazar los espacios físicos, estas últimas crearon y reforzaron canales de comunicación que se asimilen a dichos espacios para la realización de las actividades diarias. Es así como hoy en día, conocemos plataformas como Zoom, Microsoft Teams, Google Meet, Cisco Webex, entre otras. Asimismo, el uso de nuevas tecnologías se encuentra regulado por el Derecho y sus diversas ramas, ya que, sin una regulación legal, el uso de estas sería desordenado, e incluso podría ocasionar problemas para los usuarios.

Entonces, podemos concluir que el internet es una macrored que permite que las personas, independientemente de dónde se encuentren, se puedan conectar unas con otras e intercambiar información, así como entablar comunicaciones. Asimismo, internet se constituye en el punto de partida para conceptualizar lo que son las nuevas tecnologías, ya que sirve como el medio de soporte, y por el cual se materializan estas. Finalmente, que la relación entre el Derecho y las nuevas tecnologías es una relación bilateral, de contribución mutua.

C. Aproximación conceptual al *big data*

Luego de la aproximación realizada al concepto de internet, y su incidencia e importancia en el mundo de las nuevas tecnologías, corresponde desarrollar el concepto de *big data*. Sobre el particular Hernadez-Leal, Duque-Mendez y Moreno-Cadavid nos indican que el *big data* es una gran agrupación de datos, pero que además dentro de este gran volumen, existe una gran variedad, a la cual pueden acceder de manera inmediata los usuarios que contraten este servicio (2017, p. 3).

En ese mismo sentido, Hernandez-Leal, Duque-Mendez y Moreno-Cadavid conceptualizan al *big data* como un conjunto de datos de gran tamaño, rápidos o complejos, a los cuales no se podría acceder de manera tradicional, sino que se requiere que se utilice una base de datos (2017, p. 3). Entonces podemos decir que el *big data* es la agrupación de una gran cantidad de datos complejos y a los cuales se puede acceder de manera veloz a través del uso de una plataforma o un sistema que lo faculte.

Por su parte Cotino Hueso (2017) caracteriza al *big data* a partir de las 5V: volumen, variedad, velocidad, valor y veracidad. La primera característica alude al volumen masivo de la información, pues está constituido por una ingente cantidad de datos que pueden ser inabarcables para el cerebro humano; datos que también son variables debido a su diversidad de fuentes y naturaleza (banco de datos públicos o privados, automatizados y digitalizados y puestos en línea); que pueden ser gestionados y actualizados a gran velocidad; que tienen un gran valor potencial presente y futuro; que deben ser, veraces en lo posible (dado que también estos datos podrían contener información incorrecta o no actualizada); y que no pueden ser manipulados, procesados y analizados con mecanismos tradicionales (manuales) (2017, pp. 131-132).

Es en ese sentido que, el *big data*, al ser parte de las nuevas tecnologías, es una gran innovación para aquellos usuarios que deseen acceder a una gran cantidad de datos confiables y acordes a la coyuntura de manera célere. Es entonces, una herramienta útil para aquellas instituciones o empresas que desean filtrar información, y así lograr sus objetivos con el apoyo de las nuevas tecnologías.

No obstante, el *big data* puede ser sumamente problemático para el Derecho, puesto que se ve constantemente que esta condensación de datos puede incluir información íntima o sensible que vulnere derechos de privacidad e intimidad. En ese sentido, como se explicó anteriormente, el Derecho actúa como un regulador de las nuevas tecnologías, es por ello que, si se detecta una intromisión ilegítima en las esferas de privacidad e intimidad de una persona, por el uso de *big data*, este debe de tomar las medidas necesarias para finalizar dicha afectación.

Para ayudar a la conceptualización del *big data* tomaremos como referencia a Scopus, una base de datos bibliográfica de resúmenes y citas que son utilizadas en artículos de revistas científicas. Esta base de datos tiene como peculiaridades realizar opciones de búsqueda, calcular la cantidad de citas utilizadas, analizar el rendimiento de un autor específico, entre otras. Es así que, esta base de datos se encarga de facilitar y optimizar la labor de los autores al momento de redactar ensayos, ya sean literarios, jurídicos, científicos, entre otros.

Sin embargo, dicha optimización no sería realizable si es que esta plataforma, además de las funcionalidades que ofrece, permitiría que los autores puedan revisar el historial médico de los autores que citan, puesto que, ello ya constituye una afectación a la esfera de privacidad de otra persona. Es en esos momentos en los cuales el Derecho actúa y regula la operación del *big data* para que sirva como una herramienta para la sociedad, pero que respete y no vulnere los derechos de otras personas.

Es así que, el *big data* es el conjunto de datos de gran tamaño que cuenta con las características antes aludidas (volumen, variedad, velocidad, variabilidad y veracidad). Asimismo, esta herramienta virtual es de suma utilidad para las actividades del sector público como privado. No obstante, al estar regulado por el Derecho, el ejercicio del *big data* debe de respetar los límites establecidos por la regulación al momento de realizar su funcionalidad. Cabe mencionar que, actualmente, es uno de los íconos de las nuevas tecnologías, ya que sirve como herramienta para diversas empresas o instituciones a nivel mundial.

D. Aproximación conceptual a los algoritmos

Así como el *big data*, hoy en día los algoritmos cobran vital importancia para el desarrollo de muchas aplicaciones, redes sociales y base de datos. Pero, ¿qué es un algoritmo? Un algoritmo es una secuencia de instrucciones que ofrecen una forma de resolución a un determinado tipo de problema, es decir, es un sistema que emite una respuesta especial para un tipo de problema específico. En otras palabras, podemos definir al algoritmo como una respuesta específica para un problema específico, disponible en la red (Joyanes Aguilar, 2008, p. 64). Incluso, Joyanes Aguilar indica que los algoritmos muchas veces son más importantes que los lenguajes de programación de computadoras. ¿En qué basa dicha afirmación? Puesto que, el lenguaje de programación es un medio para expresar, finalmente, un algoritmo; es decir, que el algoritmo es el producto final de un proceso de programación.

¿Cuál es el uso de los algoritmos en la sociedad? Para responder esta pregunta, cabe reflexionar en torno a la siguiente cuestión: ¿han advertido que cuando se está haciendo uso de alguna red social, ya sea Facebook, Instagram, entre otras, aparecen anuncios de intereses que buscamos antes en algún buscador o en la misma red social? Pues, estamos seguros de que sí. Muchas veces buscamos algún objeto en Google, Safari, Mozilla Firefox, etc., e inmediatamente al ingresar a alguna red social observamos que aparecen varios anuncios relacionados a nuestra anterior búsqueda. Es así que, podemos señalar que los algoritmos, en el ejemplo comentado anteriormente, son utilizados por las aplicaciones a través de una lectura y análisis de preferencias y gustos de los usuarios para ofrecerle las mejores opciones acorde a sus búsquedas anteriores para optimizar su experiencia de navegación o hacer de esta una herramienta

más eficiente (en términos de tiempo y uso de la infraestructura tecnológica que se emplee).

Los algoritmos se caracterizan porque son precisos, ya que no tienen margen de error, y, por ende, no incurren en ambigüedades al momento de emitir un resultado. En segundo lugar, son definidos, puesto que si se repite el algoritmo varias veces el resultado seguirá siendo el mismo. En tercer lugar, son finitos, debido a que no será eterno, sino que tendrá un final en algún momento. Por último, debe de emitir un resultado al cumplirse el proceso interno de cada algoritmo (Joyanes Aguilar, 2008, p. 65).

En buena cuenta, los algoritmos son una secuencia de instrucciones que arrojan un resultado que será preciso y no ambiguo; asimismo, estará definido a que el resultado siempre sea el mismo; y, del mismo modo, estará limitado a un número finito de repeticiones. Entonces, los algoritmos siempre serán el resultado de acciones que realicen los usuarios ante una preferencia o interés.

No obstante, los algoritmos a través de su funcionalidad pueden constituir una afectación a la protección de los datos personales de cada usuario, puesto que, si bien cuando se instala una aplicación se acepta los términos y condiciones, generalmente el usuario no suele leerlas. En ese sentido, al aceptar las condiciones sin la debida diligencia, se otorga consentimiento para que haya un tratamiento de datos sin restricciones para las empresas operadoras, lo que lleva a que estas manipulen de manera legítima o no la información y datos personales. Sin embargo, esta problemática será abordada en un apartado posterior del presente trabajo (numeral IV.D).

E. Aproximación conceptual a la inteligencia artificial

Continuando con la exposición, ahora nos toca conceptualizar a la inteligencia artificial. La inteligencia artificial ha generado un gran impacto y revuelo en la sociedad actual, ello en virtud de las razones que expondremos a continuación. Según Carolina Martínez Bahena, la inteligencia artificial es una rama de la informática que es utilizada para que las máquinas puedan realizar tareas que solo pueden ser realizadas por el ser humano, ya que se requiere cierto grado de razonamiento (2012, p. 828). En ese mismo sentido, Enrique Cáceres indica que la inteligencia artificial es el desarrollo de programas cuya finalidad es el procesamiento de información de manera inteligente, realizado por una máquina, con la finalidad de que sea esta última la que reemplace de manera permanente a las personas (2006, p. 606).

Es en ese sentido que la inteligencia artificial está revolucionando los conceptos clásicos y convencionales de la informática, ya que al introducir una tecnología que permita que un ordenador o una máquina pueda tener un grado de razonamiento e inteligencia emocional, genera que esta convencionalidad se vea quebrantada. Asimismo, genera preocupación en algunos sectores de la sociedad, ya que la esencialidad del trabajo humano podría estar en riesgo, puesto que el capital humano ya no sería necesario (Toyama Miyagusuku & Rodríguez León, 2019, pp. 257-265).

Sin embargo, consideramos que la inteligencia artificial es una herramienta de suma utilidad para la sociedad porque, al ser un sistema inteligente, puede realizar actividades que son catalogadas como sumamente peligrosas para el ser humano. Asimismo, consideramos que esta nueva tecnología tiene incidencia en todos los campos en los que interactúa el ser humano, especialmente en el Derecho, ámbito en el cual la inteligencia artificial puede facilitar la toma de decisiones judiciales (Nieva Fenoll, 2018, pp. 18-31).

Ello porque los jueces suelen tener esquemas de juicio de manera rígida, lo que se pone en evidencia en algunos casos con características similares o que están referidos al mismo delito, por lo que muchas veces no valoran los medios probatorios, como en el robo, y adoptan generalmente la misma decisión para estos casos (Cáceres, 2006, pp. 607-609). Asimismo, en Estados Unidos los abogados defensores, en algunos estados, suelen utilizar Lexis Nexis, plataforma que utiliza inteligencia artificial, así como algoritmos y base de datos, ya que permite consultar en su amplio y completo servicio de información en línea (s.f., p. 2).

Es así como podemos apreciar que la inteligencia artificial funge como una herramienta de suma utilidad para la población, ya que puede apoyar desde la construcción de un puente hasta para predecir el resultado de una decisión judicial con suma precisión. Entonces, con miras a la modernización global de la sociedad, se debe poner de relieve que la inteligencia artificial empieza a ser un punto de referencia para esta revolución. Muestra de ello, es la construcción de COG, un robot humanoide creado por el Massachusetts Institute of Technology (MIT), cuyo objetivo radica en su interacción con el medio ambiente y con las personas que lo rodean, para que así pueda realizar actividades diarias tal como un ser humano lo haría.

Asimismo, es importante mencionar que el Derecho juega un papel muy importante para regular la actividad de la inteligencia artificial, ya que todas las facilidades que otorga a la sociedad deben de

guiarse por un respeto irrestricto a los derechos fundamentales de las personas.

Entonces, como un recuento general, la inteligencia artificial es un sistema que genera que una máquina cuente con razonamiento propio (especialmente de aquellos que aprenden de su propio funcionamiento) o, al menos, muy parecida al razonamiento humano. Es así que, sirve de apoyo tanto para la realización de actividades cotidianas como para aquellas que requieren un alto grado de experticia.

Tras exponer los principales elementos que conforman las nuevas tecnologías (tales como el internet, el *big data*, los algoritmos y la inteligencia artificial), podemos indicar que todos estos componentes tienen una característica en común: innovan y revolucionan el mundo, las relaciones entre pares, las relaciones laborales, las ciencias, y, sobre todo, los modelos convencionales y tradicionales de diversas áreas del conocimiento, como el Derecho, y, desde luego, los derechos fundamentales. Por ello, seguidamente pasaremos a detallar la incidencia que estas nuevas tecnologías tienen en la teoría general de los derechos fundamentales, así como en algunos de ellos.

III. INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN LA TEORÍA DE LOS DERECHOS FUNDAMENTALES

La teoría general de los derechos fundamentales está constituida por una serie de herramientas conceptuales que son comunes a todos los derechos y a partir de los cuáles se puede comprender y estudiar el régimen jurídico constitucional de cualquier catálogo de derechos reconocidos en las constituciones nacionales (Pino, 2018, pp. 115-120).

Estos elementos conceptuales buscan responder a las siguientes preguntas: ¿por qué razones consideramos que algo es un derecho fundamental? ¿Qué es un derecho fundamental? ¿Quién es titular de un derecho fundamental? ¿Cuál es el contenido de los derechos fundamentales? ¿Quién está obligado a respetar y optimizar el ejercicio de los derechos fundamentales? ¿Cuáles son los límites al ejercicio de los derechos fundamentales? Estas preguntas, respectivamente, tratan sobre el fundamento, el concepto, la titularidad, el contenido protegido, los sujetos obligados y los límites de los derechos fundamentales (Castillo Córdova, 2020, pp. 120-153).

Por ello, resulta de interés advertir la incidencia que tienen las nuevas tecnologías en los distintos aspectos conceptuales indicados. En los siguientes apartados se presentarán una serie de posiciones académicas que si bien parten de presupuestos filosóficos y teóricos disímiles (algunos incluso son abiertamente críticos entre sí), lo que se busca poner de relieve es que existen desarrollos sobre la teoría de los derechos fundamentales y que, en mayor o menor medida, sirven para el análisis de la irrupción de las nuevas tecnologías en los derechos fundamentales.

A. En relación con el fundamento de los derechos fundamentales

En la teoría de los derechos fundamentales se han formulado distintas posiciones teóricas sobre el fundamento de los derechos (Pérez Luño, 2004, pp. 105-133), por mencionar solo algunas tenemos aquellas basadas en la dignidad; los principios de autonomía, inviolabilidad y dignidad de la persona; los bienes humanos; y las necesidades básicas.

La finalidad principal de estos discursos radica en justificar o dar razones que permiten sostener que algo (conducta, acción, prestación u otro objeto jurídicamente relevante) califica como derecho fundamental. En ese sentido, se ha indicado que la dignidad de la persona, que hace de esta fin y no medio, constituye el fundamento de los derechos y del propio ordenamiento jurídico, de modo tal que los derechos que se vayan reconociendo sean tributarios de la dignidad, en tanto permiten lograr mayores niveles de tratamiento de la persona como fin y como destinatario de la acción estatal (Landa Arroyo, 2000, p. 14).

Complementariamente, podríamos entender que los derechos fundamentales son tales en tanto coadyuvan a lograr los mayores niveles posibles de libertad de la persona para elegir sus propios planes y proyectos de vida (principio de autonomía), que por esa consideración son valiosos y determinan que los sacrificios o restricciones que se le imponen sean realizados en su propio beneficio, con lo que se prohíbe las intervenciones públicas o privadas que no redundan a su favor (principio de inviolabilidad), por lo que las personas deben ser tratadas según lo hayan determinado sus decisiones, intenciones o expresiones de consentimiento (principio de dignidad) (Nino, 1989, pp. 204-205, 237 & 287).

En igual medida, se indica que el concepto de persona incluye una serie de bienes humanos necesarios para su perfeccionamiento y que precisamente, esos bienes (salud, educación, libertad, etc.) siendo necesarios se protegen bajo la forma de derechos fundamentales (Castillo Córdova, 2020, pp. 100-101). En tanto que, desde la tesis de las necesidades

básicas, se sostiene que son derechos fundamentales aquellas prestaciones que tienen por finalidad satisfacer esas necesidades que se consideran esenciales e indispensables para la propia existencia de la persona (Sosa Sacio, 2015, p. 96).

A partir de estas estrategias argumentativas es posible justificar que a raíz de la incidencia de las nuevas tecnologías en la vida cotidiana de las personas estamos frente a nuevos derechos fundamentales, en tanto los mismos sirvan para optimizar la dignidad de la persona, reforzar su autonomía individual, sirvan para su perfeccionamiento o satisfagan sus necesidades básicas.

Así, por ejemplo, el acceso a internet, que desde Naciones Unidas se postula como un nuevo derecho humano (Consejo de Derechos Humanos, 2016), se constituye además como un verdadero derecho fundamental, en tanto el internet (y la infraestructura tecnológica necesaria para su acceso y uso) coadyuvan a que la persona pueda desarrollar su vida en condiciones de dignidad en tanto le permite el acceso a la sociedad de la información y a distintas fuentes para el desarrollo de su proceso educativo, la protección de su salud (siempre que se trate de información confiable y científicamente validada) y el desarrollo de sus actividades laborales (sea bajo trabajo remoto o presencial) o educativas. De modo que el acceso a internet coadyuva a reforzar la dignidad de las personas. Sin embargo, este acceso también se constituye como un bien humano dado que permite su perfeccionamiento (educación y trabajo). Además, debido al alcance que hoy tienen las nuevas tecnologías, donde la comunicación y el acceso a la información son una necesidad indispensable para el desarrollo de casi todas las actividades diarias, el acceso al internet se constituye como un derecho en tanto busca satisfacer una necesidad básica o esencial para la persona.

De este modo, desde la irrupción de las nuevas tecnologías de la información y comunicación, las distintas posiciones teóricas sobre el fundamento de los derechos fundamentales permiten elaborar argumentos para justificar que ciertos objetos asociados a ellas se constituyen como verdaderos derechos fundamentales.

B. Sobre el concepto de los derechos fundamentales

El concepto de los derechos fundamentales agrupa las características que estos deben reunir para ser calificados como tales. En dicho sentido, para Ferrajoli, los derechos fundamentales son derechos subjetivos que corresponden a todos los seres humanos (universalidad) en cuanto tengan reconocido el estatus de persona, de ciudadanos o de personas con capacidad para obrar. En su aproximación, el 'derecho subjetivo' debe entenderse como una expectativa de recibir una prestación (sentido positivo) o no ser objeto de lesiones (sentido negativo) que se adscriba a un sujeto por una norma jurídica positiva, y por *status* debe ser entendida la condición de sujeto de derecho prevista por una norma jurídica positiva, de modo que esta condición haga de la persona un sujeto idóneo para ser titular de situaciones jurídica o autor de los actos que son ejercicio de estas (2016, p. 37).

Para Castillo Córdova, los derechos humanos o fundamentales son todos los bienes humanos debidos a la persona humana por hecho de ser persona humana, y cuyo goce y disfrute le permite lograr su pleno desarrollo (2020, p. 105).

Por su parte, Gregorio Peces-Barba Martínez comprende a los derechos fundamentales a partir de un concepto compuesto por tres ámbitos integrados: los derechos son pretensiones morales justificadas éticamente, que están incorporadas al ordenamiento jurídico (requieren su reconocimiento como tales por el derecho positivo) y que cuya eficacia –cumplimiento en la realidad– debe ser posible (1995, pp. 101-112).

En lo que corresponde a Landa Arroyo (2019b), desde su posición institucional, los derechos fundamentales son derechos subjetivos ciertamente pero que tienen un doble carácter o dimensión. Por un lado, su consideración subjetiva de facultades que se reconocen a las personas, pero también tienen una dimensión institucional, en tanto los derechos son valores objetivos del ordenamiento jurídico. A partir de esta segunda dimensión, el Estado asume una serie de obligaciones, tales como proporcionar protección legal, judicial y administrativa (que se deriva del artículo 44 de la Constitución Política del Perú), la que se extiende a los propios particulares (a partir del deber de defender la Constitución que establece su artículo 38) (Landa Arroyo, 2019b, p. 140).

En la posición de Ferrajoli advertimos una suerte de dependencia del concepto 'derecho fundamental' a su reconocimiento por parte del derecho positivo, esto es, que debe existir una norma (dada por el ser humano) para reconocer algo como un derecho fundamental (con independencia de su fundamentación). Con esta orientación, una posición más extrema es la que desarrolla Giorgio Pino, para quien un derecho fundamental es un derecho subjetivo que viene reconocido por una norma que, dentro de la estructura del ordenamiento, es considerada de rango fundamental (2018, pp. 170-

171). En tanto que la postura de Luis Castillo Córdova (2020) se centra más en una aproximación filosófica de tipo circular, para quien, el derecho fundamental lo es porque le pertenece a la persona, con lo cual, en cierta forma, el concepto se funde con la fundamentación que el propio autor ofrece sobre los derechos (para quien son bienes humanos de la persona, y los derechos son tales por ser de la persona).

Por otro lado, la postura de Peces-Barba Martínez (1995) incorpora el fundamento en el concepto de los derechos y además la integra con la eficacia, lo cual consideramos puede generar confusiones, dado que, desde una perspectiva académica, lo más apropiado es distinguir y diferenciar las distintas dimensiones, porque cada una de ellas presenta aproximaciones propias y genera distintos problemas. En relación con lo primero, en el presente trabajo se han presentado distintas perspectivas teóricas sobre el fundamento de los derechos fundamentales y, como se ha podido apreciar, cada una parte de presupuestos distintos. En cuanto a lo segundo, el problema del fundamento tiene consecuencias prácticas que son distintas a su reconocimiento por el derecho positivo, en la medida que en función al fundamento, los derechos pueden ser aplicados de forma distinta, por ejemplo, los derechos de fundamentación liberal presuponen que el Estado asume deberes de abstención o no lesión (no privación arbitraria de la libertad, inviolabilidad de la propiedad y de los contratos, etc.), en tanto que los derechos de fundamentación igualitaria proponen que el Estado tiene deberes positivos (de actuación) para satisfacerlos (empleo, salud, educación, pensiones, entre otros). Esto último, en el plano de la eficacia, puede conllevar problemas muy diferentes: ¿es necesario que el Estado intervenga en la economía? ¿se necesitan recursos públicos para satisfacer los derechos liberales?, etc. No obstante, cabe rescatar que, dentro del concepto de derecho fundamental de Peces-Barba Martínez, se requiere necesariamente de su reconocimiento por parte del ordenamiento jurídico (1995).

En lo que corresponde a la posición de César Landa Arroyo (2019b), en su aproximación se concibe a los derechos fundamentales como institutos que presentan un doble carácter, de derecho subjetivo y de principio, y que como tales vinculan al Estado y a los sujetos privados y, aunque no se mencione, en tanto derechos subjetivos reconocidos, deben estarlo en un instrumento normativo (derecho positivo) que les reconozca tal carácter (una Constitución desde luego).

Por lo que, siendo así, se advierte que esencial al concepto es el reconocimiento del derecho por parte del derecho positivo. Entonces, bastaría que se aprobaran disposiciones constitucionales o instrumentos internacionales que reconozcan como derechos fundamentales a ciertos objetos (en sentido amplio) vinculados con las nuevas tecnologías de la información y comunicación, como ha sucedido con los derechos a la protección de datos personales, al olvido digital o al acceso a internet.

No obstante, de acuerdo a la experiencia que se ha tenido en nuestro país, el reconocimiento de nuevos derechos se ha encaminado mediante la jurisprudencia antes que por cambios constitucionales. En dicho sentido, tenemos los derechos a la verdad, al *ne bis in ídem*, el plazo razonable y el agua potable, siendo este último además incorporado expresamente al texto constitucional mediante una reciente reforma el año 2018. En tanto que, vinculados con las nuevas tecnologías, se han incorporado los derechos a la protección de datos personales y el derecho al olvido digital.

En relación con el primero, el artículo 2.6 de la Constitución Política del Perú (1993) (en adelante, la Constitución) reconoce un derecho a la autodeterminación informativa, cuyo ámbito protegido jurisprudencialmente se reconoció a partir de su contenido subjetivo (Expediente 1797-2002-HD/TC, 2003, fundamento 3), pero el ámbito protegido del derecho a la protección de datos personales es más amplio, conforme puede verse de los distintos aspectos sustantivos (facultades subjetivas, principios objetivos) e institucionales (estructura administrativa de tutela, además de procedimientos administrativos y procesos judiciales) regulados en la Ley 29733, Ley de Protección de Datos Personales (2011).

El derecho al olvido digital se ha incorporado al ordenamiento peruano por la Autoridad Nacional de Protección de Datos Personales, mediante la Resolución Directoral 045-2015-JUS/DGPDP, del 30 de diciembre de 2015, confirmada por la Resolución Directoral 026-2016-JUS/DGPDP, del 11 de marzo de 2016. En esta oportunidad se han seguido los lineamientos del caso *Google Spain S.L. y Google Inc. c. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (Caso C-131/12, 2014) resuelto por el Tribunal de Justicia de la Unión Europea, pero aún no ha sido incorporado en la Constitución o en la legislación nacional. Sin perjuicio de ello, se señala que puede derivarse de la conjunción de los derechos de oposición y cancelación que, dicho sea de paso, están reconocidos en los artículos 20 y 22 de la Ley de Protección de Datos Personales (Ley 29733, 2011), aunque bajo la forma de un derecho a la supresión de datos personales (Landa 2019a, p. 153).

En atención a lo señalado, las nuevas tecnologías no tendrían mayor incidencia en el concepto de derecho fundamental. Su incidencia se presenta en su contenido, en lo que, a partir de su reconocimiento e incorporación al texto de la Constitución, ya sea por vía jurisprudencial o mediante reformas constitucionales, puede exigirse al sujeto obligado por el derecho.

C. En torno a quién es titular de los derechos fundamentales y sujeto obligado por ellos

Los distintos conceptos trascritos en la sección previa tienen como elemento común y central la consideración de los derechos como atributos de la persona, es decir, del ser humano (hombre, mujer, niño, niña, adolescente, adulto mayor), con lo que la cuestión vinculada con la irrupción de las nuevas tecnologías sobre este punto es si es posible hablar de derechos fundamentales en sujetos distintos al ser humano.

En línea de principio y al menos por ahora eso no sería posible, dado que todos los discursos en torno a los derechos humanos o fundamentales tienen como punto de partida que estos se dicen ser propios de los seres humanos (personas). No obstante, el debate no podría cerrarse, especialmente a propósito de los avances de la inteligencia artificial y la robótica. En dicho sentido, la pregunta que debemos abordar es qué es lo que nos hace realmente humanos: (i) un cuerpo físico, compuesto de órganos que funcionan entre sí como un sistema y que dentro del cuerpo existen diversos sistemas (circulatorio, respiratorio, digestivo, etc.), los cuales están debidamente coordinados y hacen posible el funcionamiento del cuerpo humano (del aspecto somático); (ii) la capacidad de sentir o tener emociones y reaccionar conforme a ellas en las situaciones cotidianas, incluso tomar decisiones basadas en ellas o ser sensibles y empáticos con nuestro entorno; o (iii) la capacidad de razonar: analizar datos y variables, desagregarlas, reordenarlas y sistematizarlas para con ello tomar decisiones de forma autónoma.

En fin, en mayor o menor medida, ciertos sistemas de inteligencia artificial emulan ello e incluso tienen la capacidad de aprender. No obstante, no son totalmente autónomos, hay un diseño y un diseñador detrás, pero con el tiempo estos sistemas irán alcanzando mayores niveles de autonomía. Como se ha indicado, la inteligencia artificial, que puede ser entendida como totalmente autónoma (fuerte) o medianamente autónoma (débil) (Susskind, 2020, pp. 305-318), hoy no puede reemplazar totalmente al ser humano y apunta hacia actividades colaborativas. Sin perjuicio de ello, no es menos cierto que esta tendrá algún impacto en el mercado profesional (Uscamayta, 2020).

Ahora bien, regresando al punto, la irrupción de esta nueva tecnología nos debe llevar a repensar el fundamento de la humanidad y de su privilegio para ser titular de derechos fundamentales protegidos con la fuerza institucionalizada que el Derecho representa, quizás no tanto para postular nuevos sujetos derechos (robots con inteligencia artificial capaces de aprender y tomar decisiones autónomas), pero sí para reafirmar la humanidad de los seres humanos.

Por el lado de los sujetos obligados, tenemos que el Estado debe propiciar un marco regulatorio que promueva el desarrollo de las nuevas tecnologías, respetando los derechos fundamentales de las personas y de las empresas que las desarrollan. Este deber de aplicar adecuadamente las nuevas tecnologías se deben a que le resulta beneficiosa para afianzar el desarrollo del gobierno digital y la prestación de servicios públicos (que de hecho ya aplican estas tecnologías, con mayor o menor éxito). Al respecto, desde las políticas públicas, el Decreto Legislativo 1412, publicado en el año 2018, que aprueba el Decreto Legislativo sobre Gobierno Digital y que, entre otras medidas, establece los lineamientos para que las distintas entidades del sector público puedan digitalizar toda su infraestructura de servicios públicos, reconoce el derecho a la identidad digital, establece la interoperabilidad entre las distintas dependencias y medidas para la seguridad, lo cual constituye indudablemente un paso adelante para institucionalizar el uso de las nuevas tecnologías en el sector público.

Por el lado de los actores privados, estos deberán respetar los derechos fundamentales que van surgiendo en el entorno digital, como lo son los datos personales, los que no deberán ser manipulados sin el consentimiento de sus titulares; o el acceso a internet sin discriminación y sin censura de los usuarios de la red (principio de neutralidad). Al respecto, resulta paradigmático que, en el entorno digital sobre las relaciones entre los proveedores y usuarios de los servicios y la regulación, se tengan dos grandes modelos regulatorios: (i) la autorregulación, propia de los Estados Unidos y sus grandes corporaciones tecnológicas, a partir del cual los derechos valen en tanto estén reconocidos y con los alcances que estipulan los contratos que los usuarios suscriben con los proveedores de los servicios tecnológicos; y (ii) la intervención regulatoria estatal de la Unión Europea que pone el acento en la protección de las personas y sus derechos en el entorno digital (Téllez Carvajal, 2020, p. 180). Debido a la importancia que tienen los derechos fundamentales, un modelo de autorregulación no

sería lo más apropiado para el desarrollo de las nuevas tecnologías en el Perú, con lo cual la clave está en encontrar el nivel adecuado de intervención regulatoria y, por supuesto, el diseño de mecanismos (administrativos y judiciales) que sean realmente efectivos para proteger los derechos de quienes emplean las nuevas tecnologías en los entornos digitales.

D. Sobre el contenido de los derechos fundamentales

El contenido de los derechos alude al objeto protegido por ellos y que conecta los valores, principios y bienes que protege la Constitución, así como sus límites (Expediente 1417-2005-PA/TC, 2005, fundamento 21). En términos prácticos, el contenido de un derecho fundamental es aquello que sus titulares pueden hacer o pueden exigir que otros –Estado o particulares– hagan en su favor. En la doctrina hay una gran discusión teórica en torno a cómo determinar el contenido de los derechos (Alexy, 2008; Castillo Córdova, 2020; Landa Arroyo, 2019b; Häberle, 1997). No se ingresará en dicho debate, de por sí muy amplio, solo se tendrá en cuenta que el contenido protegido de un derecho fundamental, con independencia de la metodología que se adopte, está constituido por aquello que el titular del derecho puede hacer o exigir. Como ha señalado Ferrajoli, esto pueden ser tanto expectativas positivas (prestaciones) como expectativas negativas (no lesión), que se incardinan en la dimensión subjetiva o individual de los derechos; y que también comprenden prestaciones estatales que tienen como destinatarios a todas las personas (dimensión institucional) (2016, p. 37).

Entonces, ingresando al ámbito de los derechos que surgen en el entorno digital, una vez reconocidos estos derechos, pasa a tener sentido discutir en torno a qué es lo que esos derechos protegen. Esto es, ¿qué es lo que sus titulares pueden exigir del Estado y de los particulares en sentido positivo y negativo?

Al respecto, si nos centramos en el derecho al internet, en principio, será exigible al Estado. En sintonía con lo indicado por el Consejo de Derechos Humanos (2016), se exige al Estado brindar, con el mayor grado de alcance posible, el acceso sin ningún tipo de discriminación ni restricciones al entorno digital; con el correspondiente acceso a todas las fuentes que existan en dicho ámbito. Eso presupone que desde el Estado se procure establecer, *per se* o con intermediación de agentes privados, la infraestructura tecnológica que lo haga posible. Otro contenido vendría dado por las prestaciones mínimas que se pueden exigir a partir del derecho una vez que ya se ejerce: (i) calidad (velocidad de carga y descarga de datos) y estabilidad de la conectividad; (ii) protección de la identidad y privacidad (derecho a anonimizarse en el entorno digital); y (iii) derecho a no ser privado de la conexión a internet de forma arbitraria.

En lo que respecta al derecho a la protección de datos personales, tenemos que legislativamente se ha reconocido los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) en la Ley de Protección de Datos Personales (Ley 29733, 2011) y se ha creado una institucionalidad para darle efectividad. A estos derechos debe agregarse, como un derecho autónomo, el derecho al olvido digital. Con relación a este, toda persona, en el entorno digital, tiene reconocido los derechos de acceder a los datos personales que obren en bases de datos digitalizados y virtualizados, sean públicos o privados, así como a rectificarlos (modificarlos), cancelarlos (suprimirlos) y oponerse al tratamiento indebido y el acceso no consentido de terceros a los datos personales. Así, el derecho al olvido garantizaría la cancelación de datos por parte de los motores de búsqueda que permitan preservar la intimidad o el honor de las personas frente a informaciones que, aunque puedan ser indexadas, pierden relevancia pública por el paso del tiempo. Cabe agregar que en el ámbito europeo se ha incorporado este derecho al olvido como parte del derecho a la protección de datos personales, mediante el artículo 17 del Reglamento General de Protección de Datos (Reglamento 2016/679, 2016).

E. En relación con los límites de los derechos fundamentales

El contenido del derecho también se encuentra integrado con sus límites, habida cuenta que ningún derecho fundamental es absoluto. Su tratamiento se hace a partir de aquellos que se han establecido de forma expresa en la Constitución, como aquellos que se derivan de forma implícita, como es el caso del derecho de libre tránsito (Expediente 5994-2005-PHC/TC, 2005, fundamento 7). Entre los primeros tenemos, por ejemplo, al artículo 59 de la Constitución (1993) que establece que la protección de la salud pública es un límite al ejercicio de la libertad de empresa. Los segundos, en cambio, se derivan de la conjunción de los distintos derechos en casos concretos, lo que lleva a realizar un examen de razonabilidad y proporcionalidad para resolver el conflicto (Bernal Pulido, 2007) o aparente conflicto (Castillo Córdova, 2020, pp. 329-358).

En ese sentido, en relación con el *big data*, los algoritmos y la inteligencia artificial se han ido presentando distintos problemas que plantean límites

a su uso por parte de las empresas proveedoras y de los usuarios, límites derivados de los derechos fundamentales, tanto los que van surgiendo en el entorno digital, como de otros que podemos calificar de clásicos (cuyo contenido se deriva del paradigma de la presencialidad).

Al respecto, por ejemplo, el uso del *big data* y de los algoritmos puede dar pie a la manipulación de las preferencias en el consumo de las personas, esto con el fin de optimizar los rendimientos de las empresas que proveen servicios digitales (como las redes sociales para el incremento de las ventas por publicidad) o la manipulación de las preferencias electorales de los usuarios (el caso *Cambridge Analytica* es un muy buen ejemplo de ello).

De igual manera, puede haber usos indebidos en cuanto al tratamiento de los datos personales por usos no autorizados, lo que resulta lesivo del consentimiento de su titular. Por ende, dicho tratamiento sería *per se* inconstitucional por lesionar el derecho a la protección de datos personales.

En el caso de la inteligencia artificial, un problema muy presente y que se discute a partir de algunas experiencias es el del llamado 'sesgo algorítmico'. Los sistemas de inteligencia artificial, tanto los programados enteramente, como aquellos diseñados para aprender, recogen sesgos de sus propios diseñadores. Esto se debe a que los sistemas de inteligencia artificial reflejan los valores y las preferencias de los humanos que estuvieron inmersos en su diseño y codificación, así como en la recolección de los datos que se emplean para entrenar a dicho sistema. Lo que puede ocasionar problemas de discriminación como lo demuestran algunas experiencias aplicadas a los sistemas judiciales para predecir condenas (prediciendo condenas más altas a personas de color en los Estados Unidos) (Morales Cáceres, 2019) y también el ámbito laboral (Toyama Miyagusuku & Rodríguez León, 2019, p. 259).

Por otro lado, un tema que no puede pasar desapercibido también es la incidencia que tiene el uso de la infraestructura tecnológica (*hardware*) en el medio ambiente. Si bien el internet es un espacio virtual, en términos técnicos, hay un lugar físico donde se almacenan los datos. Existe todo un rubro empresarial dedicado a prestar estos 'alojamientos' para los datos. Son los servicios de almacenamientos de datos que ofrecen el servicio en línea o 'en la nube', no obstante, todos los datos terminan almacenándose en servidores que físicamente están alojados en algún lugar. Las empresas que prestan estos servicios y los gigantes tecnológicos (como Facebook o Google) han comprado extensos terrenos en zonas alejadas de centros urbanos, incluso en lugares cercanos al polo norte, y toda esta infraestructura requiere de sistemas de enfriamiento para mantener estables las temperaturas para su adecuada operatividad durante las veinticuatro horas del día. Esto indudablemente tiene un impacto en los entornos, dado que el calor que se genera tiene una incidencia en el calentamiento local y global (causando descongelamiento o elevación de temperatura del suelo), así como en el uso de las fuentes de agua (que suelen utilizarse como fuente de energía de los sistemas de enfriamiento).

Por otro lado, también tenemos el tratamiento de los residuos que se derivan de los miles o millones de equipos de cómputo que son desechados diariamente, algunos de los que tienen componentes tóxicos (especialmente las baterías y cargadores). Toda esta 'basura tecnológica' va a algún lugar, con lo cual se hace necesario que se establezcan regulaciones para el adecuado tratamiento de estos residuos que pueden y, de hecho, tienen un impacto en el medio ambiente, y a la larga, en la salud pública.

En todo caso, estas situaciones conflictivas requieren de distintos tipos de intervención estatal (regulatoria o mediante decisiones judiciales), los cuales para ser aplicados deberán ser evaluados a la luz de los principios de razonabilidad y proporcionalidad.

IV. INCIDENCIA DE LAS NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN EN ALGUNOS DERECHOS FUNDAMENTALES ESPECÍFICOS

En esta sección, se abordará la incidencia de las nuevas tecnologías en algunos derechos específicos (tales como la libertad personal y la ciberseguridad; las libertades de expresión e información y las redes sociales; la privacidad y la construcción de perfiles de usuarios; y la protección de los datos personales y el *big data*). Si bien podrían tratarse otras problemáticas también (como la educación virtual, el trabajo remoto y la aplicación de estas tecnologías a la justicia), las mismas no pueden ser abordadas por ahora debido a la extensión que debe cumplir el presente trabajo.

A. Libertad personal y ciberseguridad

¿Alguna vez advirtió en el espacio público, tales como veredas y carreteras, que hay cámaras de videovigilancia? ¿Ha leído u oído de la ciberseguridad? ¿Quién no se ha sentido alguna vez observado al conectarse a un ordenador con la cámara encendida? ¿Alguna vez quiso acceder a una página web y al intentarlo el ordenador indicó que no

se podía acceder por cuestiones de seguridad? A lo largo de la vida, al menos una vez se va a enfrentar con alguna de estas circunstancias. Es por ello que, este apartado se enfocará en evidenciar la relación entre la ciberseguridad y el derecho fundamental a la libertad personal.

La ciberseguridad puede ser entendida como todo el conjunto de herramientas, políticas, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas destinadas a proteger la información de las organizaciones y de los usuarios en el entorno digital (Unión Internacional de Telecomunicaciones, 2010, p. 20). En el mismo sentido, según Aldo Valdez Alvarado, la ciberseguridad debe ser entendida como un proceso, el cual implica prevención, detección y respuesta ante una situación simple o compleja (2019, p. 13). Entonces, podemos afirmar que la ciberseguridad es un proceso, el cual alberga un conjunto de actos destinados a proteger, detectar amenazas y responder ante estas, con el objetivo de proteger los activos de una empresa privada o pública, o institución estatal.

Por ello, la ciberseguridad es una innovación en el mundo de las nuevas tecnologías, ya que no solo es apreciado como un acto de prevención o de solución, aislado de todo un conjunto, sino como un conjunto de actos interrelacionados. Como proceso, la ciberseguridad se desarrolla en diferentes etapas: (i) prevención; (ii) detección; (iii) respuesta; y (iv) inteligencia. La prevención implica un control de accesos, prevención de fuga de datos y seguridad de la red. Por su parte, la detección conlleva la gestión de vulnerabilidades y monitorización continua. Luego, la respuesta funciona mediante sistemas de recuperación, en caso exista alguna fuga de datos, así como contramedidas, para evitar que estas vulnerabilidades no generen un impacto mayor. Finalmente, la fase de inteligencia implica funciones adicionales y externas, tales como compartir información y datos (Sáinz Peña, 2016, p. 20).

En lo que corresponde al derecho a la libertad personal, la Constitución lo reconoce en su artículo 2.24, siendo un ámbito concreto del mismo la prohibición de las detenciones arbitrarias (1993). Esto significa que la Constitución admite formas de restricción de la libertad de las personas. En dicho sentido, se establece que solo se puede detener a una persona en flagrancia o por mandato de un juez (1993, art 2.24 inciso f). Por otro lado, el Código Penal (1991) establece que cuando un juez penal emite una sentencia condenatoria, se tiene como consecuencia una privación de la libertad. De igual forma, la detención judicial preventiva, regulada por los artículos 268, 269 y 270 del Código Procesal Penal (2004), se constituye en una forma legítima de restringir este derecho, salvo que no se cumplan con las exigencias constitucionales y legales para ello, como la debida motivación de la resolución judicial que la dispone.

La relación que se presenta entre la ciberseguridad y la libertad personal, por un lado, se advierte por los programas de vigilancia, monitoreo o control de las personas que usan los Estados y las corporaciones (empleando programas de reconocimiento facial, por ejemplo). No obstante, también se evidencia por el lado de las pruebas que se pueden obtener, respecto de la comisión o presunta comisión de un delito, y las restricciones que puedan imponerse a la libertad personal del sujeto involucrado en los hechos.

Al respecto, las empresas y el Estado invierten en sistemas de ciberseguridad para evitar ataques a su infraestructura digital o hurto de información por parte de piratas informáticos *(hackers*), por lo que estos sistemas se constituyen en herramientas valiosas para la propia integridad y seguridad de la información empresarial, y de aquella que se genera al interior del Estado. Asimismo, sirve para la identificación de los autores de los ataques y, así, justificar medidas de restricción de la libertad personal sobre ellos, como la prisión preventiva, ya que los reportes o informes de ciberseguridad son los medios de prueba que permitirían a los jueces penales sustentar el grado de vinculación entre el sujeto investigado y los hechos que constituirían el delito.

Entonces, la ciberseguridad es un conjunto de herramientas orientadas a un proceso, más que a un solo acto, el cual está compuesto por acciones de prevención, detección, respuesta e inteligencia. Dichas acciones tienen la finalidad de asegurar los activos de una entidad pública o privada, y así evitar posibles afectaciones a esta. Asimismo, la relación entre el uso de la ciberseguridad y el derecho a la libertad personal puede ser considerado como no notoria, sino como un efecto del uso de la primera. Del mismo modo, coincidimos que el uso de la ciberseguridad puede generar efectos positivos para dichas entidades, y para el Estado, pues optimiza sus funciones, resguardando la integridad de la información que generan, reciben y gestionan.

B. Libertades de expresión e información y redes sociales

Las libertades de expresión e información protegen el discurso de las personas basadas en juicios de valor (opiniones) o en la transmisión de infor-

mación veraz. Siendo así, sus límites están dados por el respeto de la dignidad y el principio de veracidad, puesto que no está protegido por las libertades citadas un discurso que tenga como objetivo denigrar a otras personas o grupos de personas (como sucede con la injuria, la calumnia o el discurso de odio) o la transmisión de informaciones cuyo contenido sea falso (noticias falsas) (Landa Arroyo, 2017, pp. 56-57 & 63).

En líneas generales, esta es la comprensión estándar sobre las libertades de expresión e información que toma en consideración derechos y principios muy valiosos para el ejercicio de la ciudadanía dentro del sistema democrático.

En un sentido positivo, las redes sociales representan para las libertades referidas un escenario que optimiza su ejercicio. Hoy son millones los usuarios de las redes sociales (especialmente Facebook, Twitter, WhatsApp, etc.), que se comunican e interactúan compartiendo contenidos y expresando su parecer sobre cualquier tema que resulte de su interés. Asimismo, el internet, en general, se convierte en un gran repositorio de información de toda índole y en cualquier formato (escrito, auditivo [*podcast*], visual [infografías y mapas conceptuales] y audiovisual), lo que potencia, por ejemplo, el ejercicio del derecho a la educación y la investigación científica.

Sin embargo, estos estándares jurídicos en el escenario digital también presentan, entre otros muchos, dos desafíos debido a la irrupción de las redes sociales: el discurso de odio (*hate speech*) y las notificas falsas (*fake news*). Esto debido al potencial de personas que pueden ser receptores de mensajes con contenido lesivo de la dignidad de las personas o de los grupos sociales vulnerables, o de las noticias falsas. Ambas problemáticas tienen sus propias complejidades. Si nos referimos específicamente al discurso de odio, algunos proponen una suerte de control sobre el contenido del discurso, lo que trae reminiscencias de la censura previa que está prohibida por la Constitución y la Convención Americana sobre Derechos Humanos; por otro lado, otros proponen intervenciones pragmáticas (no dogmáticas), argumentativas (y no generalistas), haciendo uso de la ponderación para evaluar su prohibición o permisión (Marciani Burgos, 2017, pp. 295-301).

No obstante, dado que el internet y, por extensión, las redes sociales funcionan en un espacio en donde la presencia regulatoria del Estado es mínima (al menos en Latinoamérica), así como la presencia de la autorregulación contractual y la asunción unilateral del control sobre el contenido por parte de los proveedores del modelo, tenemos que Facebook, el mayor proveedor de redes sociales del mundo con más de dos mil cuatrocientos millones de usuarios activos (Fernández, 2020), por ejemplo, tiene treinta y cinco mil trabajadores dedicados exclusivamente a revisar el contenido de las publicaciones y de efectuar un control ex post de las mismas, siendo que, por citar un ejemplo, entre enero y marzo de 2020 se borraron nueve millones y medio de mensajes de odio (DW Español, 2020, min. 10:25 & 10:35).

Por otro lado, en relación con las noticias falsas, los procesos electorales en los Estados Unidos y en muchos de los países latinoamericanos, incluyendo el Perú, demuestran la vulnerabilidad de opinión pública y las simpatías electorales ante la difusión masiva de noticias falsas, ya sea que tengan por objetivo mellar la credibilidad o imagen de un candidato opositor, como la de fortalecer la posición del candidato que está detrás de su difusión. Esto depende, en buena cuenta, del aparato (tecnológico y personal) que tenga quien dirige el ataque al opositor o busca ganarse simpatía de los electores.

Al respecto, podemos hacer referencia al caso *Cambrigde Analytica*, compañía británica que se dedicaba a la minería y el análisis de datos masivos. Utilizando los datos proporcionados (vendidos) por Facebook, Cambrigde Analytica elaboró perfiles de usuarios de dicha red social en función de sus propias preferencias, las cuales se obtenían a través de las reacciones que realizaban en las distintas publicaciones: me gusta, me importa, me enoja, me divierte, me entristece (BBC News Mundo, 2018). Con estos perfiles, la compañía pudo seleccionar, en función de sus simpatías o antipatías, miedos y fortalezas, el tipo de información a enviarles para favorecer la candidatura republicana de Donald Trump o para desacreditar a su opositora demócrata Hillary Clinton, durante el proceso electoral estadounidense de 2016.

Estas situaciones ponen en evidencia que el avance de la tecnología en las redes sociales y el acceso ilimitado a fuentes de información puede potenciar el ejercicio de los derechos de libertad de expresión e información, como también puede llevar a la censura del discurso y la manipulación de las preferencias electorales, lo cual indudablemente tienen una incidencia institucional muy peligrosa en el funcionamiento del propio sistema democrático.

C. Derecho a la privacidad y perfiles de usuarios

En la actualidad, especialmente los más jóvenes, son usuarios de redes sociales, por lo que se crean

cuentas o perfiles en Facebook o Instagram. De igual forma, al postular a un empleo, suele ser habitual que los cazadores de talento soliciten el perfil del candidato o candidata de LinkedIn. Todo esto evidencia que nuestra cultura social está migrando a espacios virtuales como las redes sociales. Siendo ello así, los perfiles de los usuarios, al tener diversos grados de visibilidad, se convierten en una fuente de información sobre la persona, la que puede ser utilizada para los más diversos fines (con fines lícitos e ilícitos). De este modo, en algunas ocasiones, los perfiles de usuario pueden resultar invasivos y afectar los derechos fundamentales a la privacidad e intimidad.

Los perfiles de usuarios se sostienen en la construcción de perfiles de una persona basados en un grupo de usuarios objetivo, es decir, se construye un perfil para intentar cubrir las necesidades de un grupo reducido. Por ejemplo, cuando se quiere ubicar a un grupo de usuarios que cuentan con una condición socioeconómica determinada, se usa los perfiles de usuario, ya que estos agruparán a ese grupo determinado de usuarios, según las características que se requiera.

Por ello, se señala que estos son el conjunto de características y rasgos presentes en un usuario en particular, derivados de los datos que él mismo haya ofrecido al momento de crear o construir su perfil; aunque, también se construye a partir de su experiencia virtual, con las 'reacciones' que hoy ofrece Facebook. De igual modo, la autora Darinka Martínez Jané indica que existen diversos tipos de perfiles de usuario: (i) los que se crean para planear servicios o sistemas de información, a través de la bibliotecología; (ii) los perfiles de usuario de Windows que se elaboran con el objetivo de crear cuentas de usuario del dominio; y (iii) los que se crean para interactuar en las redes sociales (Facebook, Instagram, Twitter, entre otros) (2014, p. 26).

Entonces, podemos indicar que los perfiles de usuario son aquellas acciones que realizan las empresas con el fin de determinar grupos objetivos de personas que presenten características y rasgos determinados, los cuales son extraídos de la información o comportamientos que realicen los usuarios. Un ejemplo se presenta cuando un usuario elabora su perfil de LinkedIn y coloca la experiencia laboral con la que cuenta, las características que los diferencia, sus objetivos, entre otros datos. De ahí que, un empleador que requiera de un trabajador que cuente con experiencia previa en el sector de la construcción, a través de los perfiles de usuario de la citada red social, determinará qué grupo de todos los postulantes al puesto cuenta con ese requisito en particular, así como si cumplen todas las características que se buscan para el puesto.

De otro lado, el derecho fundamental a la privacidad, reconocido en el artículo 2.7 de la Constitución (1993), protege aquella información o acción de la vida privada de cada persona, y que no desea ver expuesta a terceros (Sanz Salguero, 2018, p. 136).

De ahí que este derecho cuente con diferentes esferas de protección: la esfera pública, la esfera privada, y la esfera íntima. La primera está compuesta por la información que cada persona desea compartir con el mundo exterior, puesto que es información de conocimiento público y no importante. La esfera privada se delimita a partir de aquella información que la persona desea no compartir con el mundo exterior, por lo que su divulgación será ilegítima y constituirá una vulneración a su privacidad. Esta esfera también está compuesta por información relativa a la vida privada, hábitos, actos y relaciones de la persona. Finalmente, para comprender la esfera íntima debe tenerse presente que 'lo íntimo' es todo aquello que vive muy dentro de cada persona y lo que cada quien desea guardar para sí mismo. Por ende, la esfera íntima puede estar compuesta por datos referidos a la identidad de cada persona, así como sus gustos, orientación sexual, historial médico, datos familiares y, sobre todo, todo aquello que pueda ser considerado como datos sensibles (Sanz Salguero, 2018, pp. 137-140).

Entonces, un cazador de talentos solo podría solicitar a los postulantes información vinculada con su esfera pública, mas no su información de carácter privado o íntimo, menos aún aquella que pueda considerarse sensible. Con lo cual, si el empleador busca información privada o íntima a través de una exploración de las redes sociales o los perfiles que tiene el postulante para determinar quién es apto o no, estaría lesionando el derecho a la privacidad e intimidad de los postulantes, incluso podría incurrir en actos discriminatorios, en tanto la información privada o íntima generalmente no guarda ningún tipo de relación con el tipo de actividad laboral que se va a desempeñar; salvo que esa relación exista razonablemente (por ejemplo para desempeñar labores físicas en condiciones ambientales hostiles, será necesario contar con un perfil médico del postulante a fin de no comprometer su salud, integridad o su propia vida).

A partir de lo señalado, se puede advertir que los perfiles de usuario representan una utilidad para la sociedad, especialmente cuando se trata de información hecha pública por el propio usuario, pero no si se trata de información privada o sensible.

D. Derecho a la protección de datos personales y *big data*

El uso que se le da al *big data* y a los algoritmos, en el ámbito público y privado, tiene por finalidad optimizar los servicios que se brindan a las personas, tanto al Estado como a las corporaciones privadas. No obstante, para funcionar, requieren de ingentes cantidades de datos, entre ellos los datos personales de los propios usuarios que son puestos a su disposición por los Estados y las empresas.

Los datos personales son unidades de información que permiten identificar a una persona. Se componen del nombre, apellidos, edad, número de documento de identidad, número de seguro social, la dirección, la dirección de correo electrónico, el número de celular, fecha de nacimiento, historial médico, perfiles de ADN, entre otros que permitan identificar de manera unívoca a una persona (Maqueo Ramírez *et al.*, 2017, p. 8; Ministerio de Justicia y Derechos Humanos, 2013, p. 4).

En este ámbito, suele confundirse a los datos personales con los datos sensibles, estos últimos se diferencian de los datos personales, puesto que estos cuentan con una relación de género-especie, es decir, que uno está incluido dentro del otro, en este caso, los datos sensibles forman parte de los datos personales. Entre estos tenemos a los perfiles biométricos, así como por los perfiles de ADN (Maqueo Ramírez *et al.*, 2017, p. 4). El Ministerio de Justicia y Derechos Humanos, por su parte, indica que los datos sensibles están compuestos, además de los ya mencionados, por los ingresos económicos, las creencias religiosas e ideologías políticas, así como por información relacionada a la vida sexual o a la salud de las personas (2013, p. 4).

Entonces, entendemos que los datos sensibles forman parte de los datos personales. Esta distinción será importante al momento de abordar la posible vulneración que se realiza a los derechos fundamentales por el uso de *big data* y algoritmos. Antes de abordar dicha problemática, es importante desarrollar a qué se refieren las empresas o instituciones estatales al mencionar el tratamiento de datos personales. Tal como su nombre lo evidencia, el tratamiento de datos personales es aquella acción mediante la cual un ordenador o una persona utiliza los datos personales de las personas con una finalidad. Para ello, llevan a cabo una serie de acciones tales como recopilación, registro, organización, almacenamiento, conservación, extracción, consulta, entre otros actos que faciliten el acceso, correlación o interconexión de datos personales (Ley 29733, 2011, art. 2.17).

Ahora debe precisarse que hay datos personales que son de libre acceso para el público en general, puesto que, son datos que no comprometen o no son considerados como privados y mucho menos como íntimos. En dicho sentido, cuando se navega por internet o por alguna red social, se puede escribir algún nombre o razón social en el buscador, e inmediatamente aparecerán varios resultados, acordes a los criterios de búsqueda. Así, uno puede encontrarse el perfil de una persona o de una empresa, a partir del uso de sus datos personales, pero que son de uso público.

La zona de confluencia entre el *big data* (grandes cantidades de datos, incluyendo personales y sensibles), los algoritmos (programas o sistemas para efectuar el tratamiento de esos datos masivos) y los datos personales viene dado por que estos últimos son la materia prima para el desempeño de las funcionalidades de los dos primeros. Siendo ello así, esta convergencia debe estar debidamente regulada a fin de evitar intromisiones o tratamientos no consentidos de los datos que los propios usuarios proporcionan al Estado y a las empresas que ofrecen servicios digitales, y que requieren del usuario sus datos personales.

En dicho sentido, podrían darse situaciones de lesión de los datos personales cuando empresas ofrecen servicios no solicitados a los usuarios, siendo que para determinar o focalizar la oferta se han empleado datos proporcionados por las personas, aunque para fines distintos en los que son empleados. Esto suele ser una práctica habitual con los usuarios de los servicios financieros o las administradoras de fondos de pensiones, de quienes se recopilan su información económica y financiera sensible, para luego remitirles publicidad a sus correos electrónicos sobre toda una gama de servicios que se estructuran sobre la base de sus perfiles de usuarios o información personal. Siendo que, en muchos casos, estos usos de la información brindada (datos personales) no ha sido autorizado.

V. NUEVAS TECNOLOGÍAS Y DERECHOS FUNDAMENTALES: ¿NUEVOS DERECHOS O CONTENIDOS NUEVOS DE DERECHOS YA RECONOCIDOS?

La discusión en torno al surgimiento de nuevos derechos es de larga data, especialmente en la filosofía del derecho debido a los límites de la intervención judicial en la creación o incorporación de nuevos derechos fundamentales (Guastini, 2018, pp. 101-106; Rüthers, 2020; Wambier, 2016, pp. 301-376).

No obstante, dejando de lado todo este debate, lo cierto es que la irrupción de las nuevas tecnolo-

gías, debido al tratamiento masivo de datos en el entorno virtual, debe motivar la reflexión sobre si estamos frente a nuevos derechos que necesitan ser reconocidos por el derecho positivo, especialmente a nivel constitucional, o si en realidad se trata de contenidos nuevos de derechos que ya se encuentran reconocidos por la Constitución.

Un buen ejemplo de ello viene dado por la consideración del internet, en tanto objeto jurídicamente protegido, como derecho fundamental. En dicho sentido, como ya se dijo en este trabajo, desde Naciones Unidas se postula la consideración del acceso al internet como un derecho humano, pero que se basa en el ejercicio cada vez más intenso de las libertades de expresión e información en el entorno digital. Aunque el documento del Consejo de Derechos Humanos de las Naciones Unidas no lo menciona, en estricto, según se desprende de su contenido, el mismo se sustentaría en los derechos de libertad de expresión e información, porque se sostiene que "[…] los derechos de las personas también deben estar protegidos en Internet, en particular la libertad de expresión, que es aplicable sin consideración de fronteras y por cualquier procedimiento que se elija" (2016, numeral 1), en tanto que se reconoce su naturaleza mundial y abierta como instrumento para el desarrollo (2016, numeral 2); a la vez que se motiva la aplicación de un "[…] enfoque basado en los derechos humanos para facilitar y ampliar el acceso a Internet y [se] solicita a todos los Estados que hagan lo posible por cerrar las múltiples formas de la brecha digital" (2016, numeral 5).

Por otro lado, en nuestro medio, se ha postulado un derecho al internet que, si bien sustentado en los derechos antes indicados, no se limita solo al acceso, vinculado con el acceso a la infraestructura que lo hace posible, sino que también abarca otros contenidos, como la libertad de uso de internet, la seguridad en internet, la protección de la privacidad, el derecho al uso de seudónimo, olvido digital, control de la vigilancia electrónica (Landa Arroyo, 2019a, pp. 147-156).

Otro derecho sobre el que se discute si se trata de un nuevo derecho o es un derecho que se desprende de otros ya reconocidos es el derecho al olvido digital. Al respecto Mieres Mieres (2014, p. 12) señala que hay tres estrategias argumentativas para sustentar este derecho: (i) entender que es un derecho autónomo; (ii) que es una proyección del derecho a la intimidad; y (iii) que es un derecho que deriva del derecho a la protección de datos personales. Lo cierto es que, considerar las alternativas (ii) y (iii) lleva a negarle funcionalidad. Por lo que, lo más adecuado resulta comprender que es un derecho autónomo que, al menos por el momento, es oponible a los motores de búsqueda que busca impedirles que, a partir de datos personales (generalmente los nombres y apellidos u otros datos de identidad), listen (indexen) información (buena o mala) sobre cualquier persona, a partir de datos e informaciones que previamente existen en otras fuentes (páginas webs, bases de datos públicas o privadas, redes sociales), ya que lo que el motor de búsqueda hace es facilitar el acceso a esas fuentes para quien realiza la búsqueda. Este derecho, desde luego, no podría conllevar que se anule, desparezca o borre la información previamente alojada en una fuente legítima (Díaz Colchado, 2019, pp. 38-39).

Por otro lado, el cambio de paradigma en el mundo del trabajo, acelerado por la pandemia del COVID-19, ha llevado del trabajo presencial al trabajo remoto, que requiere el uso intensivo de la tecnología (equipos de cómputo, *software*, conexión a internet, aplicativos, etc.) para que los trabajadores (especialmente los que tienen trabajo de oficina) puedan desarrollar sus labores desde casa, en lugar de concurrir a un centro de trabajo. No obstante, según los reportes y estudios realizados, el trabajo remoto desborda la propia capacidad de la persona, debido a que las fronteras entre las horas de trabajo y las horas de descanso se vuelven borrosas, debido a las exigencias empresariales de que el trabajador esté a disposición o conectado durante la mayor parte del día, lo que se ha vuelto más estresante si consideramos que un equipo de telefonía móvil o una *tablet* reemplazan perfectamente a un equipo de cómputo personal (*laptop*).

Por ello, antes del inicio de la pandemia, se discutía la incorporación en las legislaciones de un derecho a la desconexión digital (Serrano Argüeso, 2019, pp. 187-188), siendo que en España ya se había avanzado desde el año 2018 (Figueroa Gutarra, 2020, p. 230), como una derivación del derecho al descanso, que la Constitución Política del Perú (1993) reconoce como uno de los derechos laborales fundamentales en su artículo 25, aunque con alcances un tanto distintos. El derecho a la desconexión digital presuponía la clara división entre las horas de trabajo presencial (jornada de trabajo), y las horas dedicadas a la vida personal y familiar. En este escenario, debido al avance tecnológico en el ámbito del trabajo, el trabajador era requerido para atender correos electrónicos, llamadas o comunicaciones por redes sociales por parte de su empleador (o jefe inmediato) fuera de las horas que integran la jornada laboral (sábados y domingos o en horas de la noche o madrugada de un día laborable). De ahí que, se postulara un derecho del trabajador para hacer efectivo su descanso, permitiéndole desconectarse digitalmente

de todos los medios por los cuáles el empleador pudiera requerirle que siga prestando su fuerza de trabajo (físico o intelectual).

No obstante, con la pandemia y el confinamiento en el hogar, la distinción entre el horario de trabajo y el horario personal del trabajador se volvió todavía más difusa (Díaz Colchado, 2020, pp. 41- 42), cuando no estresante y un riesgo para la salud emocional de las personas (Vite Vigo, 2020), lo que llevó a que el gobierno incorporara este derecho a través del Decreto de Urgencia 127-2020, publicado el 1 de noviembre de 2020, y que modificó, entre otros, el artículo 18 del Decreto de Urgencia 026-2020, publicado el 15 de marzo de 2020, que regula el trabajo remoto. Lo destacable de estas innovaciones normativas fue que se estableció la obligación del empleador público o privado para que respetara el derecho del trabajador a la desconexión digital, el que consiste en "[…] desconectarse de los medios informáticos, de telecomunicaciones y análogos utilizados para la prestación de servicios durante los días de descanso, licencias y períodos de suspensión de la relación laboral" (Decreto de Urgencia 127-2020, 2020, art. 18.1.4), por lo que "el empleador no puede exigir al trabajador la realización de tareas o coordinaciones de carácter laboral durante el tiempo de desconexión digital" (Decreto de Urgencia 127-2020, 2020, art. 18.1.5).

Como puede advertirse, en materia de nuevos derechos, la irrupción de las nuevas tecnologías representa un desafío para la teoría de los derechos fundamentales y abre el debate en torno a la incorporación de nuevos derechos en el derecho positivo (constitucional o legal), debates que seguirán abiertos en los próximos años, en la medida que esta irrupción está tornándose más intensa con el avance de los desarrollos tecnológicos y la penetración, aunque lenta, pero progresiva de la infraestructura tecnológica que hace posible el acceso a internet en nuestro país.

VI. CONCLUSIONES

En el presente artículo se ha analizado la incidencia de las nuevas tecnologías de la información y comunicación en la teoría de los derechos fundamentales, en algunos derechos y, finalmente, en los nuevos derechos, con la finalidad de comprender el impacto que ha generado la irrupción de las nuevas tecnologías en los derechos fundamentales de las personas.

En primer lugar, en cuanto a lo referente a la incidencia que han generado las nuevas tecnologías en la teoría general de los derechos fundamentales, podemos indicar que múltiples derechos fundamentales se han visto afectados, en algunos de manera justificada, no obstante, en otros, injustificada. En un ámbito jurídico, en algunos casos se precisa que estas intervenciones vendrían a ser constitucionales; mientras que en otros casos (tales como la videovigilancia permanente, perfiles de usuarios con datos sensibles y demás), vendrían a ser inconstitucionales.

En segundo lugar, las nuevas tecnologías han generado un impacto en diversos derechos fundamentales tales como la libertad personal, las libertades de expresión e información, la privacidad, entre otros. Dicho impacto, en muchos casos, ha incrementado la eficiencia, sin menguar o afectar el contenido esencial de los derechos detallados en el presente artículo.

Finalmente, tras el análisis realizado se ha llegado a la conclusión de que las nuevas tecnologías y su desarrollo –en la actualidad– representan un desafío para la teoría de los derechos fundamentales, especialmente debido a que la tecnología se encuentra en constante avance, y muchas veces no se llega a considerar la posible afectación que pueden generar en los derechos fundamentales. Sin embargo, las nuevas tecnologías están innovando y revolucionando el mundo, optimizando procesos y generando eficiencia para la sociedad, es por ello que se considera que estas, con un adecuado marco normativo, pueden contribuir a la satisfacción y bienestar general de la población.

REFERENCIAS

Alexy, R. (2008). *Teoría de los derechos fundamentales* (C. Bernal Pulido, trad.). Centro de Estudios Políticos y Constitucionales.

Barrio Andrés, M. (2017). *Fundamentos del Derecho de Internet*. Centro de Estudios Políticos y Constitucionales.

BBC News Mundo (9 de abril de 2018). Cómo Cambridge Analytica analizó la personalidad de millones de usuarios de Facebook [video]. YouTube. https://www.youtube.com/watch?v=7831NGClsrM&ab_channel=BBCNewsMundo

Bernal Pulido, C. (2007). *El principio de proporcionalidad y los derechos fundamentales. El principio de proporcionalidad como criterio para determinar el contenido de los derechos fundamentales vinculante para el legislador*. Centro de Estudios Políticos y Constitucionales.

Cáceres, E. (2006). Inteligencia artificial, derecho y E-JUSTICE (El Proyecto IIJ-CONACYT). *Boletín*

Mexicano de Derecho Comparado, *39*(116), 593-611.

Campodónico, H. (30 de noviembre de 2019). El fracaso de la red dorsal de fibra óptica y la obsesión por las APP. *Otra Mirada*. http://www.otramirada.pe/el-fracaso-de-la-red-dorsal-de-fibra-%C3%B3ptica-y-la-obsesi%C3%B3n-por-las-app

Castillo Córdova, L. (2007). *Los derechos constitucionales. Elementos para una teoría general*. Palestra Editores.

(2020). *Derechos fundamentales y procesos constitucionales.* Zela Grupo Editorial.

Cotino Hueso, L. (2017). Big Data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales. *Dilemata*, *24*(9), 131-150.

De la Cuadra, E. (1996). Internet: Conceptos básicos. *Cuadernos de documentación multimedia*, (5), 35-56.

Díaz Colchado, J. C. (2019). Olvido digital vs. verdad: el impacto del derecho al olvido digital en la preservación en internet de la memoria histórica sobre violaciones a derechos humanos y actos de corrupción. *Pensamiento Constitucional*, *24* (24), 27-47.

(2020). La (des)protección de los derechos fundamentales laborales en tiempos de pandemia: constitucionalidad de las medidas gubernamentales en materia laboral adoptadas para enfrentar el COVID-19. En C. Landa Arroyo (coord.), *Constitución y emergencia sanitaria* (pp. 37-52). Palestra Editores.

Díaz Revorio, F. J. (2010). Tecnologías de la información y comunicación y nuevas dimensiones de los derechos fundamentales. *Pensamiento Constitucional, 14*(14), 33-67.

DW Español (13 de diciembre de 2020). Enlace - Discurso de odio [video]. YouTube. https://www.youtube.com/watch?v=w49kjgRuj7c&ab_channel=DWEspa%C3%B1ol

Fernández, R. (21 de marzo de 2020). Ranking mundial de redes sociales por número de usuarios en 2021. *Statista*. https://es.statista.com/estadisticas/600712/ranking-mundial-de-redes-sociales-por-numero-de-usuarios/

Ferrajoli, L. (2016). *Derechos y garantías. La Ley del más débil* (P. Andrés Ibáñez, trad.; 8va ed.). Trotta.

Figueroa Gutarra, E. (2020). El derecho a la desconexión digital. Entre el derecho al descanso y los deberes laborales. En C. Landa Arroyo (ed.), *Derechos fundamentales. Actas de la V Jornadas Nacional de Derechos Fundamentales* (pp. 228-245). Palestra Editores.

Guastini, R. (2018). *Ensayos escépticos sobre la interpretación* (C. Moreno More, trad.). Zela.

Häberle, P. (1997). *La libertad fundamental en el Estado constitucional* (C. Ramos, J. Saligmann & C. Landa Arroyo, trads.). Fondo Editorial de la PUCP.

Hernández-Leal, E. J., Duque-Méndez, N.D., & Moreno-Cavadid, J. (2017). Big Data: Una exploración de investigaciones, tecnologías y casos de aplicación. *TecnoLógicas*, *20*(39), 15-38. https://doi.org/10.22430/22565337.685

Joyanes Aguilar, L. (2008*). Fundamentos de programación: algoritmos, estructura de datos y objetos*. McGrawHill.

Landa Arroyo, C. (2000). Dignidad de la persona humana*. Ius et Veritas*, *10*(21), 10-25. https://doi.org/10.18800/ius.v10i21.15957

(2017). *Los derechos fundamentales*. Fondo Editorial de la Pontificia Universidad Católica del Perú.

(2019a). Contenido esencial del derecho fundamental a internet: teoría y praxis. En C. Landa (ed.), *Libro homenaje del Área de Derecho Constitucional por los 100 años de la Facultad de Derecho de la Pontificia Universidad Católica del Perú* (pp. 145-173). Centro de Investigación, Capacitación y Asesoría Jurídica (CICAJ).

(2019b). *Los derechos fundamentales en la jurisprudencia del Tribunal Constitucional 2008-2018*. Palestra Editores.

Maqueo Ramírez, M. S., Moreno González, J., & Recio Gallo, M. (2017). Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario. *Revista de derecho (Valdivia), 30*(1), 77-96. http://dx.doi.org/10.4067/S0718-09502017000100004.

Marciani Burgos, B. (2017). *Tolerancia y derechos. El lugar de la tolerancia en el Estado constitucional*. Atelier y Facultad de Derecho de la Pontificia Universidad Católica del Perú.

Martínez Bahena, G. C. (2012). La inteligencia artificial y su aplicación al campo del derecho. *Alegatos*, (82), 827-846.

Martínez Jané, D. (2014). Perfiles de usuario. Una alternativa para detectar líderes y potenciar una cultura organizacional fuerte. *Ciencias de la información, 45*(1), 25-29.

Mieres Mieres, L. J. (2014). *El derecho al olvido digital* (Documento de trabajo 186/2014). Fundación Alternativas. https://www.fundacionalternativas.org/public/storage/laboratorio_documentos_archivos/e0d97e985163d78a27d6d7c23366767a.pdf

Ministerio de Justicia y Derechos Humanos (2013). *El derecho fundamental a la protección de datos personales*. Ministerio de Justicia y Derechos Humanos.

Morales Cáceres, R. (7 de noviembre de 2019). El sesgo algorítmico y la protección de datos personales. *Enfoque Derecho*. https://www.enfoquederecho.com/2019/11/07/el-sesgo-algoritmico-y-la proteccion-de-datos-personales/

Nieva Fenoll, J. (2018). *Inteligencia artificial y proceso judicial*. Marcial Pons.

Oroño, R. D. (2007). Las nuevas tecnologías ¿avances o frustraciones? *Educación y futuro: revista de investigación aplicada y experiencias educativas*, (17), 233-261.

Peces-Barba Martínez, G. (1995). *Curso de derechos fundamentales. Teoría general*. Universidad Carlos III de Madrid. Boletín Oficial del Estado.

Pérez Luño, A. (2004). *Los derechos fundamentales*. Tecnos.

Pino, G. (2018). *El constitucionalismo de los derechos. Estructura y límites del constitucionalismo contemporáneo*. Zela.

Rüthers, B. (2020). *La revolución secreta. Del Estado de derecho al Estado judicial: Un ensayo sobre Constitución y método*. Marcial Pons.

Sáinz Peña, R. (2016). Ciberseguridad, la protección de la información en un mundo digital. *TELOS, Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad*.

Sanz Salguero, F. (2018). Delimitación de las esferas de la vida privada, privacidad e intimidad frente al ámbito de lo público. *Transparencia & Sociedad*, (6), 127-149.

Serrano Argüeso, M. (2019). "Always on". Propuestas para la efectividad del derecho a la desconexión digital en el marco de la economía 4.0. *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, *2*(7), 164-191.

Sosa Sacio, J. (2015). Crítica a la dignidad humana y la noción de "necesidades básicas" como un posible mejor fundamento para los derechos. *THĒMIS-Revista de Derecho*, (67), 87-99.

Susskind, R. (2020). *Tribunales online y la justicia del futuro*. Wolters Kluwer.

Téllez Carvajal, E. (2020). Análisis documental sobre el tema del Big Data y su impacto en los derechos humanos. *Revista Derecho PUCP*, (84), 155-206. https://doi.org/10.18800/derechopucp.202001.006

Toyama Miyagusuku, J., & Rodríguez León, A. (2019). Algoritmos laborales: *Big Data* e inteligencia artificial. *THĒMIS-Revista de Derecho*, (75), 255-266. https://doi.org/10.18800/derechopucp.202001.006

Unión Internacional de Telecomunicaciones (2010). Ciberseguridad. *Actualidades de la UIT*, (9).

Universidad de Chile (s.f). *Guía de uso Lexis Nexis*. https://www.uchile.cl/documentos/base-de-datos-lexis-nexis_51510_16_3817.pdf

Uscamayta, G. (24 de noviembre de 2020). ¿Inteligencia artificial y derecho? Una breve introducción sin mentiras ni exageraciones. *Legis.pe*. https://lpderecho.pe/inteligencia-artificial-y-derecho-breve-introduccion/#_ftnref7

Valdez Alvarado, A. (2019). *Introducción a la ciberseguridad*. Universidad Mayor de San Andrés.

Vite Vigo, V. (5 de noviembre de 2020). Trabajo remoto y salud mental: algunas reflexiones laborales a raíz del impacto de la COVID 19. *Enfoque Derecho*. https://www.enfoquederecho.com/2020/11/05/trabajo-remoto-y-salud-mental-algunas-reflexiones-laborales-a-raiz-del-impacto-de-la-COVID-19/

Wambier, T. A. A. (2016). ¿Deben los jueces crear derecho?. en M. Taruffo, L. Marinoni, & D. Mitidiero (coords.), *La misión de los tribunales supremos* (pp. 301-376). Marcial Pons.

Zamora Lucio, M. (2014). *Internet*. Universidad Autónoma del Estado de Hidalgo.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Caso C-131/12, Google Spain S.L. & Google Inc. c. Agencia Española de Protección de Datos (AEPD) & Costeja González, ECLI:EU:C:2014:317 (may. 13, 2014).

Código Penal [CP], Decreto Legislativo 635, Diario Oficial *El Peruano*, 8 de abril de 1991 (Perú).

Código Procesal Penal [NCPP], Decreto Legislativo 957, Diario Oficial *El Peruano*, 29 de julio de 2004 (Perú).

Consejo de Derechos Humanos, *Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo*, U.N. Doc. A/HRC/32/L.20 (27 de junio de 2016).

Constitución Política del Perú [Const.] (1993).

Decreto de Urgencia 127-2020, Decreto de Urgencia que establece el otorgamiento de subsidios para la recuperación del empleo formal en el sector privado y establece otras disposiciones, Diario Oficial *El Peruano*, 1 de noviembre de 2020 (Perú).

Decreto Legislativo 1412, Decreto Legislativo que aprueba la ley de gobierno digital, Diario Oficial *El Peruano*, 12 de septiembre de 2018 (Perú).

Ley 29733, Ley de Protección de Datos Personales, Diario Oficial *El Peruano*, 3 de julio de 2011 (Perú).

Ley 29904, Ley de Promoción de la Banda Ancha y construcción de la Red Dorsal Nacional de Fibra Óptica, Diario Oficial *El Peruano*, 20 de julio de 2012 (Perú).

Ministerio de Justicia y Derechos Humanos, 30 de diciembre de 2015, Resolución Directoral 045-2015-JUS/DGPDP, Expediente 012-215-PTT (Perú).

Ministerio de Justicia y Derechos Humanos, 11 de marzo de 2016, Resolución Directoral 026-2016-JUS/DGPDP, Expediente 012-2015-PTT (Perú).

Tribunal Constitucional [T.C.], 29 de enero de 2003, sentencia recaída en el Expediente 1797-2002-HD/TC (Perú).

Tribunal Constitucional [T.C.], 8 de julio de 2005, sentencia recaída en el Expediente 1417-2005-PA/TC (Perú).

Tribunal Constitucional [T.C.], 29 de agosto de 2005, sentencia recaída en el Expediente 5994-2005-PHC/TC (Perú).

#20 AÑOS CONTIGO

LIMA AIRPORT PARTNERS
EN EL JORGE CHÁVEZ

LAP
LIMA AIRPORT PARTNERS

DOS DÉCADAS SIENDO LA PUERTA DEL PERÚ AL MUNDO

+ US$ 576 millones
en inversiones directas al Estado peruano durante estos 20 años.

+ US$ 2,685 millones
en transferencias directas al Estado peruano durante estos 20 años.

90 mil empleos
generados por el Aeropuerto Internacional Jorge Chávez.

23 millones de pasajeros
durante el 2019 previo a la pandemia.

@aeropuertojorgechavez
@aeropuerto_jorgechavez
www.lima-airport.com

10.18800/themis.202101.002

CONSTITUCIÓN, DERECHOS FUNDAMENTALES, INTELIGENCIA ARTIFICIAL Y ALGORITMOS

CONSTITUTION, FUNDAMENTAL RIGHTS, ARTIFICIAL INTELLIGENCE AND ALGORITHMS

César Landa Arroyo*
Miembro del Consejo Consultivo de THĒMIS
Pontificia Universidad Católica del Perú
Universidad Nacional Mayor de San Marcos

Over the last few decades, the relationship of dependence between humans and technology has been progressive and plausible. This has meant a greater use –by the public and private sector– of technological tools such as artificial intelligence and, in particular, algorithms. These last ones enable the performance of everyday activities such as bank transfers and other more complex ones like the early detection of crimes. In this context, the discussion on whether technological criteria should be the only limits in the development of such advances is increasingly growing.

In this article, the author analyzes the influence of artificial intelligence and algorithms in various areas of society, emphasizing the risk that these can generate, in terms of fundamental rights, if its application is not limited by the respect of constitutional rights and principles. Additionally, the author evidences the obligation of the State, within the framework of a democratic and social government model, to regulate practices that, making use of technology, are potential instruments of risk to the rights of individuals.

Keywords: Constitution; fundamental rights, technology; artificial intelligence; algorithms.

Durante las últimas décadas, la relación de dependencia entre los seres humanos y la tecnología ha sido progresiva y plausible. Ello ha supuesto un mayor empleo –por parte del sector público y privado– de herramientas tecnológicas como la inteligencia artificial, y, en particular, los algoritmos. Estos últimos permiten la realización de actividades cotidianas como una transferencia bancaria y otras más complejas como la detección temprana de delitos. En este escenario, la discusión sobre si los criterios tecnológicos deben ser los únicos límites en el desarrollo de dichos avances toma mayor protagonismo.

En el presente artículo, el autor analiza la incidencia de la inteligencia artificial y los algoritmos en los diversos campos de la sociedad, con especial énfasis en el riesgo que estos generan en materia de derechos fundamentales, si es que su aplicación no tiene como límite el respeto por los derechos y principios constitucionales. En adición, se expone la obligación del Estado, en el marco de un modelo democrático y social, de regular las prácticas que, haciendo uso de la tecnología, son potenciales instrumentos de riesgo en los derechos de las personas.

Palabras clave: Constitución; derechos fundamentales; tecnología; inteligencia artificial; algoritmos.

* Abogado. Doctor en Derecho por la Universidad Alcalá de Henares (Madrid, España). Ex presidente del Tribunal Constitucional del Perú. Profesor de Derecho Constitucional en la Pontificia Universidad Católica del Perú (PUCP) y en la Universidad Nacional Mayor de San Marcos - UNMSM (Lima, Perú). Vicepresidente de la International Association of Constitutional Law. Código ORCID: 0000-0003-0801-8873. Contacto: clanda@pucp.edu.pe

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 9 de enero de 2021, y aceptado por el mismo el 28 de febrero de 2021.

A la Generación Bicentenario

I. INTRODUCCIÓN

A lo largo del año 2020, en el Perú y en el mundo se ha incrementado exponencialmente el uso del internet a raíz de la pandemia generada por el COVID-19, la cual ha forzado a millones de personas a realizar cuarentenas obligatorias o voluntarias en casa. En consecuencia, muchos han tenido que continuar su vida profesional, laboral, comercial, educativa, recreativa, y sanitaria, entre otras, desde computadoras, portátiles, tabletas y celulares que les permitan buscar, registrar, procesar, transmitir y recibir información.

Este proceso ha cambiado la relación de las personas con los equipos tecnológicos, a causa de la dependencia casi absoluta en estos, lo que ha generado un impacto en el mercado del internet. Esto último se debe, no solo al alza de la demanda de equipos, programas o conectividad, sino también, al desarrollo de aplicaciones basadas en la inteligencia artificial, cuyas funciones exceden las del rastreo digital de la pandemia. Frente a ello, se presenta el problema de que el suministro del servicio está concentrado en los grandes proveedores y plataformas digitales mundiales, quienes a su vez, poseen un activo patrimonial con un alto precio de mercado para las empresas y personas naturales: los datos personales (Navas *et al.*, 2017, pp. 289-290).

Ello es así en la medida que las personas, en sus relaciones con el Estado y el mercado, requieren registrar sus datos personales de forma electrónica o biométrica. Aquello ocurre cada vez que uno busca obtener un documento de identidad o un pasaporte, proceder a pagar impuestos, interponer una demanda judicial o cuando queda registrado al pasar por el control inteligente de los semáforos y de sus cámaras. Sin embargo, también al conducir (dirigidos, oralmente, por una aplicación de tráfico y navegación), realizar operaciones bancarias por internet o compras *online* (locales, nacionales o internacionales con entrega a domicilio), detectar y filtrar correos no deseados, solicitar un servicio de taxi, o rastrear mediante la geolocalización a las personas contactadas con un diagnóstico de COVID-19, entre otros.

Todo ello se basa, en particular, en el desarrollo de la inteligencia artificial, la cual permite que un algoritmo se exprese en un lenguaje de programación para así realizar actividades registradas y procesadas por máquinas inteligentes (computadoras). Es decir, una máquina reemplaza las funciones cognitivas de los funcionarios del Estado o los empleados de las empresas, maximizando sus objetivos y tareas. Así, en este proceso, las máquinas inteligentes sustituyen las capacidades humanas para percibir, razonar, decidir, aprender y resolver problemas, realizando una interpretación adecuada de los datos captados y procesados.

No obstante, la cuestión principal es si el proceso de recojo, procesamiento y resultado se debe ajustar únicamente a criterios tecnológicos, sin perjuicio del marco del derecho constitucional de las libertades y derechos fundamentales, así como también de los deberes; o si los derechos fundamentales constituyen el fundamento y el límite del desarrollo tecnológico de la inteligencia artificial y en particular, de los algoritmos.

Por ello, en un Estado democrático constitucional, el uso de los algoritmos, en el marco del desarrollo de la inteligencia artificial, nos lleva a preguntarnos: ¿Cuál es el estado actual del contenido constitucionalmente protegido de los derechos fundamentales, a través del diseño y uso del internet? (Landa, 2019). Para ello, analizaremos, primero, la relación de la Constitución con la inteligencia artificial y, segundo, la relación de los derechos fundamentales con los algoritmos; para finalmente concluir en un balance sobre la necesidad de su regulación para cautelar el contenido constitucionalmente protegido de los derechos fundamentales.

II. CONSTITUCIÓN E INTELIGENCIA ARTIFICIAL

La Constitución es la norma jurídica suprema del Estado democrático y social de Derecho. En el Perú, la Constitución Política de 1993 establece un orden público sobre la base del respeto de los derechos fundamentales y el establecimiento de límites al poder público y privado (arts. 2 y 45). En este sentido, el orden público constitucional reconoce la libertad de empresa (art. 59), la libertad de creación intelectual y el derecho a la propiedad sobre dichas creaciones (art. 2.8), al igual que la libertad de contratar (art. 2.14). Asimismo, también establece que la defensa de la persona humana y el respeto a su dignidad es el fin supremo de la sociedad y del Estado (art. 1). Por tanto, los principios de privacidad, seguridad e inclusión digital (art. 2.6), así como, los derechos a la igualdad y no discriminación (art. 2.2) son vinculantes para el mercado y las empresas de las tecnologías de la información.

En consecuencia, en el diseño, construcción, aplicación, supervisión y control de los modelos informáticos basados en la inteligencia artificial deben observarse los principios constitucionales y los derechos fundamentales como garantías de protección –directas o indirectas– de las personas,

así como asegurar el desarrollo exponencial de las empresas tecnológicas bajo principios de sustentabilidad digital (Coelho & Da Silveira, 2015).

Ello debe ser así, porque mediante la inteligencia artificial en el mundo no solo se están almacenando datos y construyendo o vendiendo perfiles de personas a través de las técnicas de procesamiento automático de datos, como los algoritmos; sino que también, esta tecnología se está usado para la toma de decisiones casi automática o automática en las relaciones entre privados y, lo más preocupante, en las relaciones entre las instancias del Estado y de la Administración Pública con los ciudadanos.

Los procesos de decisiones entre los seres humanos que se llevan a cabo en el cerebro pueden ser analizados, a un nivel de abstracción dado que los procesos computacionales intentan reproducir y mejorar, mediante la construcción de sistemas computacionales que piensen y actúen como humanos y/o racionalmente (Ponce & Torres, 2014). Por ello, las definiciones de inteligencia artificial se relacionan con el desarrollo de métodos y algoritmos que permitan a las computadoras comportarse de modo inteligente, siguiendo la conducta y el razonamiento humano predecibles (López Takeyas, 2007).

Así, la aparición y desarrollo de los motores de búsqueda Yahoo, en 1994, y Google, en 1998, han permitido indagar en las redes y construir índices con los cuales proporcionar respuestas inmediatas a los usuarios. La información solicitada es brindada a estos mediante un cálculo de relevancia y de resultados óptimos. En la actualidad, los motores de búsqueda más utilizados en el mundo son: Google que captura más del 90% del tráfico en entornos móviles, Baidu que capta el 75% del mercado de búsquedas en China, Bing que obtiene el 33% de las búsquedas en los Estados Unidos y Yahoo que capta el 2% del tráfico internacional de búsquedas, entre otros.

Mas estos motores son básicamente softwares o programas que buscan contenidos en el internet de forma rápida y eficiente, para luego, en función de las peticiones de búsqueda, presentar los resultados que han almacenado previamente en sus bases de datos o índices. No obstante, lo relevante para este artículo, desde el punto de vista de los derechos fundamentales, es el hecho de que los motores de búsqueda se componen de cuatro partes básicas: (i) una interfaz o conexión funcional que permite al usuario hacer peticiones de búsqueda; (ii) un robot que busca la información en internet; (iii) un algoritmo que conecta las peticiones de los usuarios con las bases de datos; y (iv) una base de datos, en la cual se indexan todos los contenidos (Posicionamiento MX, 2014).

Respecto del tercer componente, el algoritmo, es necesario señalar que este tendrá poca utilidad si los buscadores no cumplen con las dos funciones previas. La primera es recoger la información usando un robot o *web crawler*. Este, a modo de síntesis, se dedica a entrar a páginas web a recoger datos, identificar los enlaces de las mismas y finalmente seguir estos enlaces como lo haría un usuario navegando por las redes. Una vez que el robot encuentra la información, se debe realizar la segunda función, que es crear un índice o *index* con la información esencial de la página web que se almacena en su base de datos y que únicamente será mostrado cuando se realice una búsqueda en el motor.

A pesar de la importancia del rol que cumplen estas funciones en los motores de búsqueda, el núcleo central de estos últimos es, sin lugar a dudas, el algoritmo que dirige al robot en la categorización de la información que mostrará, no solo en función de las peticiones de los usuarios, sino también, de acuerdo con la forma en que haya categorizado la información y los descriptores con que esta se recoja. La calidad de los resultados mostrados por el buscador dependerá en gran medida de que tan bueno o malo sea el algoritmo detrás de este. De modo que, el algoritmo depende directamente de sus desarrolladores, diseñadores, fabricantes y operadores (Committee of Experts on Internet Intermediaries, 2018, pp. 7-9).

Cada vez más empresas y organizaciones estatales confían en modelos de *machine learning*. Esta es una disciplina en el campo de la inteligencia artificial que, a través de los algoritmos, dota a los ordenadores de la capacidad de identificar automáticamente patrones en datos masivos para hacer predicciones y así poder tomar decisiones por ellas. Por ejemplo, esto puede ser utilizado para elegir a quién dar un crédito, aprobar contrataciones, poner una multa de tránsito con cámaras inteligentes o realizar el reconocimiento biométrico en los controles migratorios, entre otras.

Desafortunadamente estos modelos pueden generar decisiones sesgadas, por el desconocimiento, negligencia o desinterés de los programadores y sus empresas en el reconocimiento de los derechos de los consumidores o usuarios de los motores de búsqueda en el internet, las cuales son llevadas a cabo por máquinas que procesan el lenguaje natural a un lenguaje propio de la tecnología de la información, como son los algoritmos.

Sin embargo, el lenguaje natural no es neutro, sino que expresa el conjunto de valores en que

se desenvuelven las sociedades democráticas, pluralistas y tolerantes en forma dinámica. De ahí que, el problema importante del procesamiento del lenguaje natural es determinar el significado de una palabra, en un contexto particular de valores democrático constitucionales. Ello lleva a diferentes acepciones de las palabras y por eso son recogidas con varios sentidos como en un diccionario.

En este entendido, la tarea de "desambiguación" del sentido de las palabras es identificar el sentido correcto de una palabra en un contexto determinado (Ureña & De Buenaga, 1999). Esta tarea es compleja, pero muy útil en las variadas aplicaciones del procesamiento del lenguaje natural. Por eso, los desarrolladores de los algoritmos no pueden ni deben estar ajenos al hecho de que su labor técnica tiene como fundamento y límites al orden público constitucional y, en particular, los derechos humanos universales y locales.

III. DERECHOS FUNDAMENTALES Y ALGORITMOS

El diseño, producción y uso de los algoritmos abarca considerables desafíos, no solo para las empresas que las desarrollan, sino para la sociedad en su conjunto. Ello por cuanto, el acelerado desarrollo del cambio tecnológico impacta en los derechos fundamentales, como el derecho a la dignidad humana, el derecho a la vida, la libertad de expresión, el acceso a la información, el derecho a la intimidad, el derecho a la igualdad y no discriminación, la presunción de inocencia, el derecho a un juicio justo y el debido proceso, a elecciones libres e informadas; incluso, al propio Estado de Derecho, entre otros (Innerarity, 2020).

En la actual sociedad digital, existen una serie de problemas en los derechos fundamentales provocados por el rol que vienen cumpliendo los algoritmos en la toma de decisiones, dependiendo de las funciones que realicen, el nivel de abstracción y la complejidad del procesamiento automatizado que se utilice en cada país. Sin embargo, cabe señalar que los algoritmos solo adquieren su valor en la interacción entre los seres humanos. Por consiguiente, un algoritmo matemático o computacional en abstracto no tiene por sí mismo un impacto perjudicial sobre los derechos fundamentales, pero sí su diseño, implementación y aplicación que es obra de la acción o inacción en la interacción humana entre sí.

En ese sentido, no son los algoritmos en sí mismos, sino los procesos de toma de decisiones en torno a los algoritmos los que deben ser analizados en términos de cómo afectan los derechos fundamentales. En consecuencia,

> [...] la tecnología no es sólo objeto de regulación, sino que también participa en la misma, por ejemplo, mediante la implementación en máquinas de un conjunto de requisitos éticos y legales, de forma que puedan comportarse de acuerdo con dichas reglas (Sánchez, 2016, p. 110).

Así, en algunos países los gobiernos y auditores independientes participan en alguna forma en la regulación del desarrollo algorítmico, generalmente antes de que comience la operación, como en Australia y Nueva Zelanda en la regulación de las máquinas tragamonedas que deben contender algoritmos "justos, seguros y auditables" (Francis *et al.*, 2017). En consecuencia, los desarrolladores de tales máquinas deben enviar sus sistemas algorítmicos a los reguladores antes de que puedan ser presentados a los consumidores. Sin embargo, existen otras áreas más sensibles del quehacer humano donde el impacto de los algoritmos en los derechos fundamentales es alarmante. A continuación se abordará cada una de estas, siguiendo lo descrito en el estudio sobre derechos humanos y algoritmos preparado por el Committee of Experts on Internet Intermediaries para el Consejo de Europa (2018).

A. Debido proceso

La digitalización de los procesos judiciales –demandas, audiencias y sentencias digitales– facilita a los justiciables el acceso a la justicia sin desplazamientos innecesarios y en plazos menos dilatados; sin embargo, en el sistema de justicia penal, se resienten principios procesales como la inmediación y la valoración de las pruebas, en la medida en que una audiencia virtual nunca llega a ser igual a una audiencia presencial, ya que en la primera la estación probatoria o el careo pierden su sentido. En cambio, en la esfera policial, el uso cada vez mayor de los algoritmos predictivos facilita la detención de presuntos responsables de un hecho ilícito, en virtud del registro de cámaras y el cotejo con la gran base de datos (*big data*) de registros dactilares, faciales o biométricos para la prevención y combate del delito.

Así, por un lado, en países donde en los últimos tiempos han habido ataques terroristas, como en Estados Unidos y en Europa, se han implementado plataformas de redes sociales en línea que permiten utilizar algoritmos de reconocimiento facial para identificar a posibles terroristas. Además, han comenzado a utilizar algoritmos para identificar cuentas en las redes sociales que generen contenidos extremistas. Este enfoque predictivo sobrepasa las facultades humanas para derivar conclusiones de delitos pasados, logrando predecir posibles patrones futuros de delitos.

En ese sentido, se desarrollan algoritmos que permiten implementar sistemas destinados a predecir dónde sería probable que se cometa un delito en un momento determinado; valiosa información que sirve a la policía para priorizar el tiempo y los posibles lugares para sus investigaciones y posibles detenciones. No obstante, estos enfoques podrían ser discriminatorios en función de las características raciales y antecedentes étnicos, así como, sus zonas de habitación y frecuencia; motivo por el cual, se requiere una supervisión escrupulosa con garantías constitucionales adecuadas, como la presunción de inocencia.

Aquella preocupación es legítima, porque es usual que dichos sistemas se construyan en función de las bases de datos policiales existentes que, de forma no intencionada o intencionada, reflejan sesgos o prejuicios. Asimismo, dependiendo de cómo se registran los delitos, qué delitos se seleccionan para ser incluidos en el análisis y qué herramientas analíticas se utilizan; los algoritmos predictivos pueden contribuir a una decisión perjudicial, lo que derivaría en resultados discriminatorios (Xu, 2019).

Así, por ejemplo, en el caso *Estado de Wisconsin c. Loomis* de 2016, la Corte Suprema de Wisconsin revisó la sentencia condenatoria de seis años de prisión de Eric Loomis, por su participación en un tiroteo, en la que se aplicó la herramienta de Perfiles de Gestión de Delincuentes Correccionales para Sanciones Alternativas (Correctional Offender Management Profiling for Alternative Sanctions, conocido como COMPAS), la cual utiliza algoritmos para realizar una evaluación de riesgos. La Corte confirmó el fallo. Sin embargo, con relación a dicha herramienta señaló que: (i) se desconocían los factores de riesgo exactos utilizados; (ii) la identificación de los grupos de alto riesgo no brinda un perfil determinante para individuos específicos; (iii) algunos datos podrían tener prejuicios raciales; (iv) no había sido validado o normalizado en una muestra de Wisconsin; y (v) no había sido desarrollado para su uso en una sentencia (Fischel *et al.*, 2018, p. 35).

Por otro lado, los algoritmos se utilizan cada vez más en el contexto de los sistemas de justicia civil donde se está desarrollando la inteligencia artificial para eventualmente apoyar o reemplazar la toma de decisiones por parte de los jueces. Estos sistemas se están probando actualmente para identificar los resultados de las decisiones con miras a detectar patrones en la compleja toma de decisiones judiciales. Hasta ahora, la tasa de predicción confiable es relativamente baja, alcanzando el 79% (Altreas *et al.*, 2016, p. 2).

Al respecto, si las decisiones judiciales que deben asegurar la aplicación de la ley bajo principios constitucionales, la predictibilidad del razonamiento judicial que se hace de la ley y de las pruebas pueden ser identificadas y registradas en la base de datos de la jurisprudencia; entonces, con los algoritmos correspondientes se podría ofrecer a los ciudadanos la seguridad jurídica, en principio, de cómo fallan los jueces, y a los propios jueces se les podría brindar un valioso instrumento de construcción de sus decisiones ordinarias. Pero, sería una práctica que requiere de regulación legal, para no afectar el derecho no solo a la igualdad ante la ley, sino también de igualdad en la aplicación judicial de la ley.

Esta transformación ha dado lugar a que, en China, desde el 2017, en las ciudades de Hangzhou, Pekín y otras, se venga implementando 'Cortes de Internet' con el uso de jueces robots diseñados con inteligencia artificial para resolver disputas sobre comercio electrónico y propiedad intelectual, mediante el uso de la tecnología del *blockchain.* Esta almacena evidencia de forma segura y evita el uso del papeleo, dado que como señalan "justicia demorada es justicia negada" (Xu, 2019). Más aún, un Tribunal de Nanshan de la provincia de Guangzhou, reconoció derechos de autor a un artículo escrito por un algoritmo *dreamwritter* de inteligencia artificial desarrollado por la empresa Tencen (Gutiérrez, 2020). Asimismo, la Corte de Internet de Pekín reconoció el derecho de propiedad intelectual a la creación de un *software* hecho por inteligencia artificial en función de la información acumulada de su base de datos (Xu, 2019).

Todo eso lleva a pensar que resulta necesario desarrollar un debido proceso tecnológico en la medida que un número creciente de empresas está utilizando cada vez más técnicas de análisis a través los algoritmos de *big data* para categorizar a los consumidores y hacer predicciones sobre sus comportamientos. Por eso, la supervisión de los algoritmos de puntuación contribuiría en gran medida a garantizar su imparcialidad y precisión tanto para los sistemas gubernamentales como privados. La supervisión de la determinación de las construcciones de las puntuaciones y sus aplicaciones debería estar sometida a un debido proceso tecnológico para garantizar la equidad en el goce de sus derechos fundamentales (Crawford & Schultz, 2014).

B. Derecho a un recurso efectivo

Toda persona cuyos derechos hayan sido violados tiene derecho a un recurso efectivo ante una autoridad privada o pública. El derecho a un recurso efectivo implica el derecho a obtener como respuesta una decisión motivada e individual.

Históricamente, todas estas decisiones han sido tomadas por seres humanos a quienes, en el ejercicio de sus funciones, sobre la base de una formación integral y en línea con los procesos de toma de decisiones aplicables, se les ha otorgado un margen de discrecionalidad, en función de la ley.

Sin embargo, en el acelerado mundo digital, las grandes corporaciones, frente a los sistemas de protección estatales –administrativos y judiciales–, están desarrollando sistemas complejos de respuestas automatizadas para las plataformas de internet, como los que utilizan Facebook, Google o Microsoft para atender las consultas y quejas de los usuarios (Wagner, 2016).

A menudo, muchos usuarios necesitan quejarse sobre un tipo específico de contenido, antes de que un algoritmo automatizado lo identifique como relevante, para que este sea derivado a un operador humano para su revisión. Se informa que estos operadores trabajan a menudo bajo presión durante un tiempo considerable y con instrucciones mínimas, de acuerdo con sus reglas internas.

En ese sentido, cada vez más, un número de empresas, especialmente las más grandes, utilizan algoritmos y técnicas de procesamiento de datos automatizados para ejecutar sus procedimientos de quejas. En el contexto de los procesos de eliminación de contenido automatizado en las plataformas de redes sociales, el uso de algoritmos es particularmente evidente en las respuestas que reciben los diferentes tipos de contenidos y cómo se prioriza la queja.

Por lo tanto, las plataformas de internet deben garantizar que las personas tengan acceso a realizar procedimientos de denuncia sobre las violaciones a sus derechos fundamentales en línea. Ello sin perjuicio de la existencia de los mecanismos administrativos o judiciales para buscar reparación, como las instituciones nacionales de protección de los usuarios y consumidores o la Autoridad Nacional de Protección de Datos y Acceso a la Información Pública (en adelante, ANTAIP), adjunta al Ministerio de Justicia y Derechos Humanos del Perú, en nuestro caso.

Así, por ejemplo, el 30 de diciembre de 2015, mediante Resolución Directoral 045-2015-JUS/DGPDP, la ANTAIP consideró que el permitirse a los robots de búsqueda de Google Search vincular e hipervisibilizar los datos personales (nombres y apellidos) junto con la información que un reclamante pidió cancelar –porque no se ajustaba a los nuevos hechos, dado que había sido absuelto del delito por el que se le procesaba–, constituía una lesión al derecho a la protección de sus datos personales. Ante ello, la ANTAIP concluyó que la difusión de aquella información mediante el motor de búsqueda debía cesar.

Por otro lado, desde el 2019, Facebook ha creado un Consejo Asesor de Contenidos, denominado en inglés Oversight Board for Content Decisions (en adelante, OBCD), cuya finalidad básica consiste en revisar y seleccionar un determinado número de las apelaciones de los usuarios de esta plataforma de internet con respecto a las decisiones de contenido –imágenes, videos, textos, *links*– que realizan los moderadores de Facebook. El OBCD es un órgano colegiado de cuarenta personas, con perfiles interdisciplinarios, representativo de las principales regiones del planeta, y, en principio, con una estructura operativa y remunerativa que asegura su autonomía frente al mismo Facebook (López, 2019).

Por su parte, cabe mencionar que la Unión Europea ha expedido la Directiva 2020/1828 del Parlamento Europeo y el Consejo relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores. Con ella, los Estados miembros deben disponer en su derecho procesal de un mecanismo de acción colectiva, mediante el cual puedan reclamar judicialmente un remedio resarcitorio, en interés de consumidores afectados por la conducta de, por ejemplo, las grandes empresas tecnológicas infractoras de las normativas de protección de los derechos de los consumidores y usuarios de sus plataformas digitales (Directiva 2020/1828, 2020).

Entonces, es importante garantizar que los actores del sector privado respeten los derechos fundamentales en todas sus operaciones, en particular, mediante el establecimiento de mecanismos de denuncia efectivos que resuelvan rápidamente las quejas de las personas. De lo contrario, el Estado deberá investigar, determinar responsabilidades y reparar los daños.

C. Privacidad y datos personales

La principal preocupación sobre el recojo y procesamiento automatizado de datos se relaciona con el derecho a la privacidad, en la medida que los algoritmos facilitan la recopilación, el procesamiento y la retransmisión de gran cantidad de datos e imágenes personales. En los últimos tiempos, este tipo de registro ha tenido graves consecuencias para el goce y ejercicio del derecho a la vida privada personal y familiar, incluido el derecho a la autodeterminación informativa.

Así, por ejemplo, el 5 de febrero del 2020, el Tribunal de Distrito de La Haya dictó un fallo histori-

co en el marco del caso *NJCM et al./Países Bajos,* en el cual se anuló la recopilación de datos y la elaboración de perfiles de riesgo de los ciudadanos que venía realizando el System Risk Indication (en adelante, SyRI) para detectar el fraude a la seguridad social. Este instrumento legal que utiliza el gobierno holandés se usa para combatir el fraude en áreas como la seguridad social y los impuestos. Para ello, se recopilan datos sobre ingresos, pensiones, seguros, tipo de vivienda, impuestos, multas, integración, educación, deudas o prestación por desempleo de los contribuyentes, para luego calcular, sobre la base de algoritmos, quién tiene más probabilidades de defraudar a la administración.

Como se mencionó, estos perfiles de riesgo de los ciudadanos se obtienen a través de algoritmos. En otras palabras, el sistema va delineando qué ciudadanos tienen más probabilidades de cometer fraude. En atención a ello, el Tribunal de Distrito de La Haya señaló que el sistema de SyRI no cumplía con los requisitos del artículo 8, inciso 2 del Convenio Europeo de Derechos Humanos, en el que se establece el respeto de la vida privada y los requisitos que permiten justificar la recopilación e intercambio mutuo de datos personales (Collosa, 2021).

Esto se concluyó debido a que se utilizan algoritmos para el seguimiento en línea y en la elaboración de perfiles de personas, cuyos patrones de navegación se registran mediante *cookies*. Además, los datos de comportamiento en línea se procesan desde dispositivos inteligentes, como la ubicación geo-referencial o GPS, a través de aplicaciones de los dispositivos móviles (Tene & Polonetsky, 2012).

En términos del volumen de datos registrados, procesados y la velocidad de su transmisión, la toma de decisiones algorítmicas puede tener ventajas sobre determinados tipos de toma de decisiones humanas privadas y públicas. Sin embargo, algunos algoritmos pueden tener sesgos incorporados difíciles de detectar o corregir. Esto es particularmente importante cuando las variables individuales, en los algoritmos de macro-datos, sirven como **sustitutos** de las categorías constitucionales especialmente protegidas por ser poblaciones históricamente vulnerables por raza, sexo, edad, nacionalidad, etc.

Un algoritmo sesgado que discrimina sistemáticamente a un grupo en la sociedad –por ejemplo, en función de la edad, orientación sexual, raza, género o posición socioeconómica–, puede generar afectaciones considerables tanto en términos del acceso a los derechos de los usuarios o clientes afectados por estas decisiones, como también para la sociedad en su conjunto. Al respecto, se podría argumentar que toda persona debe tener derecho a tener acceso a su perfil digital, en una versión 'neutral' de sus resultados de búsqueda.

En ese sentido, en Europa, el nuevo Reglamento General de Protección de Datos (en adelante, RGPD) ha dispuesto que: "[t]odo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar" (Reglamento 2016/679, 2016, art. 22.1). Esto significa que la decisión debe de generar en el particular que se ve sometido a este tratamiento unos efectos similares a los que se derivarían de una decisión que tenga efectos jurídicos. Esto supone, de antemano, que no toda decisión se encuadra en este precepto, sino solo aquella que genere efectos de cierta relevancia o importancia (Palma Ortigosa, 2019).

De este modo, los algoritmos deberían ser herramientas útiles para reducir el sesgo en lugares donde es común que se afecte la autodeterminación informativa y la privacidad, erigiendo una suerte de un derecho a la privacidad e identidad digital constitucional; dado que los expertos han advertido que la automatización y el aprendizaje automático tiene el potencial de reforzar los sesgos existentes. Esto es aún más preocupante si se considera que, a diferencia de los humanos, los algoritmos pueden no estar equipados para contrarrestar conscientemente los prejuicios incorporados –consciente o inconsciente– por sus desarrolladores.

D. Libertad de expresión

El diseño y funcionamiento de los algoritmos y las técnicas de procesamiento de datos tienen un enorme impacto sobre el derecho a recibir y difundir información, que es la base de la libertad de expresión. En ese sentido, los algoritmos y motores de búsqueda producen efectos positivos para el derecho fundamental a la libertad de expresión; sin embargo, también existen fundadas preocupaciones sobre si este modelo es propicio para el debate público, pluralista y tolerante, el cual debe ser igualmente accesible e inclusivo para todos dentro de una sociedad democrática. En adición, las preocupaciones respecto de la privacidad y la protección de datos señaladas anteriormente, también se reproducen en este punto, debido a que estas pueden constituir un obstáculo para la capacidad de las personas de expresarse libremente.

Los grandes motores de búsqueda son los instrumentos para buscar, recibir o impartir información; sin embargo, sus contenidos están indexados o

clasificados por algoritmos que pueden conducir a la fragmentación informativa, favoreciendo solo determinadas plataformas y tipos o conglomerados de medios de comunicación. En ese sentido, el algoritmo también puede estar sesgado hacia ciertos tipos de contenido o proveedores de contenido, con el peligro de afectar valores relacionados con el pluralismo y la tolerancia informativa de diversos medios.

Para muchos usuarios, las grandes plataformas como Google o Facebook constituyen la experiencia principal del internet y unos de los espacios fundamentales de comunicación, con capacidad para difundir masivamente la voz de los internautas. Esto, de ninguna manera, es un asunto trivial. Por ello, no se debería obstaculizar el libre flujo de la información; salvo que, por razones legales aplicadas razonable y proporcionalmente, se solicite borrar información ilícita. Este es el caso de la frecuente suspensión en Twitter y Youtube o el bloqueo indefinido de Facebook e Instagram al saliente presidente de los Estados Unidos, Donald Trump, causados por sus declaraciones racistas y de apología a la violencia, que culminaron incitando a sus seguidores fanáticos a tomar violentamente el Capitolio, sede del Congreso (Roose, 2021).

En la Unión Europa, también existen las preocupaciones por la divulgación de noticias falsas y el discurso de odio o incitación a la violencia que inundan el internet. Por ejemplo, la red social Facebook comunicó a las administradoras de la web feminista "Locas del coño" que quedaba clausurada por no cumplir con las normas comunitarias de no utilizar lenguaje que incite al odio (elDiario.es, 2016). De manera sistemática, en el 2016, la Comisión Europea aprobó un Código de conducta para la lucha contra la incitación ilegal al odio en internet (en adelante, el Código de conducta), por el cual las cuatro empresas de internet –Facebook, Microsoft, Twitter y YouTube– se comprometieron públicamente a evitar la proliferación de mensajes que fomentaran el odio, el racismo y la xenofobia a través de la red.

Por otra parte, en atención al cumplimiento del Código de conducta, en el 2016, Facebook, Microsoft, Twitter y Google, borraron 163 contenidos denunciados por doce Organisaciones No Gubernamentales de nueve diferentes Estados miembros que participaron en una evaluación de publicaciones. Al respecto, cabe señalar que en la Unión Europea no existe ningún instrumento normativo específico destinado a la persecución de los discursos de odio en internet. De modo que, se hace necesario acudir a las legislaciones nacionales que, en su gran mayoría, han optado por la vía penal para sancionar las incitaciones al odio; en consecuencia, se requiere de la armonización de la legislación europea (Valero, 2017).

Los casos mencionados demuestran que la eliminación de contenidos en las plataformas de redes sociales ya se realiza a menudo mediante procesos semiautomatizados o automatizados. Esta situación genera un impacto directo en la libertad de expresión y plantea, en algunos casos, preocupantes cuestiones para el Estado de Derecho sobre legalidad, legitimidad y proporcionalidad. Así, el mecanismo de filtrado automático para videos extremistas ha sido adoptado por Facebook y YouTube; sin embargo, no se ha divulgado la información sobre el proceso o sobre los criterios adoptados para establecer qué videos son extremistas o de contenido claramente ilegal.

Por tanto, el bloqueo, filtrado o eliminación algorítmica de contenido puede tener un impacto adverso significativo en el contenido legítimo. El dilema respecto a la eliminación de grandes cantidades de contenido legal, debido a los términos de servicio de las plataformas de internet, se ve agravado por la presión que se ejerce sobre ellas para filtrar activamente de acuerdo con nociones como 'extremista', 'discurso de odio' o 'contenido claramente ilegal', las cuales demandan una clara configuración constitucional y legal (Ortego, 2015, pp. 77-87).

E. Derecho a elecciones libres

El uso del internet en las campañas políticas y electorales ha ido cambiando la forma en que la política y las elecciones han concebido el rol de los votantes. No obstante, el uso de los algoritmos y los sistemas automatizados de información ha puesto en evidencia hasta qué punto la creación y manipulación de contenidos en las plataformas de las redes sociales, sobre las elecciones y los candidatos, puede generar desinformación selectiva en la formación de la opinión política. Esto se ve agravado por la desinformación que generan las noticias falsas o *fake news* por las redes y la que promueven agresivamente los '*trolls*' durante los debates personales que se gestan en la Red (Calvo & Aruguete, 2020).

Así como las redes sociales registran las preferencias de millones de usuarios, diversas empresas de mercadeo han trabajado para obtener esa información, algunas para usarla con fines políticos. Por ejemplo, la ex compañía británica Cambridge Analytica obtuvo millones de cuentas de usuarios de Facebook para generar propaganda política; lo que, en el 2016, tuvo incidencia en la elección de Donald Trump como presidente de los Estados Unidos y en la campaña del Brexit, que deci-

dió la salida de Reino Unido de la Unión Europea (Griffin, 2016). Este escándalo finalmente condujo a que, en julio de 2019, la Federal Trade Commission de los Estados Unidos (en adelante, FTC) le imponga una multa récord de cinco mil millones de dólares a Facebook.

Sin embargo, la acción de la FTC fue criticada por no pronunciarse adecuadamente sobre la privacidad y otros daños producidos como consecuencia de la liberación de aproximadamente 87 millones de datos de usuarios de Facebook, los cuales fueron explotados sin su autorización. Por eso, en la comunidad académica, se ha puesto la atención en la necesidad de explorar el potencial de incorporar las consultas y protecciones del tipo del debido proceso sustantivo y adjetivo, dentro de las acciones de aplicación de las agencias reguladoras como la FTC (Hu, 2020).

De allí que, en el mundo de las elecciones, la grave preocupación es que estas podrían ser ganadas, no por los candidatos con las mejores propuestas políticas, sino por aquellos que usan la tecnología que proveen las redes sociales para manipular a los votantes, a veces de manera emocional e irracional. Así, los datos que se recopilan y registran discretamente, a través de los algoritmos, se han revalorado en la medida en que podrían emplearse directamente para la micro focalización de votantes, en función de diferentes variantes o perfiles registrados en la *big data*, posiblemente con efectos decisivos en las elecciones.

Si bien la publicidad política en la televisión y la radio están reguladas, y existen requisitos de neutralidad e imparcialidad impuestos a las emisoras, no existen medidas similares para las redes sociales, en las cuales el uso de los algoritmos de preferencias y comportamiento de los votantes pueden tener un impacto igualmente o más poderoso que los medios de comunicación tradicionales. En consecuencia, esto requiere que las redes sociales apliquen los estándares legislativos de la publicidad electoral a sus plataformas y que estos sean mejorados tomando la experiencia comparada.

Más aún, si el uso de los robots con cuentas controladas algorítmicamente que emulan la actividad de los usuarios humanos, opera a un ritmo mucho más rápido. Por ejemplo, estos producen contenidos automáticamente o participan en interacciones sociales, mientras mantienen con éxito su identidad artificial sin revelarla. Por eso, en el debate sobre la gobernanza algorítmica, el enfoque inicial europeo ha buscado llegar a acuerdos con las compañías tecnológicas sobre el trato de las *fake news*; pero, ha derivado hacia los alcances regulatorios.

De acuerdo con el Profesor Magallón Rosa, la regulación de las *fake news* se puede plantear desde, al menos, dos perspectivas:

1. La necesidad de regular los contenidos independientemente de la forma en la que éstos se presentan.
2. La necesidad de legislar la forma en la que se presentan los contenidos como un mecanismo de transparencia y de defensa de nuestros derechos como consumidores (2018, p. 1).

Sin embargo, dada la importancia del desarrollo de los procesos democráticos, también se considera una dimensión temporal y de la intensidad legislativa para impedir el desequilibrio de los procesos electorales, sea, por ejemplo, en las encuestas o los resultados a boca de urna.

De allí que sea importante destacar la necesidad de la regulación del uso del internet en los procesos electorales sobre la base de los principios de transparencia, pluralismo de la información política y electoral que aseguren unas elecciones libres y transparentes. Para ello, se deben establecer disposiciones normativas positivas respecto al voto informado, pero también, relacionadas con sanciones a la manipulación de la información electoral –*fake news* y *trolls*–, a fin de que las elecciones expresen la libre, auténtica y espontánea voluntad de los electores y que los escrutinios sean reflejo exacto y oportuno de ello.

Al respecto, para las elecciones políticas presidenciales y congresales del 2021, en el Perú, los partidos han suscrito un Pacto Ético Electoral, en el que se han comprometido, entre otras cosas a: "[h]acer uso de manera ética de la inteligencia artificial, evitando el uso de *bots*, *trolls*, o cuentas falsas para difundir propaganda electoral o posicionar sus propuestas en redes sociales" (p. 8). Sin embargo, en caso de incumplimiento, el Tribunal de Honor solo puede exhortar a los responsables.

F. Libertad de asociación y reunión

En los últimos tiempos, el uso del internet, a través de los servicios de redes sociales, constituye una herramienta vital para el ejercicio y goce del derecho a la libertad de reunión y asociación, permitiendo mejorar la participación de las personas en la vida política, social y cultural. La libertad de las personas para asociarse, reunirse pacíficamente e, incluso, protestar mediante el uso de las plataformas de internet, como las redes sociales, se ha convertido en una práctica social; sobre todo, para la nueva generación, dada su condición de nativos digitales

De allí, el potencial de convocatoria, creación y difusión, a través de las redes sociales, en la organización y movilización de activistas y manifestantes es indudable. Un claro ejemplo es la movilización acontecida en la semana del 9 al 15 de noviembre del 2020 en Perú, fecha en la cual la llamada 'Generación Bicentenario' llevó a la renuncia del malhadado presidente Merino, quien provocó la arbitraria vacancia del presidente Vizcarra. En estudios realizados, se muestra cómo se vivió la coyuntura social y política desde la plataforma del Twitter (Medrano, 2020).

Sin embargo, las restricciones al derecho a la libertad de reunión pacífica y de asociación, como todo derecho, deben estar prescritas por la ley, perseguir un objetivo legítimo y ser aplicadas de forma razonable y proporcional. En este marco, el funcionamiento de los algoritmos, en las plataformas de redes sociales, permite el registro de gran cantidad de información e identificación personal de los participantes, la cual también puede usarse para rastrear e identificar a dichas personas. Ello puede conducir a la clasificación automática de las personas o grupos que hacen las convocatorias a las reuniones y protestas, lo que podría tener un impacto negativo significativo en la libertad de reunión.

La elaboración de fichas de los líderes y el control de multitudes de manifestantes siempre ha sido una labor mecánica de la policía; sin embargo, el uso del internet abre una ventana al uso de métodos de control de multitudes basados en datos dentro o fuera de línea. Teóricamente, los algoritmos utilizados para predecir posibles conflictos y situaciones de protesta también podrían usarse como herramienta preventiva para evitar manifestaciones o protestas, arrestando a ciertas personas, incluso antes de que se reúnan, como antiguamente se ha realizado por parte de las fuerzas de seguridad. Por ello, su regulación por parte del Estado demanda asegurar la libertad de asociación y reunión, tipificando claramente aquellas prácticas que atenten contra derechos de terceros y otros bienes públicos.

G. Derecho a la igualdad y prohibición de discriminación

Los algoritmos y los motores de búsqueda no tratan toda información por igual, dado que los procesos utilizados para seleccionar e indexar información se pueden aplicar según la relevancia percibida o buscada. En consecuencia, diferentes elementos de información recibirán diferentes grados de visibilidad según los factores que se tengan en cuenta en el algoritmo de clasificación.

Más aún, si los sistemas algorítmicos de toma de decisiones se basan en decisiones humanas previas, es probable que los mismos prejuicios que potencialmente socavan la toma de decisiones cotidianas se repliquen y multipliquen en los sistemas algorítmicos de toma de decisiones, solo que luego serán más difíciles de identificar y corregir. Un algoritmo sesgado que discrimina sistemáticamente a un grupo en la sociedad (por ejemplo, en función de su edad, orientación sexual, raza, género o posición socioeconómica) puede generar preocupaciones considerables, no solo en términos del acceso a los derechos de los usuarios, sino también para la sociedad en su conjunto. Por ello, la Declaración de Toronto del 2018, ha señalado que:

> Todos los actores, públicos y privados, deben prevenir y mitigar los riesgos de discriminación en el diseño, desarrollo y aplicación de tecnologías de aprendizaje automático. También deben asegurarse de que existan mecanismos que permitan el acceso a un recurso efectivo antes de la implementación y durante todo el ciclo de vida del sistema (párr. 17).

Así, por ejemplo, la reducida incorporación de las mujeres en los campos de la ciencia, tecnología, ingeniería y matemática (STEM por sus siglas en inglés) fue resultado del uso de un algoritmo encargado de la selección de trabajadores en Amazon. Este se basó en la información de los trabajadores más exitosos de la compañía de los últimos diez años que en su mayoría eran hombres, por lo que el algoritmo estaba creado para que destacaran los hombres, en perjuicio de las mujeres (Sainz *et al*., 2020, pp. 52-54).

Por ello, es una consideración potencialmente útil hacer referencia a la distinción entre discriminación directa e indirecta, para discernir cuando los algoritmos promueven o previenen el trato discriminatorio. La discriminación directa ocurre cuando una persona que toma decisiones basa su decisión directamente en criterios que se consideran prohibidos como la raza, etnia, religión, género, orientación sexual, edad o discapacidad. La discriminación indirecta ocurre cuando una determinada característica o factor se presenta con mayor frecuencia en los grupos de población considerados como categorías sospechosas por haber sido históricamente discriminados (Landa, 2021).

Por tanto, al utilizar los sistemas algorítmicos en la toma de decisiones, es importante buscar evitar tratamientos diferenciados injustificados y, por el contrario, diseñar sistemas algorítmicos de toma de decisiones que proscriban que, en la correlación entre conjuntos de datos y consideraciones de eficiencia, se pueda discriminar directa o indi-

rectamente a las poblaciones vulnerables que la Constitución considera como categorías sospechosa de discriminación, ya sea por raza, sexo, idioma, religión, opinión, condición económica o de cualquier otra índole. Por el contrario, se debería promover la regulación de algoritmos de acción afirmativa para compensar transitoriamente las desventajas de las categorías sospechosas de la histórica discriminación.

H. Derecho al trabajo y acceso a los servicios públicos

El trabajo es otra área clave en la toma de decisiones automatizada en una sociedad digitalizada. Ello se debe a que los algoritmos se pueden utilizar en las políticas de contratación y despido del personal, en la organización y administración del personal, y en las evaluaciones individuales de los empleados. A raíz de ello, aparecen interrogantes acerca de los derechos de los trabajadores, la autodeterminación de los empleados y cómo las sociedades en su conjunto creen que los seres humanos deben ser tratados en el lugar de trabajo.

El aumento del registro y la automatización de datos en los centros laborales también ha planteado desafíos en relación con el derecho a la privacidad de los trabajadores en el lugar de trabajo. La recopilación de datos se relaciona con el uso de algoritmos por parte de las empresas privadas o entidades públicas para monitorear las comunicaciones del personal o para realizar clasificaciones internas de los empleados que no forman parte del proceso de evaluación formal; ello con la finalidad de garantizar que el personal represente bien a una empresa o a una burocracia.

Así, en un tribunal italiano de Bolonia, falló que el algoritmo utilizado por la aplicación europea de entrega de alimentos Deliveroo, para clasificar y ofrecer turnos a los trabajadores (pasajeros), era discriminatorio (Collosa, 2021). Ello debido a que, el algoritmo determinaba la confiabilidad de un ciclista que trabaja para la empresa sobre la base de si no cancelaba un turno previamente reservado a través de la aplicación, al menos 24 horas antes del inicio, sin considerar que podía deberse a una emergencia o enfermedad grave, en cuyo caso tendrían menos oportunidades de trabajo en el futuro.

Ante esta situación, el tribunal señaló que el hecho de que el algoritmo no tenga en cuenta los motivos de una cancelación equivale a una discriminación y penaliza injustamente a los trabajadores con motivos legalmente legítimos. Así, ordenó a Deliveroo pagar 50 000 euros a los demandantes (Collosa, 2021).

Actualmente, el sector público en Europa viene empleando la toma de decisiones automatizadas en áreas tan diversas como la seguridad social, la tributaria, la atención médica o el sistema judicial (Tufekci *et al*., 2015). Existe un peligro considerable en la clasificación social de los datos médicos o el perfil de los desempleados, ya que los algoritmos pueden clasificar a los grupos de ciudadanos específicos mediante perfiles humanos, los cuales pueden generar decisiones arbitrarias; por ejemplo, con respecto a la recepción de beneficios sociales.

El impacto de los algoritmos en los derechos fundamentales también se expresa en los derechos a la vida, la salud, la libertad de conciencia, religión, derecho a la salud y a la educación o en el uso de robots, drones militares, entre otros. Sin embargo, son los derechos fundamentales de naturaleza política y social señalados los que sientan las bases para el goce y ejercicio de los demás derechos fundamentales y que serán materia de análisis en otra oportunidad. Sin duda, estos temas no están ajenos a los debates sobre la gobernanza algorítmica en la medida en que hace falta desarrollar un marco regulatorio amplio para las decisiones automatizadas de protección al consumidor y la regulación antimonopólica puedan contribuir a reforzar la responsabilidad algorítmica (Roig, 2020).

IV. CONCLUSIONES

El creciente uso de la automatización y la toma de decisiones mediante el uso de la inteligencia artificial en todas las esferas de la vida pública y privada ya no es una amenaza, sino que es un hecho que altera el concepto mismo de los derechos fundamentales como fundamento del Estado democrático constitucional. La tradicional asimetría de poder e información entre las poderosas redes sociales y los seres humanos se ha desplazado hacia una asimetría de poder e información entre los diseñadores de algoritmos y los ciudadanos.

Los derechos fundamentales son universales, indivisibles, interdependientes e interrelacionados; sin embargo, en la actualidad, se ven potencialmente desintegrados por el uso de tecnologías, en particular las algorítmicas. Ello debido a que la inteligencia artificial involucra tecnología que percibe elementos de su propio entorno humano –incluidos los valores y prejuicios–, con la esperanza de lograr con éxito algún objetivo específico, generalmente a través de la réplica de al menos una de las cuatro nociones de inteligencia: desempeño humano, razonamiento, procesos de pensamiento o en la búsqueda de una noción idealizada de racionalidad.

Así, se han visto afectados derechos fundamentales que los grandes operadores tecnológicos en los últimos tiempos tratan de autorregularse, pero al ser insuficiente para la protección razonable y proporcional de los derechos a la libertad de expresión, derecho a la privacidad y datos personales, igualdad y no discriminación, derechos al voto libre y adecuadamente informado, derecho al debido proceso y al acceso a tutela procesal efectiva, derecho de asociación y protesta, derecho al trabajo y acceso a los servicios públicos, entre otros, se requiere que se garantice el interés general. Por eso, cabe preguntarse si la interpretación de una norma se puede traducir en un algoritmo.

De ahí que, le correspondería al Estado regular la labor de los desarrolladores de algoritmos y datos de la tecnología, a fin de que se permita evaluarlos y así facilitar la rendición de cuentas de sus diseños, la responsabilidad a través de las evaluaciones claras de las relaciones causales o cadenas de mando, y la transparencia con respecto a cómo hacen lo que hacen. El funcionamiento interno de las tecnologías de inteligencia artificial debe dejar de ser un constructo complejo, oculto e indiscutible, dado que está al servicio de las personas (Xu, 2019).

Finalmente, el Estado, como garante del interés general, debe asegurar tanto las creaciones y el desarrollo del internet en beneficio de todos; como también, regular los algoritmos en aras de proteger los derechos de la persona humana y el respeto de su dignidad.

REFERENCIAS

Altreas, N., Tsarapatsanis, D., Preoţiuc-Pietro, D., & Lampos, V. (2016). Predicting judicial decisions of the European Court of Human Rights: A Natural Language Processing perspective. *PeerJ Computer Science*, *2*(93), 1-19. https://doi.org/10.7717/peerj-cs.93

Calvo, E., & Aruguete, N. (2020). *Fake news, trolls y otros encantos: Cómo funcionan (para bien y para mal) las redes sociales (Sociología y Política).* Editora digital Kindle.

Coelho, A., & Da Silveira, V. (2015). O proceso de inovação e os elementos da sustentabilidade digital. En G. Mendes, I. Sarlet & A. Coelho (eds.), *Direito, invovação e tecnología*. Editora Saraiva.

Collosa, A. (8 de febrero de 2021). Algoritmos, sesgos y discriminación en su uso: A propósito de recientes sentencias sobre el tema. *Centro Interamericano de Administraciones Tributarias (CIAT)*.https://www.ciat.org/ciatblog-algoritmos-sesgos-y-discriminacion-en-su-uso-a-proposito-de-recientes-sentencias-sobre-el-tema

Committee of Experts on Internet Intermediaries (2018). *Algorithms and human rights-Study on the human rights dimensions of automated data processing techniques and possible regulatory implications*. https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5.

Coppola, M. (12 de agosto de 2021). Los 17 buscadores de internet más utilizados en 2021. *HubSpot*. https://blog.hubspot.es/marketing/buscadores-mas-utilizados

Crawford, K., & Schultz, J. (2014). Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, *55*(93), 92-128.

elDiario.es (22 de diciembre de 2016). Facebook cierra la página feminista 'Locas del Coño' tras "un acoso machista organizado". https://www.eldiario.es/sociedad/facebook-feminista-locas-cono-organizado_1_3668986.html.

Fischel, S., Flack, D., & De Matteo, D. (2018). Computer risk algorithms and judicial decision-making. *Monitor on Psychology*, *49*(1), 35.

Francis, L., Livingstone, C., & Rintoul, A. (2017). Analysis of EGM licensing decisions by the gambling regulator, Victoria, Australia. *International Gambling Studies*, *17*(1), 65-86. https://doi.org/10.1080/14459795.2016.1263353.

Griffin, A. (5 de mayo de 2016). How Facebook is manipulating you to vote. *The Independent*. http://www.independent.co.uk/life-style/gadgets-and-tech/news/uk-elections-2016-how-facebook-is-manipulating-you-to-vote-a7015196.html.

Gutiérrez, L. (30 de enero de 2020). China: Un tribunal reconoce derechos a un artículo escrito por un algoritmo de Inteligencia Artificial desarrollado por una empresa. *Instituto Autor.* http://www.institutoautor.org/es-ES/SitePages/EstaPasandoDetalleActualidad.aspx?i=2592&s=1.

Hu, M. (24 de agosto de 2020). Cambridge Analytica's black box. *Big Data & Society.* https://journals.sagepub.com/doi/10.1177/2053951720938091.

Innerarity, D. (2020). El impacto de la inteligencia artificial en la democracia. *Revista de las Cortes Generales*, (109), 87-103. https://doi.org/10.33426/rcg/2020/109/1526.

Landa, C. (2019). Contenido esencial del derecho fundamental al Internet: Teoría y praxis. En C. Landa (ed.), *Libro de Homenaje del Área de Derecho Constitucional por los 100 años de la Facultad de Derecho de la Pontificia Universidad Católica del Perú.* Pontificia Universidad Católica del Perú.

(2021). *El derecho fundamental a la igualdad y no discriminación en la jurisprudencia del Tribunal Constitucional del Perú*. Tribunal Constitucional del Perú.

López, S. (25 de noviembre de 2019). Facebook y el fin de la libertad de expresión. *El Juego de la Suprema Corte.* https://eljuegodelacorte.nexos.com.mx/?p=10573

López Takeyas, B. (2007). *Introducción a la Inteligencia Artificial.* Instituto Tecnológico de Nuevo Laredo. http://itnuevolaredo.edu.mx/takeyas/Articulos/Inteligencia%20Artificial/ARTICULO%20Introduccion%20a%20la%20Inteligencia%20Artificial.pdf.

Magallón Rosa, R. (4 de mayo de 2018). Leyes 'fake news': El problema para la libertad de información de no legislar. *Telos Fundación Telefónica.* https://telos.fundaciontelefonica.com/las-leyes-las-fake-news-problema-la-libertad-informacion-no-legislar/.

Medrano, H. (28 de noviembre de 2020). La historia de un "hashtag" en los días más intensos. "Generación del bicentenario" fue la frase más usada en Twitter en protestas. *Grupo de Diarios América.* http://gda.com/detalle-de-la-noticia/?article=4247897.

Navas, S., Górriz, C., Camacho, S., Robert, S., Castells, M., & Borge, I. (2017). *Inteligencia artificial, Tecnología, Derecho.* Tirant lo Blanch.

Ortega, M. (2015). *Prestadores de servicios de Internet y alojamiento de contenidos ilícitos*. Editorial Reus.

Palma Ortigosa, A. (2019). Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos. *Revista General de Derecho Administrativo*, (50).

Ponce, J., & Torres, A. (2014). Introducción y Antecedentes de la Inteligencia Artificial. En *Inteligencia Artificial.* Iniciativa Latinoamericana de Libros de Texto Abiertos. http://dx.doi.org/10.13140/2.1.3720.0960

Posicionamiento MX (23 de mayo de 2014). ¿Cómo funcionan los motores de búsqueda?. *Posicionamiento MX*. https://www.posicionamiento.mx/blog/seo/como-funcionan-los-motores-de-busqueda.

Roig, A. (2020). *Las garantías frente a las decisiones automatizadas: Del Reglamento General de Protección de Datos a la gobernanza algorítmica*. J.M. Bosch. https://doi.org/10.2307/j.ctv1dv0v54.

Roose, K. (7 de enero de 2021). The President Is Losing His Platforms. *The New York Times.* https://www.nytimes.com/2021/01/07/technology/trump-social-media.html.

Sainz, M., Arroyo, L., & Castaño, C. (2020). *Mujeres y digitalización. De las brechas a los algoritmos*. Red.es. Ministerio de Asuntos Económicos y Transformación Digital (coords.). DOI: 10.30923/MujDigBreAlg-2020.

Sánchez, A. (2016). *Reflexiones de un replicante legal*. Thomson Reuters Aranzadi.

Tene, O., & Polonetsky, J. (2012). To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising. *Consortium on Law and Values in Health, Environment & the Life Sciences, 13*(1).

Tufekci, Z., York, J., Wagner, B., & Kaltheuner, F. (2015). *The Ethics of Algorithms: From Radical Content to Self-Driving Cars*. European University Viadrina Frankfurt. https://cihr.eu/publication-the-ethics-of-algorithms/.

Ureña, L., & De Buenaga, M. (1999). Utilizando WordNet para Complementar la Información de Entrenamiento en la Identificación del Significado de las Palabras. *Inteligencia Artifcial*, *3*(7).

Valero, A. (10 de enero de 2017). ¿La libertad de expresión en manos de un algoritmo? [Entrada de blog] *Al revés y al Derecho*. http://blogs.infolibre.es/alrevesyalderecho/?p=4805

Wagner, B. (2016). *Global Free Expression: Governing the Boundaries of Internet Content*. Springer International Publishing.

Xu, B. (2019). Algorithm regulation under the framework of human rights protection. *The Journal of Human Rights*, *18*(4).

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Acta de subscripción al Pacto Ético Electoral (Pacto Ético Electoral, Jurado Nacional de Elecciones [JNE], 28 de enero de 2021.

Código de conducta para la lucha contra la incitación ilegal al odio en Internet*, Comisión Europea*, 30 de junio de 2016 (UE).

Constitución Política del Perú [Const.] (1993) (Perú).

Declaración de Toronto: Protección del derecho a la igualdad y la no discriminación en los sistemas de aprendizaje automático, del 16 de mayo de 2018 (Amnesty Int'l).

Directiva 2020/1828 del Parlamento Europeo y del Consejo de 25 de noviembre de 2020 relativa a las acciones de representación para la protección de los intereses colectivos de los consumidores, y por la que se deroga la Directiva 2009/22/CE, 2020 O.J. (L409)1 (UE).

Estado de Wisconsin c. Loomis, 881 N.W.2d 749 (Wis. 2016).

Rb Dan Haag 5 februari 2020, NJ 2020, 368 m.nt. van E.J. Dommering (NJCM et al. /Países Bajos) (Países Bajos).

Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), 2016 O.J. (L 119) 1 (UE).

Resolución Directoral 045-2015-JUS/DGPDP de la Dirección General de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, de 30 de diciembre de 2015 (Perú).

10.18800/themis.202101.003

NEUTRALIDAD DE RED Y LIBERTAD DE EXPRESIÓN: UNA RELACIÓN EN DEBATE

NET NEUTRALITY AND FREEDOM OF SPEECH: A DISPUTED RELATIONSHIP

Omar Alvarado Escobar*
Miranda & Amado

In this article, the author addresses the issue of net neutrality and its relationship with freedom of speech. Specifically, he studies if net neutrality policies that operate ex ante regulations really have an important and supportive role in the protection of freedom of speech on the internet. Thus, the aim is to review certain premises that support the current regulations that rule net neutrality and the other fundamental rights with which these regulations collide.

In that way, the article gives a conceptual framework of the actors in cyberspace; later, it presents the arguments with which net neutrality has been connected with freedom of speech; and, finally, the author makes a critic about the importance that has been given to net neutrality in the protection of freedom of speech and the possible collisions with other fundamental rights that they may have.

Keywords: Net neutrality, freedom of speech, internet, fundamental rights, ISP.

En el presente artículo, el autor aborda el tema de la neutralidad de red y su relación con el derecho a la libertad de expresión. En específico, busca cuestionar y reflexionar sobre si las políticas de neutralidad de red que establecen regulaciones ex ante *en verdad tienen un papel irremplazable y favorecedor en la protección de la libertad de expresión en internet. Así, se tiene el objetivo de revisar ciertas premisas que fundamentan las normativas actuales que versan sobre la neutralidad de red y los otros derechos fundamentales con los que estas regulaciones colisionan.*

Con este objetivo, dentro del artículo, primero, se da un marco conceptual de los actores en el ciberespacio; después, se desarrollan los fundamentos con los que se ha venido conectando a la neutralidad de red con la libertad de expresión; y, por último, se realiza una crítica a la importancia que se le ha dado a la neutralidad de red en la protección de la libertad de expresión y las colisiones con otros derechos fundamentales que esta puede conllevar.

Palabras clave: Neutralidad de red, libertad de expresión, internet, derechos fundamentales, ISP.

* Abogado. Master of Science (M.Sc.) en Regulación por la London School of Economics and Political Science (LSE). Asociado senior de Miranda & Amado Abogados (Lima, Perú). Correo: oalvarado@mafirma.com.pe

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 7 de febrero de 2021, y fue aceptado por el mismo el 25 de junio de 2021.

I. INTRODUCCIÓN

Internet es la plataforma de difusión de información y opiniones más relevante para la sociedad contemporánea. A diferencia de los medios de comunicación tradicionales, cuya audiencia es limitada, tienen altos costos de publicación e imponen dificultades para encontrar la información que contienen (Harris, 2016, p. 223), internet permite no solo que los creadores de contenido puedan publicar digitalmente sus producciones asumiendo bajas inversiones (Adamson, 2002, p. 272), sino que los usuarios enfrenten menores costos de búsqueda para acceder a los contenidos que necesitan (Body of European Regulators for Electronic Communications [BEREC], 2016, p. 4).

Esta naturaleza del internet es determinante para el cumplimiento de funciones democráticas y culturales vitales (Audibert & Murray, 2016, p. 118). Ha impulsado en el mundo movimientos democráticos como la Primavera Árabe en Egipto y Túnez, donde "seis de cada diez usuarios de redes sociales compartieron su opinión política en línea" (Pew Research Center, 2012) [traducción libre][1]. De igual manera, ha hecho posible que se promueva la participación de comunidades marginadas como la afrodescendiente, la LGBTIQ+ o las minorías religiosas (Free Press, 2019). Internet es, así, uno de los desarrollos más significativos para el empoderamiento de la ciudadanía en la historia, cumpliendo un papel privilegiado en el fomento de un derecho fundamental: la libertad de expresión[2].

Bajo este contexto, las decisiones sobre el manejo y gestión de internet son centrales en el debate de este derecho fundamental. Siguiendo a Balkin, en un entorno como el actual, liderado por la difusión digital, "las decisiones más importantes que impactarán sobre el futuro de la libertad de expresión no ocurrirán exclusivamente en el mundo formal del derecho constitucional; serán decisiones que versan sobre diseño de tecnologías" (2008, p. 427) [traducción libre][3]. Una de esas decisiones tecnológicas es la referida a la adopción y alcances de la implementación de la neutralidad de red.

La neutralidad de red como política pública, representa, en simple, la idea de que los usuarios de internet tienen derecho a que los agentes privados que prestan el servicio de acceso a internet no diferencien en función del origen, destino o propiedad del protocolo o aplicación que se transmite a través de las redes que administran (Jordan, 2007, p. 428).

Basados en este axioma de no discriminación entre contenidos que promueve la neutralidad de red, sus promotores sugieren que esta surge como una herramienta con impacto sobre "política de medios, política social, supervisión de los procesos políticos y de libertad de expresión" (Wu, 2014, p. 70) [traducción libre][4]. Según un recuento de la literatura más relevante sobre la materia hecho por Brouwer, la neutralidad de red constituiría una política sin la cual no sería posible la libertad de expresión en el ciberespacio (2015, p. 14).

Sin embargo, ¿qué tan cierto es que sin neutralidad de red la libertad de expresión quedaría desprotegida? Este es un debate que ha cobrado protagonismo y que nos obliga a someter a escrutinio esta premisa que parece pacíficamente asumida en nuestro medio. Por ejemplo, en Estados Unidos se sostuvo hace no mucho una intensa discusión pública sobre el dudoso rol de la neutralidad de red en la libertad de expresión. Tras recibir casi 22 millones de comentarios y pese a una intensa oposición de la opinión pública (83% de norteamericanos) (Fung, 2017), en diciembre de 2017 –luego de considerar, entre otras razones, que no se había acreditado que la prohibición *ex ante* de neutralidad de red haya proporcionado un valor adicional significativo para proteger la libertad de expresión por encima de las fiscalizaciones caso por caso– la Comisión Federal de Comunicaciones (en adelante, FCC) votó 3 a 2 para revocar dicha regulación (pp. 93, 159, 253, 296-297).

Si en Estados Unidos –uno de los países con una de las más amplias tradiciones en materia de libertad de expresión– el compromiso de la neutralidad de red a favor de este derecho fundamental es debatido, esto invita, cuando menos, a revisar algunas

---

1 Texto original: "six-in-ten social networkers share their views about politics online".

2 Algunos académicos argumentan que el acceso a internet debería ser considerado un derecho humano independiente, mientras que otros expertos argumentan que el Internet es solo una tecnología que facilita el ejercicio de otros derechos fundamentales (entre ellos, el de libertad de expresión). Para efectos de este artículo, asumiremos la última posición planteada.

Mayor detalle sobre este interesante debate se puede consultar en las siguientes fuentes: De Hert y Kloza (2012); The Guardian (2016); Consejo de Derechos Humanos de la Organización de las Naciones Unidas (Recomendación A/HRC/32/L.20, 2016); y Cerf (2012).

3 Texto original: "the most important decisions affecting the future of freedom of speech will not occur in constitutional law; they will be decisions about technological design".

4 Texto original: "media policy, social policy, oversight of the political process, issues of free speech".

premisas. Pensemos por un momento en el caso de un proveedor de internet privado que decide diferenciar en el tráfico que transporta y darle una 'porción' dedicada de la red a un proveedor de contenido que requiere mayor ancho de banda y quien le retribuye ese beneficio (*e.g.*, YouTube frente a TikTok). Bajo las reglas de neutralidad de red establecidas en nuestra regulación, dicha práctica de priorización estaría vedada *per se*[5]. Sin embargo, ¿en dónde entra a tallar en esta ecuación la libertad de expresión? ¿Cómo podría impactar en la libertad de información y opinión de los ciudadanos el otorgar prioridad a un contenido por sobre otro por razones meramente comerciales, que no se inspiran en la censura de algún discurso o contenido? ¿No tienen acaso los propios proveedores de internet, que administran el tráfico, un 'control editorial' legítimo –similar al de un medio de prensa– para decidir qué contenido privilegian por sobre otro y, por tanto, no ejercen también estos proveedores de internet su propia libertad de expresión, de empresa y de contratación? ¿Se justifica una regla de prohibición *ex ante* y *per se,* como la pregonada por la neutralidad de red, o sería mejor contar con un sistema de control *ex post* y caso por caso de las intervenciones sobre el tráfico de internet?

El presente artículo se abocará a reflexionar sobre estas interrogantes y poner en tela de juicio un concepto que se da por sentado: que la neutralidad de red es una política pública que favorece, en todos los casos, la protección del derecho fundamental a la libertad de expresión en el ciberespacio.

A tal efecto, la sección II de este documento explorará algunas definiciones técnicas elementales que permitirán a los lectores entender quiénes son los actores involucrados en el ciberespacio, la actividad que desarrollan y lo que se entiende por neutralidad de red. La sección III desarrollará los fundamentos conceptuales y bases normativas que vinculan a la neutralidad de red con la libertad de expresión, repasándose a tal efecto fundamentalmente lo que se ha escrito en la literatura anglosajona, europea continental y los pocos trabajos nacionales sobre la materia. Finalmente, la sección IV examinará críticamente estas bases teóricas y legales presentadas en la sección anterior, para determinar si el rol de la neutralidad de red en la protección de la libertad de expresión es tan profundo como se asume normalmente o si, incluso, colisiona con otros derechos fundamentales.

II. DEFINICIONES

A. Los actores

La arquitectura del internet depende de diversos agentes organizados de manera vertical, que proveen cada uno ciertas funcionalidades (Jordan, 2007, p. 432). Dos de esos actores que interactúan en el proceso de transmisión de la información a través de la red son los denominados proveedores del servicio de acceso a internet y los llamados proveedores de aplicaciones, servicios o contenidos en internet. Veamos.

1. Proveedor de servicios de internet (ISP)

Según la sección de Definiciones del Reglamento de Neutralidad en Red aprobado por Resolución de Consejo Directivo 165-2016-CD-OSIPTEL (en adelante, el Reglamento), un *internet service provider* (en adelante, ISP por sus siglas en inglés) es un operador de telecomunicaciones que presta el servicio público de conmutación de datos por paquetes y permite que sus clientes (usuarios individuales o empresas) accedan a internet[6].

¿Cómo lo permiten? Los ISP conforman un gran ecosistema de múltiples redes interconectadas que permiten la transmisión de información (Jordan, 2007, p. 437). Los ISP están interconectados y se encargan del enrutamiento de las señales a otros ISP. Esta señal escala a otros ISP medios hasta que es captada por un más grande y veloz *backbone* de internet que constituye el punto de intercambio de internet, desde el cual la señal desciende al ISP de destino, que constituye la conexión de '**última**

[5] Según el artículo 35.3 del Reglamento de Neutralidad en Red aprobado por Resolución de Consejo Directivo 165-2016-CD-OSIPTEL, se considerará arbitraria la medida asociada a la oferta comercial que establezca una "priorización de cualquier tipo de tráfico, protocolo, servicio o aplicación en los Componentes con Tratamiento Diferenciado; en relación a los equivalentes disponibles en los Componentes sin Tratamiento Diferenciado" (2016). Se entiende que es un 'Componente con Tratamiento Diferenciado' aquel grupo de servicios o aplicaciones a los que se le da un tratamiento comercial distinto (con tarifas especiales o gratuitas).

[6] Reglamento, Anexo I, Definiciones:

18. Proveedor del Servicio de Acceso a Internet: Operador de Telecomunicaciones, que en la forma de persona natural o jurídica, cuenta con el registro correspondiente para prestar el servicio público de valor añadido de conmutación de datos por paquetes (Internet). Se encuentran comprendidos en esta categoría las empresas que se dedican únicamente a prestar servicios de Acceso a Internet; así como los concesionarios de servicios portadores, finales y de difusión, empresas con registro de comercialización de servicios públicos de telecomunicaciones, empresas con registro de operador móvil virtual, que además de sus respectivos servicios autorizados, también presten servicios de Acceso a Internet (Resolución de Consejo Directivo 165-2016-CD-OSIPTEL, 2016).

milla' (Departamento de Comercio de los Estados Unidos, 2014, p. 1; Shuler, 2002).

En ese sentido, los ISP, como controladores del enrutamiento, son capaces de generar un "efecto paralizador en la impartición y recibimiento de datos" (Koops & Sluijs, 2012, p. 511). Los ISP controlan el tránsito de los paquetes de datos a través de la red y, por consiguiente, "están en la posición de guardianes entre el acceso de los usuarios finales a contenido de los proveedores como aplicaciones, servicios, dispositivos y viceversa" (Comisión Federal de Comunicaciones [FCC], 2017, p. 261).

2. Proveedor de servicios de aplicación y contenido

De acuerdo con la sección de Definiciones del Reglamento, esta capa de la arquitectura de internet abarca a toda persona natural o jurídica, vinculada o no al ISP, que "provee aplicaciones, servicios o contenidos, soportados en el Acceso a internet, de forma gratuita o con una tarifa determinada" (Resolución de Consejo Directivo 165-2016-CD-OSIPTEL, 2016, Anexo I, numeral 17). Esto comprende todos los materiales que son almacenados, transmitidos y accedidos a través de la red y que se encuentran disponibles para los usuarios finales en línea (Murray, 2007, pp. 43-44). Así, son proveedores de servicios de aplicación y contenido (en adelante, Proveedores de Contenido) desde el titular de una pequeña web en la que se aloja una tienda virtual que acaba de emerger en pandemia hasta gigantes de internet tales como Amazon, YouTube, Facebook, Google o Netflix.

B. La relación entre ISP y Proveedores de Contenido: gestión de tráfico y neutralidad de red

Para contactar a los usuarios finales a través de la 'última milla', los Proveedores de Contenido recurren a las ISP, de quienes son sus clientes.

Estos clientes no cuentan con proveedores que les proporcionen recursos infinitos. Pese a los grandes avances de la era digital, la capacidad de transmisión de las ISP no es ilimitada ni de bajo costo (May, 2007, pp. 204-206). En ciertos escenarios, el tráfico de las aplicaciones consume mucho ancho de banda (por ejemplo, transmisión de un video en alta definición); y esta demanda de tráfico ocasiona una ralentización en la transmisión de información de otros servicios o contenidos (Saunders *et al*., 2012, p. 11). La capacidad de red es limitada, por lo tanto, el consumo de cada Proveedor de Contenido o usuario final puede crear latencia y retraso entre las conexiones (Doverspike *et al*., 2010, pp. 55-56).

La forma en que los ISP enfrentan esta congestión es a través de la gestión del tráfico que viaja por sus redes. Técnicamente, el tráfico puede ser controlado por los ISP sin diferenciaciones, fundamentando la prioridad en el envío de los paquetes de datos en función de quien llegue primero, independientemente si son clientes o no de la ISP (Jordan, 2007, p. 434). Sin embargo, el protocolo de gestión del tráfico de los ISP puede ser programado con funciones más avanzadas y complejas (BEREC, 2015; Shatz, 2017). Los ISP pueden gestionar el tráfico de la red por razones de administración de la calidad de servicio que requiere cada aplicación (por ejemplo, latencia, pérdida de datos o ancho de red) para aliviar la congestión (BEREC, 2016) o pueden simplemente dar cumplimiento a órdenes gubernamentales (Kreimer, 2006). También ha sido ampliamente documentado que la prioridad puede tener intereses puramente comerciales (Nunziato, 2009, pp. 9-19). Por consiguiente, técnicamente los ISP podrían examinar los paquetes de información de los Proveedores de Contenido que están enrutando, diferenciarlos y privilegiar un contenido por sobre otro.

Sin embargo, frente a esta segunda forma de gestión de tráfico, se erige la prohibición de la neutralidad de red. La literatura califica a la neutralidad de red como una prohibición *ex ante* y *per se* frente a cualquier forma que represente un trato preferente y que implique limitar o degradar un tipo de tráfico de internet o de aplicaciones por sobre otro (Belli, 2016, pp. 18-19), lo cual se produce desde las prácticas más simples de bloqueo hasta algunas más sofisticadas como la asignación de porciones dedicadas de la capacidad de red a la ISP (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2007; Office of Communications [OFCOM], 2013) o el cobro de precios relacionados a la congestión (Hahn & Wallsten, 2006). En otras palabras, la neutralidad de red "determina condiciones básicas para que ninguna aplicación (como Skype o Netflix) sea discriminada arbitrariamente por un proveedor de conexión (como Claro o Movistar)" (Morachimo Rodríguez, 2017, p. 250).

A nivel normativo peruano, el principio regulatorio de la neutralidad de red ha sido recogido por la Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica, aprobada por Ley 29904 (2012) (en adelante, Ley de Banda Ancha), y su Reglamento aprobado por Decreto Supremo 014-2013-MTC (2013).

Conforme a lo establecido en el artículo 6 de la Ley de Banda Ancha, la neutralidad de red implica que los ISP no pueden de manera arbitraria bloquear, interferir, discriminar ni restringir el derecho de cualquier usuario a utilizar una aplicación

Gráfico 1

Fuente: Osiptel (2021)

o protocolo, independientemente de su origen, destino, naturaleza, naturaleza o propiedad (Ley 29904, 2012). Por su parte, el Anexo I numeral 8 del Reglamento califica como medidas de gestión de tráfico que significan una vulneración de la neutralidad de red el "bloquear, interferir, discriminar, restringir o degradar cualquier tipo de tráfico, protocolo, servicio o aplicación, independientemente de su origen, destino, naturaleza o propiedad" (Decreto Supremo 014-2013-MTC, 2013), en tanto ello constituya una forma de gestión arbitraria de tráfico, un filtro y/o bloqueo arbitrario de servicios y/o aplicaciones, o una diferenciación arbitraria de atributos en la oferta comercial. Ver gráfico adjunto donde se muestra un resumen de las medidas autorizadas y prohibidas a los ISP.

A partir de lo anterior, no solo bajo la garantía de la neutralidad de red quedará prohibido que un ISP ejerza un bloqueo con fines 'políticos' y con impacto sobre la democracia, por ejemplo, al restringir una página web de prensa independiente dedicada a destapar escándalos de corrupción de relevancia para la opinión pública que viene siendo incómoda para los accionistas. Quedará también limitado que un ISP ejerza decisiones de gestión de tráfico inspiradas en razones estrictamente comerciales, como lo sería, por ejemplo, celebrar un contrato que priorice determinado tráfico de datos con contenidos de mero entretenimiento (por ejemplo, el que proviene de Netflix por sobre el de Amazon Prime previo pago de una contribución) o que opte por imponer pagos para el acceso a una web que proporciona el mismo tipo de contenido (*e.g.*, si Movistar solicita pagos adicionales por acceder al portal web del diario deportivo El Bocón, que compite con los contenidos de su diario Movistar Deportes). Así de amplio es el espectro de protección que proporciona el principio regulatorio de neutralidad de red.

III. NEUTRALIDAD DE RED Y LIBERTAD DE EXPRESIÓN: LOS FUNDAMENTOS DE ESTE DISCURSO

La gestión de tráfico y la neutralidad de red han sido analizadas desde diferentes perspectivas. Áreas como protección de la privacidad y datos personales (Audibert & Murray, 2016, p. 133; Koops & Sluijs, 2012)[7], y libre competencia y asuntos de protección al consumidor (Becker *et al.*, 2010; Cooper & Brown, 2015), generan un alto nivel de controversia entre los especialistas. Sin embargo, el aspecto que debatiremos en este trabajo se relaciona con el impacto sobre la libertad de expresión que se argumenta tiene el principio de neutralidad de red.

En el Perú, no existe en la normativa de neutralidad de red una alusión expresa a la libertad de expresión como elemento de sustento. No obstante, esta falta de alusión expresa no debe ser confundida como falta de reconocimiento en el plano nacional. Los instrumentos normativos nacionales aluden al papel que cumple la neutralidad de red para preservar la libertad de elección de

[7] El argumento de estos autores es que, para decidir si el contenido debe ser bloqueado o priorizado, las ISP tienen la capacidad de inspeccionar el contenido de los datos transportados.

los usuarios frente a cualquier tipo de 'protocolo, tráfico, servicio o aplicación', así como al objetivo de potenciar una 'comunicación plena', lo que en nuestra opinión traduce un reconocimiento implícito del rol de la neutralidad de red como una herramienta que potenciaría la libertad de expresión. Por ejemplo, la parte considerativa del Reglamento precisa que su finalidad es "preservar la libertad de elección de los usuarios en el acceso a internet, asegurando el libre acceso a cualquier tipo de protocolo, tráfico, servicio o aplicación disponible en internet" (Decreto Supremo 014-2013-MTC, 2013). En la misma línea, el artículo 5.1 del referido Reglamento recoge como uno de los principios rectores de la neutralidad de red el denominado "Principio de Libre Uso", el cual es enunciado como "[t]odo usuario tiene derecho a la libertad de uso y disfrute, a través del Servicio de Acceso a internet, utilizando cualquier equipo o dispositivo terminal y dentro de lo lícitamente permitido, de cualquier tráfico, protocolo, servicio o aplicación" (Decreto Supremo 014-2013-MTC, 2013).

Por su parte, la Matriz de Comentarios elaborada por el Ministerio de Transportes y Comunicaciones con ocasión de la aprobación del Reglamento de la Ley de Banda Ancha, señala lo siguiente:

> [C]on la neutralidad de red no se pretende establecer una limitación irrestricta sobre la posibilidad de que las empresas operadoras puedan implementar medidas de gestión de la red, como las indicadas en el cometario; sino es simplemente, **evitar que ocurran limitaciones arbitrarias, es decir, carentes de sustento, las que por ejemplo podrían restringir los derechos de los usuarios a gozar de una comunicación plena a través de internet** [...] (2013) [el énfasis es nuestro].

En la misma línea de lo enunciado normativamente a nivel local, los pocos trabajos doctrinales nacionales sobre esta política regulatoria sostienen la existencia de esta vinculación (Morachimo Rodríguez, 2016; Villena, 2017), reafirmando así un reconocimiento en el plano peruano, en el sentido que la libertad de expresión y la protección del sistema democrático son valores constitucionales que no podrían garantizarse sin la neutralidad de red.

En el plano internacional, buena parte de los documentos emitidos por organizaciones internacionales y la literatura especializada también dan por sentado que sin neutralidad de red no sería posible garantizar la libertad de expresión en el ciberespacio. Como indica la Relatoría Especial de la Comisión Interamericana de Derechos Humanos, "la neutralidad de red es una condición necesaria para ejercer la libertad de expresión, y es transversal a los principios rectores" (2013, párr. 25). Con ese tenor, como sostiene Tim Wu –a quien se le atribuye haber acuñado este concepto– la neutralidad de red se convierte en "un principio máximo de diseño de red donde el contenido en línea debe ser de acceso universal para todos los usuarios de internet, sin importar el contenido o plataforma" (Wu, 2003, citado por Belli, 2016, p. 16) [traducción libre][8]. Así, como sostienen sus proponentes, el uso de técnicas de gestión de tráfico puede poner en riesgo el ejercicio efectivo de los usuarios para poder buscar, recibir y compartir información e ideas, o lo que es lo mismo, para ejercer la libertad de expresión (Belli, 2016, p. 19), al punto que diversas voces han categorizado a la neutralidad de red como la verdadera 'Primera Enmienda' del internet (London School of Economics and Political Science, 2011).

¿De qué premisas parten los defensores de la neutralidad de red para sostener su papel protector indispensable de la libertad de expresión? A partir de una revisión de la literatura y decisiones de otras latitudes, hemos identificado tres premisas, que desarrollamos a continuación.

A. Primera premisa: el enfoque social y el modelo de eficacia horizontal de los derechos fundamentales

La visión del derecho fundamental a la libertad de expresión ha evolucionado desde un plano individualista –en el que se le entiende como un derecho subjetivo asociado al libre desenvolvimiento de la personalidad– hacia una visión social, en la que este derecho tiene un enfoque colectivo, relevante por su utilidad para el desarrollo del sistema democrático (Marciani Burgos, 2005; Castillo-Córdova, 2006, pp. 10-11).

Bajo este enfoque social –también denominado habermasiano o madisoniano– medidas preventivas y acciones positivas por parte del gobierno deberían ser tomadas para fomentar la libertad de expresión de los ciudadanos y así asegurar su participación en la esfera pública, permitiéndoles el más amplio acceso a temas de interés público, como educación y política. Del mismo modo, en este enfoque el pluralismo de los medios debe ser protegido proactivamente debido a la importancia de la exponer a la población a diversas posturas políticas y valores culturales (Katholische Univer-

[8] Texto original: "'network design principle' whereby a maximally useful public information network aspires to treat all content, sites and platforms equally, thus granting to all Internet users universal access to all online resources".

sität Leuven *et al*., 2009, pp. 5-6; Sunstein, 1994, pp. 1759-1760, 1804; High Level Group on Media Freedom and Pluralism, 2013, pp. 10-11).

Este enfoque social mira con recelo las interacciones entre los privados y reconoce que ellas pueden ser fuente de limitaciones a la participación democrática y pluralismo, porque el poder privado, en algunos casos, es tal que otorga la habilidad de censura (Hudson, 2018). A diferencia de la visión de libertad de expresión negativa –bajo la cual ideas y opiniones son tratadas como cualquier otro bien en los mercados, compitiendo entre ellas y arbitrándose solas, de manera que solo el Gobierno puede lesionar la libertad de expresión, en expresión de lo que se denomina "State Action Doctrine" (Lyons, 2017)–, en el enfoque social los privados también pueden restringir la libertad de expresión. Así, el Estado está justificado para intervenir en el mercado de difusión de información, pues su meta es lograr una cantidad objetivamente deseable de opiniones en asuntos de público y de relevancia social (Nunziato, 2009, p. 31).

Como puede verse, el enfoque social constituye una perspectiva que es deudora de la visión de la eficacia horizontal de los derechos fundamentales, concepto de plena aplicación en el Perú, conforme lo ha señalado el Tribunal Constitucional en diversas sentencias (Expediente 1848-2004-AA/TC, 2004, fundamento 2; Expediente 01643-2014-PA/TC, 2018, fundamento 22). Bajo esta visión constitucional, los poderes privados pueden resultar particularmente nocivos para los derechos fundamentales de los individuos y para la libertad de expresión, en particular (Mendoza Escalante, 2005, p. 228).

La neutralidad de red es una política pública que materializa este enfoque social y de intervención ante posibles violaciones de los privados en el ámbito del ciberespacio. Como reconoce la propia Exposición de Motivos del Reglamento, este marco normativo ha tenido especial atención y en cierta forma se ha inspirado en las disposiciones emitidas en Europa, que sí son explícitas en abrazar el enfoque social y la eficacia horizontal que hemos explicado, al declarar su apoyo proactivo al pluralismo y la democracia frente a actuaciones de privados en el entorno digital (Comité de Ministros de los Estados Miembros de la Unión Europea, 2007). Es a partir de estos principios que, por ejemplo, en el ámbito comunitario europeo, "muchos de los casos fuertemente informados por las disposiciones de derechos fundamentales de la UE han sido controversias privadas" (Chalmers & Trotter, 2016, p. 33) [traducción libre][9], siendo los juicios *Scarlet c. Sabam* (2011) y *Sabam c. Netlog* (2012) –en los que el Tribunal de Justicia de la Unión Europea calificó que la censura digital de los ISP socavaba la libertad de expresión– ejemplos de la afirmación del enfoque social y eficacia horizontal en el campo de este derecho fundamental. Por ello, es válido afirmar que el legislador peruano ha seguido esta visión social europea al acoger la neutralidad de red como una garantía a la libertad de expresión.

En el mismo sentido, la literatura de respaldo a la neutralidad de red da cuenta de este enfoque social y del concepto de eficacia horizontal en la protección del derecho fundamental a la libertad de expresión, pues sostiene que es ingenuo confiar en las fuerzas del mercado y en las respuestas del sistema de defensa de la competencia a las actuaciones de privados en el ciberespacio. Los privados, a decir de Ohlhausen, no considerarían valores no monetarios como la transparencia del internet, la participación democrática, la diversidad de perspectivas y la libertad de expresión (2016, p. 122). Como ha sostenido Marsden, en su trabajo sobre neutralidad de red, "[t]odos los propietarios de red tienen incentivos para detener el tráfico que es de bajo valor, alto volumen […]" (2009, p. 16) y sus "agendas difieren en gran medida respecto a la de los gobiernos" (p. 18) [traducción libre][10]. En esa línea, Sunstein precisa que

> en lugar de permitir que las nuevas tecnologías utilicen los procesos democráticos para sus propios fines, el derecho constitucional debería ocuparse del aprovechamiento de esas tecnologías con fines democráticos, incluidas las aspiraciones fundadoras de la deliberación pública, la ciudadanía, la igualdad política e incluso un cierto tipo de virtud (1994, p. 1804) [traducción libre][11].

Así, dejar que los ISP decidan quién tiene acceso a su plataforma y en qué medida, puede limitar a una proporción de la población de acceder a los

[9] Texto original: "Many of the cases in which legislative content had been heavily informed by EU fundamental rights provisions have been private disputes".

[10] Texto original: "All network owners have incentives to stop traffic flowing over their networks that is low value, high volume […] whose agendas are very different from those of governments".

[11] Texto original:

> instead of allowing new technologies to use democratic processes for their own purposes, constitutional law should be concerned with harnessing those technologies for democratic ends –including the founding aspirations to public deliberation, citizenship, political equality, and even a certain kind of virtue.

espacios necesarios para su expresión y el pluralismo (Audibert & Murray, 2016, p. 138). Sobre la base de este riesgo, la neutralidad de red se erige para sus defensores, habiendo encontrado también en el Perú espacio en la formulación de políticas públicas de protección de la libertad de expresión.

B. Segunda premisa: la libertad de expresión no solo protege contenidos. El mero acto de transmisión debe también ser tutelado

La protección otorgada por la libertad de expresión tiene, según ciertos autores, una doble faceta: la tutela frente a las intervenciones sobre los contenidos y la tutela frente a las intervenciones denominadas por la doctrina 'neutras'. El primer ámbito se refiere a la garantía clásica que se otorga frente a intervenciones que restringen las ideas, pensamientos, juicios de valor u opiniones. Por su parte, a través del segundo ámbito no se cuestiona la restricción sobre el contenido, sino simplemente intervenciones arbitrarias sobre la forma, tiempo, lugar o medio de transmisión (Huerta Guerrero, 2010, p. 325).

La neutralidad de red, aun cuando se ha justificado principalmente para garantizar la protección del pluralismo de contenidos, también opera asumiendo una tutela 'neutra' de los medios de transmisión. Recordemos que, conforme a la neutralidad de red, debe garantizarse el éxito del mero acto de transmisión de señales en el ciberespacio, sin que sea importante el contenido que este transmita. Será indiferente para que se active la protección de esta política pública que el contenido realmente promueva o no algún factor de interés público.

Esta visión es consistente con el panorama de la Unión Europea, realidad desde la cual se ha tomado prestada la noción de la neutralidad de red como garante de la libertad de expresión. A pesar del silencio *prima facie* que mantienen el artículo 10 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950) y el artículo 11 de la Carta de los Derechos Fundamentales de la Unión Europea (2000) en relación con la protección de las 'formas' o 'medios' de expresión, Belli y Van Dijk interpretan que, dado que la jurisprudencia atribuye la cobertura más amplia, el mero acto de transmisión debería estar dentro del alcance (2016, p. 23; 2006, p. 783). También en Europa, De Hert y Kloza plantearon una opinión similar y mencionaron, entre otros, los casos *Oberschlick c. Austria* (1991) y *De Haes y Gijsels c. Bélgica* (1992) –en los que el Tribunal Europeo de Derechos Humanos expresó que el artículo 10 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales no solo tutelaba la esencia de las ideas expresadas sino también la forma en que se transmiten– y el asunto Öztürk *c. Turquía* (1999) –en el que se argumentó que "cualquier restricción impuesta a los medios necesariamente interfiere con el derecho a recibir y difundir información" (2012, p. 8) [traducción libre][12]–.

Por lo anterior, el acto de transmisión de bits de los ISP (sin importar el mensaje que se transmita) es protegido por la neutralidad de red y debe ser garantizada su consecución como un elemento protegido por la libertad de expresión.

C. Arquitectura abierta

Para un sector importante de la literatura, el protocolo de tecnología que rige la transmisión de bits en la web se basa en una arquitectura abierta, conforme a la cual deben ser los usuarios quienes decidan e impulsen el crecimiento del internet (Murray, 2007, p. 70-74). Para el diseñador de este protocolo, Berners-Lee, la arquitectura abierta refleja también un enfoque filosófico: el ciberespacio debe ser un recurso universal, capaz de crecer de manera ilimitada y sin generar cuellos de botella o puntos de control (*gatekeepers*) (Lessig, 2001, p. 37).

Este principio de arquitectura abierta se conoce como 'Diseño de Extremo a Extremo' o *End-to-End*. Según este principio, la inteligencia de la red debe estar descentralizada y descansa en los usuarios finales (es decir, quienes se encargan de seleccionar los datos de los Proveedores de Contenido a los que quieren acceder), por lo que son ellos quienes deben ser la única fuente de control del destino de la comunicación en lugar de que lo haga el *gatekeeper* intermedio que se encuentra a lo largo de la ruta que toman los bits transmitidos (Saltzer *et al*., 1984, pp. 277-288). Para que la red funcione en toda su potencialidad y magnitud, el crecimiento debe fundarse en el reconocimiento del concepto de que los bienes digitales son comunes, creados bajo una lógica de compartición dirigida por los propios usuarios y sin ánimo de centralización bajo una única propiedad privada o pública intermedia. Si se dependiese de esos pocos propietarios intermedios, la rapidez del crecimiento de la red sería, se sostiene, carente de dinámica (Mackinnon, 2012, pp. 52-54),

[12] Texto original: "any restriction imposed on the means necessarily interferes with the right to receive and impart information".

Enfocarse en la inteligencia de los anfitriones finales para promover el crecimiento de la red bajo el principio *End-to-End*, como sugiere Lessig, implica que la red debe ser capaz de proveer el servicio a un nivel básico que consiste, exclusivamente, en garantizar la transmisión de la información desde y hacia esos usuarios finales (2001, p. 35). Y esta presunción, según Wu, puede ser traducida en la afirmación que "la red debe ser neutral para todas las aplicaciones" (2003, p. 146) [traducción libre][13]; de lo contrario, no se podrá asegurar la correcta transmisión de información y los puntos finales donde se encuentran los usuarios serán puestos en un segundo plano.

Así, bajo el principio *End-to-End*, se entiende que el usuario es el promotor del crecimiento de la red y tiene la posición exclusiva de decidir qué datos recibir (y cómo hacerlo), o lo que es lo mismo, una 'garantía total de transporte de bits'. Y, bajo esa premisa de arquitectura de red, se asume que el usuario tiene una autonomía absoluta en la decisión de contenidos a los que acceder, en ejercicio de su libertad de expresión, sin que el ISP pueda limitarla.

IV. ¿LA PROTECCIÓN DE LA LIBERTAD DE EXPRESIÓN ES REALMENTE UN FUNDAMENTO VÁLIDO PARA LA NEUTRALIDAD DE RED? UNA POLÍTICA PÚBLICA SOMETIDA A ESCRUTINIO

En esta sección, evaluaremos críticamente cada una de las razones esgrimidas en la sección III, con el fin de determinar si estas brindan bases adecuadas para sostener el papel esencial de la neutralidad de red en la ecuación de protección de la libertad de expresión en el ciberespacio.

A. ¿Realmente las medidas de gestión de tráfico en la red son una amenaza a la libertad de expresión? Cuando la anécdota se convierte en regulación

La neutralidad de red, como regla de protección *ex ante* de la libertad de expresión bajo un enfoque social, parte de una premisa clave: que las fuerzas del mercado no son confiables, porque las interacciones libres entre ISP privados y Proveedores de Contenido son propensas a restringir discursos y opiniones a través de las medidas de gestión de la red. En este contexto, las intervenciones precautorias serán preferibles en lugar de las respuestas *ex post*.

Sin embargo, es inevitable cuestionarnos esta premisa. Si el mercado de los ISP es un mercado competitivo (poco propenso a carecer de ella), entonces son bajos los incentivos para establecer medidas que sean poco populares ante los usuarios (como lo serían bloqueos o priorizaciones de contenidos contrarias a sus intereses). La competencia disciplina la probabilidad de medidas de gestión de tráfico que afecten al público del servicio. Esta comprobación es crucial, dado que si es baja la probabilidad de resultados perjudiciales contra los Proveedores de Contenido y estos resultados no han ocurrido de manera repetida, la teoría sostiene que adoptar una solución regulatoria preventiva –en la forma de las reglas *ex ante* de neutralidad de red– es cuestionable (Shavell, 1993; pp. 255-287; Hodges, 2015, p. 251).

La literatura y evidencia sugieren que es poco probable que haya un ambiente anticompetitivo en el segmento de las ISP. Esto ocurriría si hubiese factores concurrentes como escasez en la red, así como la falta de alternativas suficientes en el lado de la oferta (ISP) y una baja demanda insatisfecha que hace poco probable el crecimiento de proveedores en ese nicho. Sin embargo, este es un mercado en competencia, por lo que la presencia de ISP (actuales o potenciales) modera su funcionamiento.

En efecto, como Sunstein reconoce cuando explica la posición de quienes apoyan una intervención menos proactiva en el ciberespacio, la escasez ya no es un problema en un mundo de nuevas tecnologías (1994, pp. 1787-1788). A diferencia de otros sistemas de comunicación con tendencia monopólica en los que la red es manejada por una empresa dominante y donde otros operadores enfrentan limitaciones técnicas o económicas para duplicar el cuello de botella (Horwitz, 1991, pp. 27-29, 34), "[l]os ISP no operan en un monopolio natural. La competencia en la industria, pese a ser imperfecta, es real y está creciendo" (Ohlhausen, 2016, p. 149) [traducción libre][14]. A menos que surgiera un cuello de botella y la posición de un ISP no fuese replicable, estos no deberían estar sujetos a obligaciones de transporte universal, como se exige vía la neutralidad de red.

En el Perú, el regulador ha reconocido que los distintos mercados del sector de telecomunicaciones, incluyendo aquel en el que operan los ISP, han presentado "ganancias en competencia" y un "incremento en los niveles de intensidad competitiva", tras ponderar mejoras en indicadores como

[13] Texto original: "networks should be neutral as among applications".

[14] Texto original: "ISPs do not operate in a natural monopoly. Competition in the industry, though imperfect, is real and growing".

precio, calidad, usuarios y concentración de mercado (Organismo Supervisor de Inversión Privada en Telecomunicaciones [Osiptel], 2018). Es de público conocimiento lo dinámico de la competencia en el segmento de internet móvil y empresarial, por lo cual existe una importante rivalidad entre los distintos ISP de ese rubro. Por su parte, si bien a la fecha de redacción de este artículo se aprecia un alto nivel de concentración en el servicio de internet residencial entre los dos principales operadores (Movistar y Claro), también es cierto que se viene produciendo una penetración exponencial de operadores que, principalmente, recurren a conexiones satelitales y de fibra óptica de gran velocidad para ir ganando terreno en el mercado (Semana Económica, 2019). De hecho, nuevos jugadores como Win, Ultra, Fiberlux y Gpon ya comenzaron a quitarle participación a los dos agentes tradicionales en Lima y buscan ampliar su cobertura agresivamente hacia otras ciudades (Semana Económica, 2021). Esta situación, sumada al hecho que existe aún una muy baja tasa de usuarios del servicio de Internet fijo –se estima que solo 7 de cada 100 peruanos lo tienen en sus hogares, según cifras oficiales difundidas por El Comercio (2020)–, muestran una demanda desatendida que da las condiciones adecuadas para el crecimiento de la oferta y una aún más intensa competencia.

Si prestamos atención a lo que sucede en otras latitudes, la evidencia reafirma la competitividad del segmento de ISP y, por tanto, la poca (o casi nula) probabilidad de que un agente dominante incurra en prácticas de gestión de tráfico indebidas, pues la competencia lo disciplina.

Por ejemplo, el mercado de los ISP en Europa –una de las realidades con la regulación más estricta en materia de neutralidad de red– muestra un comportamiento competitivo saludable, sin condiciones estructurales que impidan el acceso o permanencia de operadores. Aunque se argumenta que los efectos de la agrupación y la red probablemente amenazarán la estructura del mercado de los ISP en el futuro (ISPreview, 2017), "el consumidor europeo promedio tiene una selección de varios proveedores de acceso" (Audibert & Murray, 2016, p. 126) [traducción libre][15]. En el Reino Unido, hasta el 7 de febrero de 2021 habían 212 ISPs (ISPreview, 2021). Un estudio conducido por Rebbeck y Yardley, reveló que el Reino Unido era el mercado de banda ancha fija más competitivo (se encontró una menor concentración del mercado y una disminución constante de los precios), mientras que, en el resto de los países europeos analizados, el índice de concentración (HHI) reveló mercados moderadamente concentrados con condiciones de competencia viables (2015, pp. 25, 33). Ver gráfico 2.

En Estados Unidos –país en el que el mercado de ISP está tradicionalmente más concentrado porque el servicio lo prestan los principales operadores de cable (Audibert & Murray, 2016, p. 126)–, se puede decir que existen presiones competitivas entre las empresas. Según los datos recopilados hasta diciembre de 2013, el Departamento de Comercio estadounidense encontró que, de las velocidades de descarga más populares en ese momento, "el 98% de la población tenía al menos dos opciones de ISP móviles y el 88% tenía dos o más ISP fijos disponibles para ello" (2014, p. 1) [traducción libre][16].

Gráfico 2

Fuente: Rebbeck & Yardley (2015)

[15] Texto original: "the average European consumer has a choice of several access providers".

[16] Texto original: "98 percent of the population had a choice of at least two mobile ISPs, and 88 percent had two or more fixed ISPs available to them".

Mientras que, en un informe del 2015 de la FCC, este regulador confirmó dichos números, añadiendo que los ISP han continuado actualizando y expandiendo sus redes (p. 65).

Las voces opositoras han afirmado que, a pesar del gran número de ISP, los consumidores no ejercen presiones competitivas sobre las decisiones anteriores y, por lo tanto, el mercado no puede prevenir prácticas de gestión de red que conduzcan a violaciones de la libertad de expresión. Cooper y Brown afirman que los consumidores tienen una capacidad limitada para cambiar de ISP porque desconocen qué significan estas medidas, enfrentan barreras de mercado y no están interesados en las políticas de gestión del tráfico (2015, p. 1). Sin embargo, incluso en tales condiciones, vale la pena mencionar la existencia de pocos incidentes de gestión de tráfico violatorios de la neutralidad de red en Perú, así como Europa y Estados Unidos, dos realidades que reportan, además, casos de poca escala, según relata Marcus (2016, p. 259).

En el Perú, por ejemplo, Morachimo Rodríguez da cuenta que en el 2009 –bajo la vigencia de una norma sectorial anterior al Reglamento (aunque de contenido similar)– el Organismo Supervisor de Inversión Privada en Telecomunicaciones (en adelante, Osiptel) sancionó a Telefónica del Perú por bloquear un puerto en un contexto de emergencia (2019, p. 4). Por su parte, el propio regulador de telecomunicaciones, en su portal oficial, difunde la existencia de un caso adicional, referido al bloqueo de puertos lógicos implementado por Claro en el periodo 2017-2018, que afectó el envío y/o recepción de correos entre servidores y generó problemas en la transferencia de archivos de manera remota desde terminales con el sistema operativo Windows de los usuarios (Osiptel, 2020). En suma, a la fecha de esta investigación (febrero de 2021), solo dos casos atestiguan la aplicación de gestiones de tráfico que ameritaron la sanción del regulador.

A nivel europeo, Marcus da cuenta de la aseveración de BEREC, organismo que aseguró que "muy pocas autoridades regulatorias nacionales han reportado incidentes relevantes respecto a la neutralidad de red [solo dos incidentes ninguno de los cuales requirió acción regulatoria explícita]" (2016, p. 266) [traducción libre][17], mientras que Belli resaltó que los usuarios afectados por algún tipo de restricción en la gestión del tráfico centraron sus cuestionamientos propiamente en bloqueos y no en otras prácticas prohibidas por la neutralidad de red, como la priorización de líneas y contenidos (2016, p. 22). May afirma que, por su parte, Estado Unidos ha experimentado una tendencia similar, porque "[a] excepción de algunos incidentes aislados y solucionados rápidamente", los ISP no han "bloqueado, impedido o restringido el acceso de los suscriptores a las aplicaciones de Internet o el contenido de entidades no afiliadas" (2007, p. 199) [traducción libre][18].

Como puede verse, las limitaciones a la libertad de expresión no han sido comunes en el ámbito de los ISP y "no es obvio que un ISP maximice las ganancias al comprometer el valor de su red al negar a los consumidores su contenido preferido" (Ohlhausen, 2016, p. 130) [traducción libre][19]. Esto probablemente explica por qué al discutir la introducción de neutralidad de red en Europa, se reconoció que "existe cierta incertidumbre acerca de si las disposiciones actuales [nos referimos a las disposiciones *antitrust* y de protección al consumidor] […] son suficientes para lidiar con el bloqueo de los servicios de la sociedad de la información" (Comisión de las Comunidades Europeas, 2007, p. 99). Las fuerzas del mercado, entonces, no han sido una limitación significativa y constante para la capacidad de transmitir bits a través del ciberespacio, poniendo en tela de juicio la necesidad de una regulación, que parece basarse en la anécdota. Ante incidentes aislados, bien puede acometerse la protección a través de herramientas de control *ex post* de conductas, canalizables a través de denuncias de competencia, de protección del usuario del servicio de telecomunicaciones o incluso vía demandas de amparo.

B. ¿La neutralidad de la red fomenta el pluralismo y otros valores democráticos?

De acuerdo con el enfoque social de la libertad de expresión, se requiere la intervención proactiva del gobierno en el mercado para alentar un mayor número de opiniones y discursos imparciales, ya que esta condición es un requisito previo para lograr el pluralismo de los medios, así como el compromiso democrático con los asuntos públicos (Sunstein, 1994, p. 1759-1760).

[17] Texto original: "BEREC noted as recently as June 2014 that "very few NRAs have reported specific relevant net neutrality incidents." BEREC noted only two incidents, neither of which required explicit regulatory action".

[18] Texto original: "Except for a few isolated and quickly remedied incidents, neither the cable operators nor the telephone companies providing broadband Internet services have yet blocked, impaired, or otherwise restricted subscriber access to Internet applications or the content of unaffiliated entities".

[19] Texto original: "It is not obvious that an ISP would maximize profit in compromising the value of its network by denying consumers their preferred content".

La neutralidad de red no implica la valoración de la naturaleza de los discursos afectados por la gestión del tráfico de ISP ni si dichas decisiones constituyen censuras por el contenido o se basan en un interés comercial (desvinculado del contenido o mensaje). Siendo ello así, la pregunta que surge es si el mero objetivo de tener más Proveedores de Contenido capaces de transmitir su contenido (sin importar de qué trate este) podría efectivamente llevar al pluralismo y potenciación de la deliberación democrática.

Este cuestionamiento arroja una respuesta dudosa y discutible en el mejor de los casos. El pluralismo, como acertadamente ha sido explicado en la literatura, se sostiene en que exista una variedad de los siguientes elementos: (i) propietarios o agentes que ejercen control, (ii) tipos y géneros de medios, (iii) puntos de vista políticos, (iv) expresiones culturales, e (v) intereses locales y regionales (Katholische Universität Leuven *et al*., 2009, p. 5). El pluralismo de opinión, además, depende de la situación de los Proveedores de Contenido en su relación con los actores políticos (High Level Group on Media Freedom and Pluralism, 2013, p. 13.), la representación justa y diversa que incluye puntos de vista e intereses de las minorías (Katholische Universität Leuven *et al*., 2009, p. 9), entre otros factores que van más allá de asegurar un mero mayor número de 'hablantes' cuya transmisión de su discurso sea garantizada. El pluralismo no puede depender exclusivamente de tener un mayor o menor número de Proveedores de Contenido cuyo mensaje tiene una garantía de transmisión bajo la neutralidad de red porque, como afirma Horwitz, concebir que el número de oradores refleja el compromiso con el pluralismo es inexacto (1991, p. 50).

En ese sentido, debe recordarse que, bajo el enfoque social de la libertad de expresión, la protección de lo transmitido dependerá de que contribuya a la formación de una opinión pública libre, lo que ha significado que, por ejemplo, el Tribunal Constitucional peruano (Expediente 2579-2003-HD/TC, 2004, párr. 6,) o su par español (Marciani Burgos, 2005, p. 357) proporcionen protección preferente siempre que el contenido lesionado abone al debate público.

Lamentablemente, la neutralidad de red no provee un marco legal para determinar si el discurso del Proveedor de Contenido que se ha visto afectado por la medida de gestión de tráfico implementada por la ISP se relaciona con asuntos de relevancia pública. Aun siendo un factor subjetivo, podría decirse que un contenido de relevancia será aquel capaz de incidir en los patrones de ignorancia o apatía y promover una toma decisión sobre asuntos públicos y de interés en la sociedad actual en oposición a contenidos que carecen de intención comunicativa (Baker, 1997, p. 319). No negamos que cada usuario es libre de elegir el contenido que desea consumir. Sin embargo, es indudable que, si el contenido elegido no contribuye a la deliberación pública, no tendría por qué tener un privilegio regulatorio y una garantía de transmisión a toda costa. En nuestra opinión, debería asumirse una visión menos estricta y pasarse de un sistema de prohibición *per se* de las medidas de gestión de tráfico a uno de revisión caso por caso, en el que se valide si el contenido tiene o no impacto sobre la deliberación pública, pluralismo y deliberación democrática, pues solo en ese supuesto podría evaluarse si corresponde privilegiarse al Proveedor de Contenido por sobre el ISP.

Por otro lado, incluso si se presumiera que el mayor número de Proveedores de Contenido resulta un factor relevante en sí mismo para la promoción de la formación la opinión pública, la investigación en el ámbito de las ciencias del comportamiento sugiere que la mayor cantidad de opciones tiende a crear marcos abrumadores que, al final del día, afectan la capacidad de las personas para ejercer su derecho a elegir. Es decir, se genera el efecto contrario. Gigerenzer y Gaissmaier identificaron situaciones en las que menos información conduce a decisiones más precisas con menos esfuerzo (2011, pp. 451-482). En la misma corriente, otros experimentos en el terreno conductual han probado que

> cuando los participantes se enfrentaron con dos docenas de opciones (en lugar de seis opciones), la situación fue abrumadora […] tener menos opciones para considerar podría ser menos abrumador, particularmente cuando las diferencias entre las opciones son triviales […] En este caso, más opciones no implicaban mayor voluntad o autonomía. (Lyengar & Leeper citados por Moller *et al*., 2006, p. 107) [traducción libre][20].

Es innegable que "los discursos en ejercicio de la libertad de expresión no pueden ser tratados como un simple *commodity"* (Sunstein, 1994, p. 1780) [traducción libre][21]. Sin embargo, no basta con ase-

[20] Texto original:
> when participants were confronted with two dozen options (rather than six options), the situation was overwhelming […] having fewer options to consider could be less overwhelming, particularly when the differences among the options are trivial […] In this case, more options did not imply greater volition or autonomy,

[21] Texto original: "speech should not be treated as a simple commodity".

gurar formalmente un mayor número de emisores en igualdad de condiciones para la transmisión de sus datos. La neutralidad de red no ofrece un marco para determinar si las decisiones de tráfico de los ISP han significado una amenaza para los diversos factores que verdaderamente dan forma al pluralismo y promueven el debate democrático, que es el sustento del enfoque social de la libertad de expresión.

C. Neutralidad de red: ¿una violación a los derechos fundamentales de los propios ISP?

Como explicamos, para algunos autores y bajo la aproximación europea, la protección otorgada por la libertad de expresión se extiende al mero acto de transmisión, lo que justifica que los bits deban viajar en el ciberespacio sin interrupciones, sin importar su contenido.

Al margen de la crítica sobre el escaso valor que esta premisa podría tener para la formación de la democracia y el interés público si el contenido transmitido no se relaciona con dichos valores, un punto de debate adicional radica en definir si la libertad de expresión realmente protege el mero acto de transmisión. Al respecto, ante la ausencia de trabajos y decisiones nacionales sobre el tema, resulta esclarecedor el trabajo de Benjamin en referencia a este tópico en los Estados Unidos, país con el *case law* quizás más prolífico sobre libertad de expresión.

Al desarrollar el alcance de la jurisprudencia de la Corte Suprema, Benjamin aclara que esta nunca ha sugerido la cobertura de la Primera Enmienda para el acto de transmisión de los bits o para todos los transmisores de voz. Así, explica Benjamin, esta Corte ha aplicado la Primera Enmienda solo a personas o empresas que hacen mucho más que simplemente transportar (2011, p. 1687). Esto ha sucedido, por ejemplo, en casos emblemáticos como el asunto *Turner Broad Sys. c. FCC* (1994), donde antes que protegerse a estos medios en su calidad de transmisores, su nivel de compromiso con el contenido editorial fue el aspecto relevante que los caracterizó como agentes protegidos por la Primera Enmienda; o en el caso *Rumsfeld c. Forum for Academic and Constitutional Rights, Inc.* (2006), en el que la Corte Suprema declaró que nunca ha sido materia de protección de la libertad de expresión o de prensa el solo hecho que la conducta cuestionada haya impactado sobre algún medio que transmite alguna forma de lenguaje (escrito, hablado o impreso), sino si la conducta incide sobre algún mensaje con contenido e intención comunicativa.

En tal sentido, Benjamin hace una analogía interesante para desacreditar el efecto que daría la mera protección del acto de transmisión de bits, por no comprobarse en él una intención comunicativa:

> Imagine que FedEx decidió acelerar la entrega de documentos dirigidos a compañías con las que tenía una relación comercial; es decir, FedEx otorgaría un tratamiento preferencial en su calendario de entrega a los documentos enviados a las compañías que pagaron por el privilegio. Una decisión del Congreso de prohibir tal práctica puede o no ser una buena política, pero no parece plantear problemas desde la Primera Enmienda […] Al decidir si una conducta particular posee suficientes elementos comunicativos para poner en juego la Primera Enmienda, debemos preguntarnos si 'había presente una intención de transmitir un mensaje particularizado […] el transporte no discriminatorio de una empresa (de bits o cualquier otra cosa) permite la comunicación, pero no tiene contenido, y por lo tanto no expresa ideas (2011, p. 1686-1695) [traducción libre][22].

No obstante, asumiendo que la libertad de expresión otorga una garantía sobre el mero acto de transmisión y que, en aplicación de ello, la neutralidad de red protege el transporte de bits, no debe perderse de vista que el ISP también tendría derechos en juego que se ven afectados si se le prohíbe decidir a qué Proveedor de Contenido privilegiar frente a otro.

De hecho, se vería impactada su propia libertad de expresión para elegir los contenidos que difunde, pues el ISP no es sino un agente en un estatus similar a un diario, que decide en ejercicio legítimo de su libertad editorial qué noticia difundir y qué columna publicar. Por lo tanto, aplicando de manera analógica el razonamiento de la Corte Suprema de los Estados Unidos establecido en el caso *Miami Herald Publishing Company c. Tornillo* (1974), en el que sostuvo que ninguna disposición legal puede obligar a los periódicos privados a incluir un contenido en sus publicaciones, la neutralidad de red

[22] Texto original:

> Imagine that FedEx decided to speed up the delivery of documents addressed to companies with which it had a financial relationship; that is, FedEx would give preferential treatment in its delivery schedule to documents sent to companies that paid it for the privilege. A congressional decision to ban such a practice may or may not be good policy, but it would not seem to raise First Amendment issue […] In deciding whether particular conduct possesses sufficient communicative elements to bring the First Amendment into play, we have asked whether '[a]n intent to convey a particularized message was present. […] a company's nondiscriminatory transportation (of bits or anything else) enable.

impone directamente una carga sobre este derecho editorial, que es manifestación de la libertad de expresión del ISP.

En suma, al exigirse, vía la aplicación de neutralidad de red, que un ISP transmita información o contenidos que comercialmente preferiría no priorizar, se "puede afectar la libertad de expresión del ISP para impartir información a los usuarios finales" (Sluijs, 2012, p. 521) [traducción libre][23]. En nuestra opinión, acogemos lo dicho por McDowell, quien, advirtiendo sobre la aplicación de la neutralidad de red, la calificó como una "extralimitación […] que también violaría la prohibición de la Primera Enmienda que prohíbe la difusión de un discurso ordenado o forzado por el Estado, convirtiéndose en la otra cara de la censura" (2014, p. 13) [traducción libre][24].

Pero, además, debe recordarse que los ISP, en el contexto de la gestión de tráfico, ejercen su libertad de empresa y de contratación, y su derecho de propiedad. La gestión de tráfico es una decisión inspirada en razones comerciales, como lo sería la decisión de establecer una priorización de contenidos (*e.g*., basados en un convenio que privilegia el ancho de banda para contenido de Netflix sobre el de Amazon Prime) o programas de *zero-rating* (*e.g*., el acceso sin costo a la plataforma educativa 'Aprendo en Casa' o a 'Discover' de Facebook, como parte de una estrategia de responsabilidad social en pandemia) (Villena, 2020). En nuestra opinión, mantener la premisa que cualquier gestión de tráfico que discrimine en el acto de transmisión de bits debe ser protegida a toda costa y prohibida bajo la neutralidad de red, implicaría asumir una suerte de protección preferente al derecho de los Proveedores de Contenido por sobre los ISP, quienes también son titulares de otros derechos fundamentales en juego. Conceder un sistema de protección preferente, como critica Marciani, es cuando menos discutible, porque el sistema nacional no establece tal jerarquía y propone un sistema de ponderación entre derechos fundamentales (2005). En ese sentido, nuevamente se debe sugerir que en lugar de asumir una regla dura de prohibición *per se* de las medidas de gestión de tráfico, se evalúe según el caso concreto, pues las señales del caso nos demostrarán si conviene limitar derechos de libertad de expresión y derechos fundamentales económicos del ISP considerando el impacto adverso sobre la deliberación pública que genera su decisión de gestión de tráfico.

Finalmente, creemos importante recordar que no todas las medidas de gestión de tráfico son iguales y, por consiguiente, es discutible que en todos los casos produzcan lesiones al supuesto derecho a transmitir bits. Un bloqueo no es similar a una priorización entre Proveedores de Contenido, por ejemplo, porque en este último caso el discurso no es bloqueado, solo retrasado (siendo finalmente accesible). Así, nos alineamos a lo ya desarrollado por el Tribunal Europeo de Derechos Humanos, que ha argumentado en el asunto *Appleby c. Reino Unido* (2003) que solo las prohibiciones completas en lugar de las interferencias parciales de entidades privadas pueden considerarse una violación a la libertad de expresión. En ese caso, la corte declaró que las obligaciones positivas sobre la propiedad privada deben ser proporcionadas y, dado que existía la capacidad de los Proveedores de Contenido para utilizar medios alternativos, no se produjo una violación.

Tendemos a apoyar esta posición y, por lo tanto, opinamos que las medidas de gestión de tráfico calificadas en nuestro Reglamento como "arbitrarias" no pueden desafiar por sí solas la libertad de expresión como lo alega la fórmula de neutralidad de red, dado que el Proveedor de Contenido –salvo que enfrente una censura absoluta– sigue siendo capaz de comunicar su mensaje. Siguiendo a Sluijs, en la evaluación de los conflictos entre la libertad de expresión y los derechos de las partes privadas (como los ISP), se debe tener en cuenta el justo equilibrio que debe lograrse entre el interés general de la comunidad y los intereses de los propios IPS. Por lo tanto, una restricción no sería nociva siquiera a la libertad de expresión del Proveedor de Contenido si frente al acto de gestión de tráfico de un ISP existen alternativas para que el Proveedor de Contenido difunda sus mensajes en internet (2012, p. 513).

Por lo anterior, somos de la opinión que es discutible que la libertad de expresión esté en juego en el mero acto de transmisión de bits o que siquiera esté restringida si la medida de gestión de tráfico no consiste en un bloqueo. Pero, en cualquier caso, de estarlo, este mismo derecho a la libertad de expresión también ampara al ISP –quien tiene un derecho editorial a decidir qué contenidos difunde y/o privilegia sobre otros–, contando además este ISP con derechos fundamentales económicos tales como la libertad de contratación, libertad de empresa y propiedad. Esto sugiere un análisis caso

[23] Texto original: "end-users or CSPs might be impeded in their freedom of expression because of a particular form of network management by an ISP".

[24] Texto original: "overreach […]. It would also violate the First Amendment's prohibition against state-mandated, or forced, speech -- the flip side of censorship".

por caso en lugar de una fórmula absoluta como la de la neutralidad de red.

D. La arquitectura abierta en juego

El principio *End-to-End* es una noción técnica y filosófica que se le atribuye al internet. Como explicamos, los defensores de este principio sostienen que, por su propia naturaleza, la inteligencia de la red reside en sus puntos finales y no se puede deber a una administración centralizada. De hecho, se afirma que la libertad de la red está integrada en su propia existencia y es bajo este principio que el concepto de neutralidad de red ha sido construido.

No obstante, la arquitectura de extremo a extremo no es un principio del cual dependa la existencia de la red. De hecho, como lo explica Marsden (2009) el internet se inició sin un modelo de arquitectura abierta. Internet fue "una creación de gobiernos e instituciones educativas, y continúa siendo regulada por el gobierno […] No hay un sesgo inherente hacia la apertura o el cierre de la red que no pueda deshacerse" (Marsden, 2009, p. 22) [traducción libre][25].

Como lo explican técnicamente Calvert y sus coautores, las condiciones de acceso actuales al internet residencial o móvil revelan que es falsa la premisa según la cual los puntos finales de la red (usuarios) son los inteligentes, puesto que estos puntos finales presentan problemas incrementales y requieren monitoreo de otros agentes (2007). Los puntos finales deben ser configurados para garantizar la interoperabilidad y sus usuarios carecen de sofisticación técnica y no pueden distinguir si el problema de acceso responde a un defecto en su computadora, el Wireless Point, el *router*, el ISP o el *website*, lo que hace necesario un sistema de manejo que recaiga en puntos intermedios. En esta línea es que la literatura anota que siempre ha habido gestión del tráfico de varios tipos en internet, siendo el aseguramiento de la calidad de servicios en internet una finalidad a priorizar que requiere servicios robustos que dependen de puntos intermedios (Sandvig & Crowcroft citados por Marsden, 2009, p. 25). Asimismo, Marcus apoya la idea que la gestión de tráfico está fuertemente vinculada a la existencia de las actividades en internet por encima del propio principio de extremo a extremo, siendo que "la priorización de envío siempre estuvo presente en el Protocolo de Internet […] El trabajo en la entrega de tráfico priorizada […] tiene una rica tradición con raíces que se remontan a los primeros días de internet" (2016, pp. 264-265) [traducción libre][26]. Estos primeros días, como explicamos, fueron manejados por agentes intermedios públicos, sin que la inteligencia de la red recayese en los puntos finales.

Actualmente, internet está "abrumadoramente manejado privadamente" (Lessig, 2001, p. 26) [traducción libre][27] y no manejado públicamente, como ocurrió en sus comienzos. De todos modos, esto no significa que la arquitectura abierta esté en su plenitud. La larga tradición de medidas de tráfico y el estado cada vez más congestionado de la red apoya el escrutinio de los méritos de la neutralidad de red y lleva a evaluar si se debe otorgar más confianza en los puntos intermedios de la red (ISP), a fin de que esta red opere bajo una interconexión dinámica y de calidad (Hahn & Litan, 2003).

V. CONCLUSIONES

Es más que obvio que los ISP deben ser supervisados en su manejo de la red, pues sería ingenuo asumir que el poder privado no puede conducir a distorsiones de la libertad de expresión, en tanto controlan los medios a través de los cuales los mensajes viajan en el ciberespacio. Pese a ello, lo que debemos preguntarnos no es sobre la capacidad de los ISP para socavar la libertad de expresión, sino si realmente constituyen una amenaza importante para esta y si la neutralidad de red cumple su función social de promover la democracia y valores deliberativos.

En lugar de encontrarse apoyada en evidencia de limitaciones recurrentes malintencionadas y graves en la transmisión de información, el principio de neutralidad de red se basa en una asunción ideológica de precaución y en la creencia de una arquitectura abierta que, como explicamos, es un concepto que debe revisitarse en una red manejada por entidades privadas, que también tienen un control editorial de los bits que transmiten y derechos como el de propiedad y libertad de empresa y contratación. Si asumimos que toda práctica de gestión de red de los ISP –como lo hace el Reglamento– está prohibida, no podríamos "reconocer el punto económico fundamental que la mayoría de las relaciones contractuales verticales benefician a los consumidores", de acuerdo con Wright

[25] Texto original: "creation of governments and educational institutions, and continues to be regulated by government, […]. There is no inherent bias towards openness or closure of the network that cannot be undone by critical decisions at this juncture".

[26] Texto original: "Prioritized delivery was always envisioned as part of the Internet Protocol […] Work on prioritized traffic delivery over IP has a rich tradition with roots going back to the earliest days of the Internet".

[27] Texto original: "overwhelmingly handled privately".

(2014, pp. 9-10). El perjuicio tiende a ser improbable porque como sostienen Palazuelos y Herrera, los derechos de los usuarios son consistentes con los intereses de los ISP, pues estos últimos no tienen incentivos para impedir a los primeros el acceso al mayor número de información y servicios, si eso es lo que el mercado demanda (2010, p. 11).

Los mercados regularmente florecen pese a la existencia de acuerdos de integración vertical, como lo serían los acuerdos entre ISP con Proveedores de Contenido. Esa es la premisa de la Ley de libre competencia peruana, que no prohíbe de forma absoluta los acuerdos verticales, por lo que establece solo una sanción relativa ante este tipo de conductas y siempre que se verifique ausencia de justificación y que el efecto perjudicial supere a los beneficios (Decreto Supremo 030-2019-PCM, 2019, art. 12). Siendo ello así, en lugar de un sistema de prohibición *ex ante* y *per se* como el de neutralidad de red, parece más aconsejable un sistema de control *ex post* y caso por caso, que bien podría ser proporcionado por el sistema de control antimonopólico o de protección al consumidor; o, si la violación es probadamente intensa sobre un contenido de valor para la opinión pública, a través de la vía judicial constitucional y tras llevar a cabo un ejercicio de ponderación entre los derechos del ISP y el Proveedor de Contenido, y los usuarios.

Aun cuando algunos autores sostienen que la inmediatez que proporciona la intervención regulatoria *ex ante* bajo el principio de neutralidad de red es preferible frente a la intervención *ex post* que requiere largos litigios para ser aplicada (Economides citado por Albert Márquez, 2018, p. 79), debe notarse que esa perspectiva pierde de vista que en estos litigios es posible obtener medidas cautelares precautorias. Nuestra opinión, en esa línea, es que es aconsejable un enfoque más indulgente respecto a prácticas de gestión de tráfico como la priorización, dado que las decisiones comerciales de los ISP no impiden por completo la libertad de expresión de los usuarios finales y de los Proveedores de Contenido, en la medida en que no bloquean completamente la transmisión.

Comparar, bajo un concienzudo Análisis de Impacto Regulatorio (RIA), la idoneidad de las obligaciones normativas de la neutralidad de red frente al valor que otorgan las intervenciones *ex post*, sería una opción de política regulatoria que las autoridades deberían acometer. Como señala Stylianou,

> la premisa más básica de la regulación es que las reglas de aplicabilidad general, como las de neutralidad de la red, deben reservarse únicamente para un daño generalizado lo suficientemente significativo como para justificar el costo inevitable que viene con la regulación (2017) [traducción libre][28].

En ese sentido, si se tienen solo casos anecdóticos y la estructura del mercado no justifica una intervención preventiva, controles de conducta con la habilidad de imponer medidas precautorias según el caso, en lugar de la prohibición absoluta vía la neutralidad de red, resultan instrumentos de intervención más aconsejables.

REFERENCIAS

Adamson, G. (2002). Internet Future: A Public Good or Profit Centre? *Science and Culture*, *11*(2), 257-275. https://doi.org/10.1080/09505430220137270

Albert Márquez, J. (2018). El Principio de Neutralidad en Internet. Una Aportación a la Libertad de Comunicación en Internet desde el Pensamiento de Francisco de Vitoria. *Estudios de Deusto*, *66*(2), 71-103.

Audibert, L., & Murray, A. (2016). A Principled Approach to Net Neutrality. *Escripted*, *13*(2), 119-143. http://dx.doi.org/10.2966/scrip. 130216.118

Baker, E. (1997). Giving the Audience What It Wants. *Ohio State Law Journal*, (58), 313-417.

Balkin, J. (2008). The Future of Free Expression in a Digital Age. *Pepperdine Law Review,* (36), 427-444.

Becker, G., Carlton, D., & Sider, H. (2010). Net Neutrality and Consumer Welfare. *Journal of Competition Law and Economics*, *6*(3), 497-519.

Belli, L. (2016). End-to-End, Net Neutrality and Human Rights. En L. Belli & P. De Filippi (eds.), *Net Neutrality Compendium* (pp. 13-29). Springer International Publishing.

Benjamin, S. (2011). Transmitting, Editing, and Communicating: Determining What 'The Freedom of Speech' Encompasses. *Duke Law Journal*, (60), 1673-1713.

[28] Texto original: "the most basic premise of regulation is that rules of general applicability, like the ones on net neutrality, should be reserved only for generalised harm significant enough to justify the unavoidable cost that comes with regulation".

Body of European Regulators for Electronic Communications [BEREC] (2015) *What is Traffic Management and What is "Equal Treatment"*?. https://BEREC.europa.eu/eng/netneutrality/traffic_management/

(2016). *Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*. https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6160-berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules

Brouwer, D. (2017). *Zero-rating and net neutrality in the European Union. What legal should the EU legislator adopt with respect to zero-rating offers where applications do not count towards the data cap of the consumer* (tesis de maestría). Universidad de Tilburg University, Países Bajos.

Calver, K., Edwards, W., & Grinter, R. (2007). *Moving Toward the Middle: The Case Against the End-to-End Argument in Home Networking*. https://www.cc.gatech.edu/~keith/pubs/hotnets07-end-to-end.pdf

Castillo-Córdova, L. (2006). Las Libertades de Expresión e Información como Derechos Humanos. En L. Castillo-Córdova (coord.), *Las libertades de expresión e información: Primeras Jornadas sobre Derechos Humanos*. Palestra Editores.

Cerf, V. (2012) Internet Access is not a Human Right. *The New York Times*. http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html?_r=1

Chalmers, D., & Trotter, S. (2016). Fundamental Rights and Legal Wrongs: The Two Sides of the Same EU Coin. *European Law Journal*, *22*(1), 9-39. https://doi.org/10.1111/eulj.12168

Cooper, A., & Brown, I. (2015). Net Neutrality: Discrimination, Competition, and Innovation in the UK and US. *Transactions on Internet Technology*, *15*(1), 1-21.

De Hert, P., & Kloza, D. (2012). Internet (access) as a new fundamental right. Inflating the current rights framework? *European Journal of Law and Technology*, (3).

Departamento de Comercio de los Estados Unidos (2014). *Competition Among US Broadband Service Providers.* https://www.researchgate.net/publication/288831808_Competition_Among_US_Broadband_Service_Providers

Doverspike, R., Ramakrishnan, K., & Chase, C. (2010). Structural Overview of ISP Networks. En C.R. Kalmanek, S. Misra & Y. R. Yang, (eds.), *Guide to Reliable Internet Services and Applications* (pp. 19-93). Springer-Verlag.

El Comercio (25 de febrero de 2020). *¿Está perjudicialmente concentrado el mercado de Internet fijo en el Perú?* https://elcomercio.pe/economia/dia-1/internet-fijo-en-el-peru-esta-perjudicialmente-concentrado-el-mercado-osiptel-operadores-movistar-claro-entel-noticia/.

Comisión Federal de Comunicaciones (2015). *2015 Broadband Progress Report and Notice of Inquiry on Immediate Action to Accelerate Deployment*. https://www.fcc.gov/reports-research/reports/broadband-progress-reports/2015-broadband-progress-report

(2017). *Restoring Internet Freedom Order*. https://www.fcc.gov/document/fcc-releases-restoring-internet-freedom-order

Free Press (2019). Save the Internet. Net Neutrality: What You Need to Know Now. *Free Press.* https://www.freepress.net/issues/free-open-internet/net-neutrality/net-neutrality-what-you-need-know-now

Fung, B. (2017) This Poll Gave Americans a Detailed Case for and Against the FCC's Net Neutrality Plan. The Reaction Among Republicans was Striking. *The Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2017/12/12/this-poll-gave-americans-a-detailed-case-for-and-against-the-fccs-net-neutrality-plan-the-reaction-among-republicans-was-striking/.

Gigerenzer, G., & Gaissmaier, W. (2011). Heuristic Decision Making. *Annual Review of Psychology*, (62), 451–482.

Hahn, R., & Litan, R. (2003). *The Myth of Network Neutrality and What We Should Do About it*. https://www.brookings.edu/wp-content/uploads/2016/06/200611.pdf.

Hahn, R., & Wallsten, S. (2006) The Economics of Net Neutrality. *Economists' Voice*.

Harris, A (2016). Net Neutrality and Its Potential Impact on Free Speech. *Czasopismo-Prawno-Historyczne*, (68), 223-235.

High Level Group on Media Freedom and Pluralism (2013). *A Free and Pluralistic Media to Sustain European Democracy*. https://wayback.archive-it.org/12090/20210108153846/https://ec.europa.eu/digital-single-market/en/high-level-group-media-freedom-and-pluralism

Hodges, C. (2015). Responsive, Meta and Compliance Theories. En *Law and Corporate Behaviour. Integrating Theories of Regulation, Enforcement, Compliance and Ethics* (pp. 241-256). Bloomsbury Publishing.

Horwitz, R. (1991). The First Amendment Meets Some New Technologies: Broadcasting, Common Carriers, and Free Speech in the 1990s'. *Theory and Society*, (20), 21-72.

Hudson, D. (2018). In the Age of Social Media, Expand the Reach of the First Amendment. *Human Rights Magazine of the American Bar Association*, *43*(4).

Huerta Guerrero, L. (2010). Libertad de expresión: fundamentos y límites a su ejercicio. *Pensamiento Constitucional*, *14*(14), 319-344.

ISPreview (2017). Report Calls for More Competition in the UK Fixed Line Broadband ISP Market. https://www.ispreview.co.uk/index.php/2017/10/report-calls-competition-uk-fixed-line-broadband-isp-market.html.

(2021). UK ISP Listing. https://www.ispreview.co.uk/isp_list/index.php.

Jordan, S. (2007). A Layered Network Approach to Net Neutrality. *International Journal of Communication,* (1), 427-460.

Koops, B-J., & Sluijs, J. (2012). Network Neutrality and Privacy According to Art.8 ECHR. *European Journal of Law and Technology*, *2*(3) 1-23.

Kreimer, S. (2006). Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link. *University of Pennsylvania Law Review*, *155*(11), 11-101.

Katholische Universität Leuven – ICRI, Central European University – CMCS, Jönköping International Business School – MMTC y Ernst & Young Consultancy Belgium (2009). *Independent Study on Indicators for Media Pluralism in the Member States – Towards a Risk-Based Approach. Report prepared for the European Commission Directorate-General Information Society and Media*. https://www.rcmediafreedom.eu/Publications/Reports/Independent-Study-on-Indicators-for-Media-Pluralism-in-the-Member-States-Towards-a-Risk-Based-Approach

Lessig, L. (2001). The Future of Ideas. *The Fate of the Commons in a Connected World*. Random House.

London School of Economics (2011). *Net Neutrality: The First Amendment of the Internet.* https://core.ac.uk/download/pdf/221873.pdf.

Lyons, D. (10 de mayo de 2017) The First Amendment Red Herring in the Net Neutrality Debate. *Forbes.* https://www.forbes.com/sites/washingtonbytes/2017/03/10/the-first-amendment-red-herring-in-the-net-neutrality-debate/?sh=63add81326ae.

Mackinnon, R. (2012). *No sin nuestro consentimiento. La lucha mundial por la libertad en internet* (Javier San Julián, trad.). Ediciones Deusto.

Marciani Burgos, B. (2005). La posición preferente del derecho a la libertad de expresión: un análisis crítico de sus fundamentos. *Pensamiento Constitucional*, *11*(11), 351-378.

Marcus, S. (2016). New Network Neutrality Rules in Europe: Comparisons to those in the US. *Colorado Tech Law Journal*, 14(2), 259-280.

Marsden, A. (2009). *Net Neutrality: Towards a Co-Regulatory Solution*. Bloomsbury Academic.

May, R. (2007). Neutrality Mandates: Neutering the First Amendment in the Digital Age. *I/S: A Journal of Law and Policy for the Information Society*, *3*(1), 197-210.

McDowell, R. (28 de agosto de 2014). Net Neutrality Vs. Free Speech. *Wall Street Journal, Eastern Edition*, A13.

Mendoza Escalante, M. (2005). La eficacia de los derechos fundamentales en las relaciones entre particulares. *Pensamiento Constitucional,* (11), 219-271.

Ministerio de Transportes y Comunicaciones (2013). *Matriz de comentarios al proyecto de Decreto Supremo que aprueba el reglamento de la Ley N°29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica*. https://portal.mtc.gob.pe/comunicaciones/regulacion_internacional/regulacion/documentos/servicios_publicos/Matriz_comentarios_Proyecto_Decreto_Supremo_Reglamento__Ley_29904.pdf

Moller, A., Ryan, R., & Deci, E. (2006). Self-Determination Theory and Public Policy: Improving the Quality of Consumer Decisions without Using Coercion. *Journal of Public Policy & Marketing*, *25*(1), 104-116. https://doi.org/10.1509%2Fjppm.25.1.104

Morachimo Rodríguez, M. (2016). Buscando las Raíces Constitucionales de las Normas sobre la Neutralidad de red. *Gaceta Constitucional y Procesal Constitucional*, (99), 243-252.

(2017). ¿Qué Significa el Reglamento de Neutralidad de red? *Gaceta Constitucional* (110), 250-252.

(2019). *Neutralidad de Red y Libertad de Expresión en Perú.* https://www.mom-rsf.org/uploads/tx_lfrogmom/documents/Neutralidad_de_Red_y_Libertad_de_Expresion_en_Peru__1_.pdf.

Murray, A. (2007). *The Regulation of Cyberspace: Control in the Online Environment*. Routledge-Cavendish.

Nunziato, D. (2009). *Virtual Freedom. Net Neutrality and Free Speech in the Internet* Age. Stanford University Press.

Office of Communications [OFCOM] (2013). *A guide to internet traffic management*. https://www.ofcom.org.uk/__data/assets/pdf_file/0012/6042/traffic.pdf.

Ohlhausen, M. (2016). Antitrust over Net Neutrality: Why We Should Take Competition in Broadband Seriously. *Colorado Tech Law Journal*, *15*(1), 119-150.

Organización para la Cooperación y el Desarrollo Económicos [OCDE] (2007). *Internet Traffic Prioritisation. An Overview.* https://www.oecd.org/sti/ieconomy/38405781.pdf

Organismo Supervisor de Inversión Privada en Telecomunicaciones [Osiptel] (2018). *Evolución de la Industria de Telecomunicaciones e Intensidad Competitiva*. https://repositorio.osiptel.gob.pe/bitstream/handle/20.500.12630/96/ppt-indicadores-telecom-intensidad-mayo-2018.pdf?sequence=1&isAllowed=y.

(2020). *Osiptel sanciona a Claro y Entel por infringir reglamentos de calidad de los servicios de telecomunicaciones y neutralidad de red.* https://www.gob.pe/institucion/osiptel/noticias/212193-osiptel-sanciona-a-claro-y-entel-por-infringir-reglamentos-de-calidad-de-los-servicios-de-telecomunicaciones-y-neutralidad-de-red.

(2021) *Neutralidad de Red*. https://www.osiptel.gob.pe/portal-de-operadoras/regulacion/neutralidad-de-red/.

Palazuelos, M., & Herrera, F. (2010). La neutralidad de red. Un debate interesado sobre los derechos de los usuarios. *TELOS, Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad,* (82), *18-30.*

Pew Research Center (2012). *Social Networking Popular Across Globe. Arab Publics Most Likely to Express Political Views Online*. http://www.pewglobal.org/2012/12/12/social-networking-popular-across-globe/.

Rebbeck, T., & Yardley, M. (2015). *Report for BT. International Benchmarking Report*. Mason Consultant https://www.mynewsdesk.com/uk/bt/documents/analysys-mason-international-benchmarking-report-49119

Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (2013). *Informe Anual 2012* (OEA/Ser.L/V/II.149. Doc. 50). http://www.oas.org/es/cidh/expresion/docs/informes/anuales/Informe%20Anual%202012.pdf

Saltzer, J., Reed, D., & Clark, D. (1984). End-to-end arguments in system design. *ACM Transactions on Computer Systems*, *2*(4), 277-288.

Saunders, J., McClure, C., & Mandel, L. (2012). Broadband applications: Categories, requirements, and future frameworks. *First Monday, 17*(11). https://doi.org/10.5210/fm.v17i11.4066

Semana Económica (2019). Internet en hogares: nuevos jugadores apuestan por la conectividad para sumar más clientes. https://semanaeconomica.com/sectores-empresas/telecomunicaciones/375112-internet-en-hogares-nuevos-jugadores-apuestan-por-la-conectividad-para-sumar-mas-clientes.

(2021). Internet en hogar: nuevos jugadores comienzan a ganar peso en este segmento. https://semanaeconomica.com/sectores-empresas/telecomunicaciones/internet-en-hogar-jugadores-de-fibra-comienzan-a-apoderarse-del-mercado

Shatz, G. (11 de enero de 2017). This is Why the Internet is Broken: A Technical Perspective on Net-Neutrality. *TechTalks*. https://bdtechtalks.com/2017/01/11/this-is-why-the-internet-is-broken-a-technical-perspective-on-net-neutrality/.

Shavell, S. (1993). The Optimal Structure of Law Enforcement. *Journal of Law and Economics*, *36*(1), 255-287.

Shuler, R. (2002). *How Does the Internet Work?* https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm.

Sluijs, J. (2012). From Competition to Freedom of Expression: Introducing Article 10 ECHR in the European Network Neutrality Debate. *Human Rights Law Review, 12*(3), 509-554. https://doi.org/10.1093/hrlr/ngs015

Stylianou, K. (2017). The End of Net Neutrality is not the End of the Open Internet. *LSE Business Review*. http://blogs.lse.ac.uk/businessreview/2017/07/29/the-end-of-net-neutrality-is-not-the-end-of-the-open-internet/.

Sunstein, C. (1994). The First Amendment in Cyberspace. *Yale Law Journal*, (104), 1757-1804.

The Guardian (29 de julio de 2016) Internet Access is Now a Human Right: part 1 - Chips with Everything tech podcast. *The Guardian*. https://www.theguardian.com/technology/audio/2016/jul/29/internet-access-human-right-tech-podcast.

Van Dijk, P. (2006). Freedom of Expression. En P. Van Dijk, F. Van Hoof, A. Van Rijn & L. Zwaak (eds.), *Theory and Practice of the European Convention on Human Rights* (4ta ed.). Intersentia.

Villena, D. (2017). La Trascendencia Constitucional de la Neutralidad de red. *THĒMIS-Revista de Derecho*, (70), 223-246.

(12 de mayo de 2020). Pandemia y Neutralidad de Red. *Hiperderecho*. https://hiperderecho.org/2020/05/pandemia-y-neutralidad-de-red/.

Wu, T. (2003). Network Neutrality, Broadband Discrimination. *Journal on Telecomm & High Technology Law*, (2), 141-179. https://dx.doi.org/10.2139/ssrn.388863

LEGISLACIÓN Y JURISPRUDENCIA NACIONAL E INTERNACIONAL

Appleby y otros c. Reino Unido, No. 44306/98, 2003-VI Eur. Ct. H.R (2003).

Carta de los Derechos Fundamentales de la Unión Europea, 7 de diciembre de 2000, 2000 O.J. (C 364) 01.

Caso C-70/10, Scarlet Extended c. Sabam, 2011 E.C.R. I-11959.

Caso C-360/10, Sabam c. Netlog, 2012 E.C.R. 85.

Constitución Política del Perú [Const.] (1993) (Perú).

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, 4 de noviembre de 1950, 213 U.N.T.S. 221.

De Haes and Gijsels c. Bélgica, No. 19983/92, 30 Eur. Ct. H.R 198 (ser. A) (1997).

Decreto Supremo 014-2013-MTC, Decreto supremo que aprueba el Reglamento de la Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica, Diario Oficial *El Peruano*, 4 de noviembre de 2013 (Perú).

Decreto Supremo 030-2019-PCM, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley de Represión de Conductas Anticompetitivas, Diario Oficial *El Peruano*, 19 de febrero de 2019 (Perú).

Ley 29904, Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica, Diario Oficial *El Peruano*, 20 de julio de 2012 (Perú).

Miami Herald Publishing Co. c. Tornillo, 418 U.S. 241 (1974).

Net Neutrality: Is Antitrust Law More Effective Than Regulation: Protecting Consumers and Innovation?: Audiencia ante el Subcomité sobre Reforma Regulatoria, Comercial y Antimonopolio del Comité Judicial de la Cámara de Representantes, 113er Congreso de los Estados Unidos (2014) (testimonio oral de Tim Wu, profesor de Derecho, Columbia Law School). https://www.govinfo.gov/content/pkg/CHRG-113hhrg88377/html/CHRG-113hhrg88377.htm

Net Neutrality: Is Antitrust Law More Effective Than Regulation: Protecting Consumers and Innovation?: Audiencia ante el Subcomité sobre Reforma Regulatoria, Comercial y Antimonopolio del Comité Judicial de la Cámara de Representantes, 113er Congreso de los Estados Unidos (2014) (testimonio oral de Joshua D. Wright, comisionado, Federal Trade Commission). https://www.govinfo.gov/content/pkg/CHRG-113hhrg88377/html/CHRG-113hhrg88377.htm

Oberschlick c. Austria (no. 1), 204 Eur. Ct. H.R. (ser. A) (1991).

Recomendación del Comité de Ministros a los Estados Miembros de la Unión Europea sobre medidas para promover el valor de servicio público de internet, CM/REC(2007)16 (7 nov. de 2007).

Recomendación 32 del Consejo de Derechos Humanos de la Organización de las Naciones Unidas sobre la promoción, protección y disfrute de los derechos humanos en internet, U.N. Doc. A/HRC/32/L.20 (27 de junio de 2016).

Resolución de Consejo Directivo 165-2016-CD-OSIPTEL que aprueba el Reglamento de Neutralidad en Red. Diario Oficial *El Peruano*, 15 de diciembre de 2016 (Perú).

Resumen de la evaluación de impacto - Documento que acompaña a la Propuesta de la Comisión de Directiva del Parlamento Europeo y del Consejo por la que se modifican las Directivas 2002/19/CE, 2002/20/CE y 2002/21/CE del Parlamento Europeo y del Consejo, SEC (2007) 1473 (13 nov., 2007).

Rumsfeld c. Forum for Academic and Institutional Rights, Inc., 547 U.S. 47 (2006).

Toxic Substances Control Act: Audiencias sobre la Sección 776 ante el Subcomité de Ambiente de la Comisión de Comercio, 94to Congreso de los Estados Unidos 343 (1975).

Tribunal Constitucional [T.C.], 6 de abril de 2004, sentencia recaída en el Expediente 2579-2003-HD/TC (Perú).

Tribunal Constitucional [T.C.], 26 de agosto de 2004, sentencia recaída en el Expediente 1848-2004-AA/TC (Perú).

Tribunal Constitucional [T.C.], 14 de agosto de 2018, sentencia recaída en el Expediente 01643-2014-PA/TC (Perú).

Turner Broadcasting c. Federal Communications Commission, 512 U.S. 622 (1994).

10.18800/themis.202101.004

LA RETIRADA DE CONTENIDOS ILÍCITOS POR LOS PRESTADORES DE SERVICIOS EN LÍNEA

THE REMOVAL OF ILLEGAL CONTENT BY ONLINE SERVICE PROVIDERS

Lidia Moreno Blesa*
Universidad Complutense de Madrid

The irruption of the internet in a globalized world brings great advantages in the commercial and business sector. However, this new reality also has a strong social impact within the sphere of people's privacy, especially when it comes to social networks

This article explores the Judgement of Eva Glawischnig-Piesczek against Facebook Ireland Limited of the Court of Justice of the European Union case, in order to identify the extent to which online service providers are liable for illegal content that is shared on their websites. To accomplish this, the author debates if Facebook is a data hosting service provider to which the European Union regulations can be applied and what liability regime would be applicable to it for the broadcast of illegal content within their website. After that, she reviews the international judicial competence and the applicable law in the face of the violation of personal rights due to the dissemination of these contents. Finally, she reviews the territorial scope that an obligation to remove this type of content imposes.

Keywords: Internet; social media; Facebook; data hosting service providers; removal of illegal content.

La irrupción de internet en un mundo globalizado trae consigo grandes ventajas en el sector comercial y empresarial. No obstante, esta nueva realidad tiene también una fuerte repercusión social dentro del ámbito de la privacidad de las personas, en especial cuando se trata de redes sociales.

El análisis del presente artículo se enmarca en el caso Eva Glawischnig-Piesczek contra Facebook Ireland Limited del Tribunal de Justicia de la Unión Europea, con el fin de identificar hasta dónde llega la responsabilidad de los prestadores de servicios en línea por los contenidos ilícitos que se viertan en los sitios web que estos gestionan. En esta línea, la autora, define si Facebook es un prestador de servicio de alojamiento de datos al cual se le pueden aplicar las normas de la Unión Europea y qué régimen de responsabilidad es aplicable a estos servicios por la emisión de contenidos ilícitos dentro de sus portales. Después, revisa la competencia judicial internacional y el Derecho aplicable ante la vulneración de derechos de la personalidad a causa de la difusión de estos contenidos. Finalmente, repasa el alcance territorial que impone una obligación de retirada de este tipo de contenidos.

Palabras clave: Internet; redes sociales; Facebook; prestadores de servicios de alojamiento de datos; retirada de contenidos ilícitos.

* Abogada. Doctora en Derecho por la Universidad Complutense de Madrid. Ex profesora de Derecho Internacional Privado en la Universidad Europea de Madrid desde 1998 hasta 2018. Ex directora de tal Departamento desde 2004 hasta 2010. Profesora Ayudante Doctora de Derecho Internacional Privado de la Universidad Complutense de Madrid (Madrid, España). Acreditada como Profesora Contratada Doctora por la Agencia de Calidad, Acreditación y Prospectiva de las Universidades de Madrid. Contacto: lidimore@ucm.es.

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 5 de enero de 2021, y aceptado por el mismo el 21 de marzo de 2021.

I. INTRODUCCIÓN

En un mundo globalizado como el actual, en donde –en algunos casos– se han reducido y –en otros– se han eliminado los obstáculos a la libre circulación de mercancías, servicios y capitales, la irrupción de internet ha supuesto la desaparición de fronteras. La principal externalidad positiva que se deriva de lo anterior está relacionada con los beneficios que comporta para la rapidez de las transacciones comerciales. Se trata de una realidad que genera nuevas expectativas para el desarrollo de los negocios internacionales, así como también ventajas para los participantes en este entorno digital (Palao Moreno, 2017, p. 270). Incluso la Organización Mundial del Comercio tiene un programa de trabajo sobre el comercio electrónico, el cual fue adoptado en septiembre de 1998 y que, aunque solo a los efectos del programa de trabajo, incluye una definición de comercio electrónico: producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos (Organización Mundial del Comercio, 1998).

El avance experimentado en las telecomunicaciones ha tenido un gran impacto en el mundo empresarial y, consecuentemente, también una fuerte repercusión social incluso en el ámbito de la privacidad con los límites a la intimidad, lo que exige un tratamiento jurídico especializado. El mundo tecnológico se abre hacia el exterior y presenta, por ende, un carácter ubicuo, con la consecuencia de no tener límites aparentes (Davara Rodríguez, 2005, p. 25). Esta ausencia de márgenes definidos plantea serias dudas en cuanto al respeto de los derechos básicos de los individuos, de tal forma que, en un escenario diáfano como es internet, será muy complicado o prácticamente imposible evitar que la convivencia pacífica entre los sujetos se vea comprometida.

Internet ha supuesto una transformación sin precedentes en prácticamente todos los campos que se nos ocurran, hasta tal punto que su presencia ha desatado la denominada Tercera Revolución Industrial (Ortego Ruiz, 2020, p. 21). En efecto, internet se considera un elemento estructural de la 'sociedad de la información' desde el momento en que facilita los más variados servicios electrónicos interactivos y la comunicación de todo tipo de informaciones como texto, imágenes, sonido, video, entre otros. Su principal característica ha sido la capacidad de distribuir información y conocimiento globalmente y a gran velocidad (Barrio Andrés, 2017, p. 33). No es de extrañar que su inusitado éxito se deba a su capacidad de difusión por todo el mundo y, por ende, a su cualidad de ser un sistema de comunicaciones de carácter universal. Por lo tanto, es su enorme potencial para distribuir información y llegar a cualquier lugar, lo cual otorga al ciberespacio un estatus especial y único, diferente de todo lo demás, ya que permite la interacción entre personas físicas y jurídicas de todo el planeta.

El espacio donde se llevan a cabo los intercambios electrónicos se configura como una dimensión paralela a la real, donde los comportamientos se producen de manera virtual. Pues bien, son los comportamientos de las redes sociales y, en particular, los de Facebook, los que van a centrar nuestra atención. El motivo se encuentra en la sentencia del Tribunal de Justicia de la Unión Europea (en adelante, TJUE) del 3 de octubre de 2019 en el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* (Caso C-18/18), por cuanto revisten especial interés las cuestiones planteadas en este caso, de cara a concretar hasta dónde llega la responsabilidad de los prestadores de servicios en línea por los contenidos ilícitos que se viertan en los sitios web que ellos gestionan. En concreto, el asunto en cuestión tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 del Tratado de Funcionamiento de la Unión Europea, por el Oberster Gerichtshof (Tribunal Supremo de lo Civil y Penal de Austria), mediante resolución de 25 de octubre de 2017, recibida en el TJUE el 10 de enero de 2018, en el procedimiento entre Eva Glawischnig-Piesczek y Facebook Ireland Limited.

En síntesis, el litigio del que trae causa la sentencia mencionada surgió de una petición a Facebook Ireland Limited para que procediera a la retirada de un comentario humillante que se había compartido en dicha red social. La información controvertida hacía referencia a la señora Glawischnig-Piesczek, en tanto actora en el procedimiento principal, y había sido incluida por un usuario del sitio web en cuestión. La perjudicada tomó cartas en el asunto e inició actuaciones judiciales en Austria, país en el que desarrollaba su actividad política objeto de la afirmación ofensiva, con el fin de conseguir que se eliminase totalmente cualquier contenido que menoscabara su reputación. El Tribunal austríaco que estaba conociendo del asunto ordenó, mediante auto de medidas cautelares, que Facebook Ireland dejara de mostrar inmediatamente y hasta el cierre definitivo del procedimiento relativo a la acción de cesación, las declaraciones contrarias al honor de la demandante. No obstante ello, la existencia de normativa en la Unión Europea sobre las obligaciones de los prestadores de servicios de alojamiento de datos que gestionan redes sociales planteó algunas dudas en relación con el alcance que habría de darse a una obligación de este tipo.

Al respecto, el Tribunal Supremo de lo Civil y Penal de Austria planteó al TJUE una serie de cuestiones

prejudiciales relativas a si las obligaciones impuestas al proveedor de la red social de retirar el contenido inicialmente publicado por el correspondiente usuario y declarado ilícito, se extendían también a otros contenidos ilícitos o similares. Además, propuso si esa obligación de retirada podía ir referida a todo el mundo o solo al Estado miembro de que se trata y también cuestionó si la retirada de esos otros datos podía adoptarse solo con respecto al contenido del usuario en cuestión (De Miguel Asensio, 2019). Para poder dar respuesta a las dudas que se acaban de esgrimir, se tendrán en cuenta varios aspectos que inciden de lleno en la materia controvertida.

En primer lugar, se despejará la incógnita de si Facebook, en tanto red social, es un prestador de servicios de alojamiento de datos al que pueden aplicársele las normas de la Unión Europea, las cuales regulan las obligaciones que recaen sobre este tipo de intermediarios. A continuación, se concretará el régimen de la responsabilidad por contenidos ilícitos que asumen los prestadores de servicios de alojamiento de datos y, por ende, si Facebook lo fuera, el que se les atribuye a las redes sociales. Unido a lo anterior, se ofrecerán algunos ejemplos sobre la responsabilidad de los prestadores de servicios, basados en los pronunciamientos jurisprudenciales. Después, serán objeto de atención tanto la competencia judicial internacional por vulneración de derechos de la personalidad como el Derecho aplicable. Al respecto, hay que tener en cuenta que el carácter ubicuo de los contenidos puestos en línea a través de internet exigirá concretar qué jurisdicción es la mejor situada para pronunciarse sobre la eliminación de toda la información ilícita o de los datos que correspondan, así como determinar la ley con la que se resolverá el fondo del asunto, ya bien sea una sola o varias. También se prestará atención al alcance territorial de un requerimiento judicial que impone una obligación de retirada. Los contenidos en internet no entienden de fronteras y se difunden universalmente, lo que exigirá precisar hasta dónde debe llegar la eliminación de los contenidos publicados en línea. Finalmente, se culminará con unas conclusiones que evidencien los comportamientos que deben seguir las redes sociales cuando de la supresión de información ilícita se trate.

II. ¿LAS REDES SOCIALES SON PRESTADORES DE SERVICIOS DE ALOJAMIENTO DE DATOS?

Para el desarrollo del comercio electrónico en redes abiertas resulta clave la figura de los prestadores de servicios de internet. Estos últimos son aquellos que facilitan el acceso a la Red y proporcionan los servicios necesarios para que las diversas aplicaciones de internet puedan ser utilizadas, incluyendo los servicios de alojamiento de datos, entre otros (De Miguel Asensio, 2020a, p. 586).

En la actualidad, los sujetos intervinientes en la prestación de servicios de la sociedad de la información constituyen un grupo muy heterogéneo que realiza diversas funciones (Barrio Andrés, 2017, pp. 325-327). Por un lado, encontramos a los proveedores que suministran acceso a internet que engloban a los operadores de telecomunicaciones, como por ejemplo a Telefónica, además de incluir a las compañías de telefonía móvil. También hay que insertar en este grupo a los operadores de cable y fibra óptica, a los proveedores de acceso a internet y, por último, a los operadores de redes wifi. Por otro lado, están los sujetos que proporcionan servicios en línea para permitir el almacenamiento de contenidos, incluyendo el alojamiento de páginas web, pero que también facilitan plataformas para los contenidos generados por los propios usuarios, tanto con un fin comercial o social. De todos ellos, son estos últimos los que nos interesan y que hacen referencia a las redes sociales que permiten la interacción de los usuarios, como por ejemplo Facebook.

Además de los anteriores, otro grupo de sujetos favorecen la navegación en la web mediante la indexación del contenido disponible en la red, permitiendo así una localización más accesible. Este es el caso de los motores de búsqueda, los agregadores (que agrupan enlaces relevantes clasificados por diversos temas) y todos los sitios web que proporcionan enlaces hacia contenidos de terceros.

También deben citarse los proveedores de economía compartida. Muchas transacciones físicas (reservas de hotel o reservas de taxi, por ejemplo) se realizan a través de una comunicación a distancia entre las partes. Lo que realizan tales proveedores es facilitar la intermediación de aquellas de modo electrónico.

Por último, encontramos a los mediadores comerciales tradicionales. Estos son un grupo muy amplio de actores tradicionales en el comercio y que son replicados en el mundo virtual, tales como minoristas, instituciones financieras, anunciantes y otros operadores muy diversos que facilitan las transacciones y el comercio electrónico.

Como el foco de atención está puesto en las redes sociales, más concretamente, en Facebook (al ser este el demandado en el asunto objeto del análisis principal en este trabajo), lo primero que parece imprescindible es ofrecer una definición de este fenómeno. Al respecto, se pueden catalogar como 'redes sociales' a todos aquellos servicios basados en la web que permiten a los usuarios construir un

perfil público o semippúblico dentro de un sistema delimitado, además de articular una lista de otros usuarios con los que comparten conexiones y, por último, visualizar y rastrear su lista de conexiones y aquellas realizadas por otros dentro del sistema (Boyd & Ellinson, 2007, p. 211). Se trata en estos casos de ofrecer un entorno de la sociedad de la información en el cual los usuarios dispongan de una plataforma de comunicación a través de internet. Una vez dentro del espacio web, los participantes generan un perfil con sus datos personales, facilitando así la creación de comunidades con base en criterios comunes y permitiendo la comunicación entre usuarios, así como su interacción, de tal forma que se puedan entablar relaciones recíprocas mediante mensajes o intercambiando información, imágenes y videos. El objetivo es que todas las publicaciones sean accesibles de forma inmediata para el conjunto de usuarios del grupo (Barrio Andrés, 2017, p. 402).

En concreto, la plataforma Facebook se funda en 2004, lo cual marcó un hito sin parangón en la historia de las redes sociales. Su funcionamiento se basa en la interacción entre usuarios a través de la transferencia entre unos y otros de sucesos cotidianos, con el complemento de fotos e historias. Además, la red se ha caracterizado por su adecuación a diferentes idiomas, por lo que ha podido llegar sin restricción a todas las geografías que correspondan (Gutiérrez de Aizpuru, 2019, p. 234). En lo que respecta a si puede ser considerado un prestador de servicios de alojamiento de datos, en el sentido requerido por la normativa de la Unión Europea, la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* se limita a señalar que "ha quedado acreditado que Facebook es un prestador de servicios de alojamiento de datos" (Caso C-18/18, 2019, apartado 22). En consecuencia, el TJUE no aborda esta cuestión y la da por acreditada.

Por su parte, el Abogado General Maciej Szpunar en sus conclusiones sobre la mencionada sentencia (Caso C-18/18, 2019) indica que el TJUE ya ha tenido ocasión de aclarar que el explotador de una plataforma de red social en línea que almacena en sus servidores información facilitada por usuarios de dicha plataforma, relativa a su perfil, es un prestador de servicios de alojamiento de datos. Además, añade que de la petición de decisión prejudicial se desprende que el órgano jurisdiccional remitente considera acreditado que Facebook Ireland es un prestador de servicios de alojamiento de datos cuyo comportamiento se ciñe al de un prestador intermediario (Caso C-18/18, Szpunar, 2019, apartado 30). Tampoco se aportan argumentos concluyentes que corroboren sus conclusiones sobre esta controvertida cuestión.

Con todo, son las conclusiones del Abogado General Henrik Saugmandsgaard Øe en los asuntos acumulados C-682/18 y C-683/18 (2020) las que pueden despejar alguna incógnita a este respecto. Esto último sin perjuicio de ver si las confirma el TJUE, pues ambos casos están todavía pendientes de decisión.

De entrada, parece desprenderse de tales conclusiones que, para ser considerado un prestador de servicios de alojamiento de datos, es necesario que se den dos requisitos acumulativos: a) debe existir una prestación de un servicio de la sociedad de la información; y b) dicho servicio debe consistir en almacenar datos facilitados por el destinatario del servicio a petición de este último (Casos acumulados C-682/18 & C-683/18, Saugmandsgaard Øe, 2020, apartado 141).

Para que se produzca lo primero, es decir, que exista una prestación de un servicio de la sociedad de la información, las mencionadas conclusiones hacen referencia a que se debe tratar de un servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios (Casos acumulados C-682/18 & C-683/18, Saugmandsgaard Øe, 2020, apartado 142). Por su parte, el segundo requisito exigirá, de conformidad con el abogado Saugmandsgaard Øe, que el prestador de servicios lo sea de intermediación, en el sentido de que el prestador desempeñe un papel neutro y su comportamiento sea meramente técnico, automático y pasivo, de manera que no tenga conocimiento ni control de la información que almacena (Casos acumulados C-682/18 & C-683/18, 2020, apartado 148). Lo contrario, es decir, que el prestador desempeñe un papel activo que pueda darle conocimiento o control de los datos almacenados, impediría considerarle como un prestador de servicios de alojamiento de datos.

Pues bien, el TJUE ya ha tenido ocasión de declarar en el caso *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV*, antes de la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited,* que el explotador de una plataforma de red social en línea almacena en sus servidores información facilitada por usuarios de dicha plataforma, relativa a su perfil, y que de este modo es un prestador de servicios de alojamiento de datos (Caso C-360/10, 2012, apartado 27). De esto se deduce que Facebook, al ser una red social, es un prestador de servicios de alojamiento de datos. Además, de conformidad con las conclusiones del Abogado General en los asuntos acumulados C-682/18 y C-683/18 (Saugmandsgaard Øe, 2020), aquel presta un servicio de la sociedad de la información a cambio normalmente de

una remuneración, a distancia, por vía electrónica y a petición individual, al mismo tiempo que su actividad presenta un carácter de intermediación, por cuanto desempeña un papel neutro y su comportamiento es meramente técnico, automático y pasivo, sin conocimiento ni control de la información que almacena.

Esto último no resulta contradicho por el comportamiento del proveedor de una red social cuando determina, mediante la aplicación de sus algoritmos, qué contenidos alojados en sus servicios se muestran a sus usuarios, lo que podría hacer dudar de que su intervención fuera meramente automática y pasiva (De Miguel Asensio, 2019). Al respecto, en las conclusiones del Abogado General en los asuntos acumulados C-682/18 y C-683/18 se indica, en el apartado 160, que el hecho de que el prestador haya desarrollado herramientas –y, en particular, algoritmos que permiten el tratamiento de los datos– y que controle, en concreto, las condiciones de aparición de los resultados de las búsquedas, no demuestra que controle el contenido de los datos buscados (Saugmandsgaard Øe, 2020). En resumidas cuentas, afirma que su intervención no deja de ser meramente automática y pasiva, de tal forma que no tiene conocimiento ni control de la información que almacena.

III. EL RÉGIMEN DE LA RESPONSABILIDAD POR CONTENIDOS ILÍCITOS

En el contexto de la Unión Europea, la Directiva sobre el comercio electrónico (en adelante, DCE), de 8 de junio de 2000 (Directiva 2000/31), es la que ha venido a disciplinar la responsabilidad de los prestadores de servicios de alojamiento.

En particular, son los artículos 12 a 15 de la DCE los que se han dedicado a regular las obligaciones que pesan sobre los prestadores de servicios de alojamiento de cara, sobre todo, al control de los contenidos que se difunden por terceros. Dichos preceptos se enmarcan en la sección cuarta, del capítulo segundo de la DCE, que lleva por título el de la responsabilidad de los prestadores de servicios intermediarios. Pero, en concreto, de todos ellos nos interesa especialmente el artículo 14, por cuanto se refiere al prestador de servicios de alojamiento de datos. Habiendo quedado acreditado en el epígrafe anterior que Facebook Ireland es un prestador de servicios de alojamiento de datos, resulta evidente que la responsabilidad por contenidos ilícitos, en la que podría incurrir, entra dentro del ámbito de aplicación del artículo 14 de la DCE.

Tal y como se indica en la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, el apartado 1 del artículo 14 de la DCE tiene por objeto eximir de responsabilidad al prestador de servicios de alojamiento de datos cuando cumpla uno de los dos requisitos establecidos en la citada disposición: a) no tener conocimiento de que la actividad o la información es ilícita; o b) actuar con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible en cuanto tenga conocimiento de estos puntos (Caso C-18/18, 2019, apartado 23).

Para despejar cualquier duda que pudiera existir sobre la aplicación de esta exención de responsabilidad a una red social y, en concreto, a Facebook, hay que tener en cuenta el considerando número 42 de la DCE. En este último se señala que, para beneficiarse de la correspondiente exención:

a) la actividad del prestador de servicios debe limitarse al proceso técnico de explotar y facilitar el acceso a una red de comunicación mediante la cual la información facilitada por terceros sea transmitida o almacenada temporalmente, con el fin de hacer que la transmisión sea más eficiente; y

b) la actividad en cuestión debe ser de naturaleza meramente técnica, automática y pasiva, lo que implica que el prestador de servicios no tenga conocimiento ni control de la información transmitida o almacenada.

Como quiera que todos los atributos que se acaban de señalar ya fueron exigidos también para identificar a los prestadores de servicios de alojamiento de datos, en el epígrafe tercero de este trabajo, y se catalogó a las redes sociales y, en particular, a Facebook como un ejemplo de este tipo de prestadores, puede asegurarse sin temor a equivocarnos que, por ende, aquellos se benefician de la exención de responsabilidad.

Ahora bien, la razón de ser de la DCE no era establecer un régimen mínimo de responsabilidad de los prestadores de servicios de alojamiento de datos, sino de blindarles mediante la creación de una zona de exención de responsabilidad para favorecer la prestación transfronteriza de servicios de la sociedad de la información (Ortego Ruiz, 2015, p. 34). A pesar de la exención, en la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* se señala, en su apartado 24, que del apartado 3 del artículo 14 de la DCE, en relación con su considerando 45, se desprende la posibilidad de que un tribunal o una autoridad administrativa nacional exija al prestador de servicios de alojamiento de datos que se trate de poner fin a una infracción o impedirla, incluso suprimiendo los datos ilícitos o impidiendo el acceso a ellos. Aquello se justifica porque, debido a la peculiar posición de los in-

termediarios, la actuación de estos proveedores puede resultar determinante para lograr que cese la actividad infractora por parte del responsable, típicamente al hacer efectiva la retirada o bloqueo de los contenidos ilícitos (De Miguel Asensio, 2015, p. 240).

Ha quedado acreditada la existencia de una exención de responsabilidad para los prestadores de servicios de alojamiento de datos y, por consiguiente, para las redes sociales y Facebook, por los contenidos ilícitos vertidos por los usuarios. Exención que, no obstante, puede ser mitigada con la obligación de que aquellos pongan fin a la infracción o la impidan, incluso suprimiendo los datos ilícitos o impidiendo el acceso a ellos.

Por su parte, hay que tener en cuenta el artículo 15, apartado 1, de la DCE. Este precepto impide que los Estados miembros impongan a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, así como una obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas, respecto de los servicios previstos en los artículos 12, 13 y 14. De tal forma que, en la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited,* las cuestiones prejudiciales que se plantearon al TJUE por el Tribunal Supremo austríaco se circunscribieron a concretar el alcance personal y material de los mandamientos de retirada de contenidos ilícitos, así como el territorial, aunque este último lo abordaremos más adelante en el epígrafe sexto de este trabajo.

Por lo que respecta al alcance personal y material de los requerimientos judiciales de retirada de contenidos ilícitos, se debe precisar que lo prohibido por el artículo 15, apartado 1, de la DCE son las obligaciones de supervisión general. Sin embargo, se permiten las obligaciones de supervisión en casos específicos, tal y como se predica en el considerando 47 de la DCE. Lo que se entiende por supervisión en casos específicos ha sido precisado por el TJUE en el apartado 35 de la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* (Caso C-18/18, 2019). Al respecto, se indica que tal caso específico puede tener su origen, en particular, como sucede en el litigio principal, en una información precisa, almacenada por el prestador de servicios de alojamiento de datos de que se trata a instancia de un determinado usuario de su red social. El contenido de la información en cuestión, además, ha sido analizado y apreciado por un tribunal competente del Estado miembro que, al término de su apreciación, lo ha declarado ilícito. Si bien esta delimitación de que se entiende por 'supervisión en casos específicos' toma como referencia las circunstancias del asunto en el litigio principal, nada impide apreciar que puede haber situaciones en las que concurran otros elementos y la supervisión quede igualmente limitada a casos específicos (De Miguel Asensio, 2019).

En consecuencia, se constata que existe un riesgo real de que una información que ha sido declarada ilícita sea reproducida y compartida posteriormente por otro usuario de la red. Pero, al mismo tiempo, el artículo 15, apartado 1, de la DCE impide que para evitar ese peligro se imponga una obligación excesiva al prestador de servicios de alojamiento de datos, tal y como rezan los apartados 36 y 44 de la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited.* Por lo tanto, el TJUE se tuvo que manifestar sobre la posibilidad de que el artículo 15, apartado 1, de la DCE se opusiera a que un órgano jurisdiccional de un Estado miembro pudiera obligar a un prestador de servicios de alojamiento de datos a suprimir los datos que almacene. En concreto, cuando el contenido sea 'idéntico' o 'similar' al de una información declarada ilícita con anterioridad o a bloquear el acceso a ellos, sea cual fuere el autor de la solicitud de almacenamiento de tales datos.

Al respecto, el Abogado General en el apartado 109 de sus conclusiones sobre el asunto *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* (Caso C-18/18, Szpunar, 2019), se decantó por interpretar el artículo 15, apartado 1, de la DCE como compatible con un mandamiento judicial que obligue a un prestador de servicios de alojamiento de datos a que busque e identifique, entre todos los datos difundidos por los usuarios, datos idénticos a los declarados ilícitos. Para los datos similares, sin embargo, solo lo consideró apropiado si se circunscribía a los difundidos por el usuario que publicó tales datos. Para justificar su decisión, en el apartado 74 de sus conclusiones, tuvo en cuenta que imponer una obligación de identificar datos similares a los declarados ilícitos procedentes de cualquier usuario no garantizaría un justo equilibrio entre la protección de la intimidad y los derechos de la personalidad, libertad de empresa y libertad de expresión e información (Caso C-18/18, Szpunar, 2019). Además, añadió que la búsqueda e identificación de esos datos precisaría de soluciones costosas, que deberían ser desarrolladas e implantadas por el prestador de servicios de alojamiento de datos (Caso C-18/18, Szpunar, 2019). Incluso, consideró que la aplicación de esas soluciones daría lugar a una censura, de modo que la libertad de expresión y de información podría verse sistemáticamente limitada.

Por su parte, el TJUE en la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* ha optado por una interpretación más amplia. En

este sentido, considera ajustado al artículo 15, apartado 1, de la DCE un mandamiento judicial que obligue a un prestador de servicios de alojamiento de datos a que realice una supervisión y búsqueda de los datos idénticos a los declarados ilícitos, con independencia del autor que los haya difundido (Caso C-18/18, 2019). También si versa sobre datos de contenido similar y aunque provengan de cualquier usuario del servicio (Caso C-18/18, 2019, apartado 53). En efecto, para las informaciones similares, la obligación de eliminarlas no se limita a las vertidas por el autor que publicó las catalogadas de ilícitas con anterioridad. Esta solución parece razonable, habida cuenta de que no cabe excluir que, en ocasiones, medidas de retirada relativas a contenidos similares de otros usuarios puedan ser precisas y estar configuradas de manera que no impongan soluciones excesivamente costosas ni menoscaben de manera excesiva la libertad de expresión ni el resto de los derechos fundamentales afectados (De Miguel Asensio, 2019).

Además, el TJUE en la sentencia *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* ofrece aclaración sobre cómo acreditar los datos similares (Caso C-18/18, 2019, apartado 45). Al respecto, indica que deben contener elementos concretos debidamente identificados por el autor de la medida cautelar, como el nombre de la persona víctima de la infracción constatada anteriormente, las circunstancias en las que se ha comprobado dicha infracción, así como un contenido similar al que se ha declarado ilícito. Por lo tanto, será posible imponer a los prestadores de servicios de alojamiento de datos medidas de supervisión tanto de los contenidos idénticos, como de los similares a los declarados ilícitos anteriormente, ya bien se hayan difundido por el autor de estos últimos o por cualesquiera otros usuarios del servicio.

Ahora bien, hay doctrina que disiente con el planteamiento que se acaba de esbozar. Así, en el caso de los datos similares a los declarados ilícitos anteriormente, se viene a indicar que el estado actual de la tecnología impide identificar información parecida cuya equivalencia con la controvertida puede venir del contexto en el que se ha producido o del sentido que se le quiere otorgar, por ejemplo, si su significado pretende satirizar o criticar el contenido original. Esta situación requeriría que las plataformas tuvieran que acudir a la supervisión humana para realizar una serie de evaluaciones sustantivas que, además, serían indefinidas en el tiempo. De tal forma que los prestadores de servicios de alojamiento de datos tendrían que seguir evaluando cualquier nueva circunstancia que pudiera entrar en colisión con el contenido ilícito declarado con anterioridad. Incluso, a la inversa, podría ocurrir que la información sobrevenida, que hiciera referencia a la actuación posterior del perjudicado inicialmente, convirtiera en lícita y verdadera la difusión de la información que se hubiera dado al respecto (Cavaliere, 2019).

En esta misma línea, se indica que las herramientas de filtrado automatizadas proporcionan fácilmente 'falsos positivos' al identificar incorrectamente el contenido como ilegal, lo que lleva a la eliminación de contenido legítimo. Incluso las herramientas que se basan en la inteligencia artificial son incapaces de comprender la ironía o la sátira o darse cuenta de que el discurso del odio se puede utilizar en una cita para crear conciencia (Rauchegger & Kuczerawy, 2020, p. 1518). También se ha dicho que un contenido idéntico no implica necesariamente un significado idéntico. En algunos casos, el mensaje podría ser idéntico al original, pero en otros casos podría ser diferente, con el resultado de que el contenido, aunque idéntico, podría no ser ilegal, por ejemplo, si está inserto en un comentario más amplio (Rosati, 2019). Esto último se podría producir cuando el contexto modifique el sentido y, en consecuencia, el contenido idéntico presente un significado diferente, de manera que no acabe resultando lesivo.

En definitiva, parecería que la supresión del contenido idéntico o similar no se podría realizar solo de manera automatizada: habría una primera preselección mecanizada de la información y, después, una decisión final por el sujeto correspondiente tras la evaluación oportuna. Al respecto, la regulación más reciente de la Unión Europea en materia de contenido *online* sigue esta misma estela de requerir la revisión de las decisiones de filtrado automatizadas por parte de las personas competentes. Así, por un lado, la Directiva 2019/790 sobre los derechos de autor y derechos afines en el mercado único digital, en su artículo 17, apartado 9, establece que "las decisiones de inhabilitar el acceso a los contenidos cargados o de retirarlos estarán sujetas a examen por parte de personas" (2019). Por otro lado, la Propuesta de reglamento para la prevención de la difusión de contenidos terroristas en línea (Comisión Europea, 2018), en su artículo 9, estipula algo parecido: indica que los prestadores de servicios de alojamiento de datos aplicarán garantías eficaces y adecuadas cuando usen instrumentos automatizados para tomar decisiones sobre la retirada de los contenidos considerados terroristas o bloquear el acceso a ellos. Esto último persigue que las decisiones de retirada o bloqueo sean precisas y bien fundamentadas, para lo que se basarán, en particular, en la supervisión y verificaciones por personas.

IV. ALGUNOS EJEMPLOS SOBRE LA RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS

La responsabilidad de los prestadores de servicios de alojamiento de datos puede quedar exonerada, en un primer momento, si desconocían que la actividad o la información eran ilícitas. En caso contrario, todavía podrían evitar ser reclamados, en un segundo momento, si proceden a la inmediata retirada de los contenidos ilícitos alojados. En relación con el conocimiento sobre la ilegalidad de los contenidos alojados, el TJUE se ha mostrado partidario de interpretarlo de manera extensiva, es decir, mediante el llamado conocimiento indiciario (Ortego Ruiz, 2015, p. 49). La sentencia de 12 de julio de 2011, caso *L'Oréal SA et al. c. eBay International AG et al.*, tuvo ocasión de señalar que la percepción sobre el carácter ilegítimo de los contenidos se equipara a cualquier situación en la que el prestatario en cuestión adquiera conocimiento, de una forma o de otra, de tales hechos o circunstancias (Caso C-324/09, 2011, apartado 121).

La afirmación anterior se ilustra haciendo referencia a que en este supuesto encaja, en particular, la hipótesis en la que el operador de un mercado electrónico descubra la existencia de una actividad o información ilícitas como consecuencia de una investigación realizada por su propia iniciativa. Además, se incluiría el supuesto en el que le sea notificada la existencia de este tipo de actividad o información. Por su parte, para el segundo caso, se aclara que la existencia de una notificación no determina automáticamente que el operador pierda la posibilidad de invocar la exención de responsabilidad. Al respecto, cabría invocarla cuando la notificación de la existencia de actividades o informaciones supuestamente ilícitas resulte excesivamente imprecisa o no esté suficientemente fundamentada. En cualquier caso, la notificación constituye, como regla general, un elemento que el juez nacional debe tomar en consideración para apreciar si el operador tenía realmente conocimiento de hechos o circunstancias a partir de los cuales uno diligente hubiera debido constatar ese carácter ilícito (Caso C-324/09, 2011, apartado 122).

En la misma línea, la sentencia del TJUE de 23 de marzo de 2010, en los asuntos acumulados C-236/08 y C-238/08, también señaló que la responsabilidad de los prestadores de servicios de alojamiento de datos queda acreditada cuando la ilicitud de los datos o de las actividades del destinatario del servicio llegan a su conocimiento. Esto último puede suceder gracias a la información recibida de un perjudicado o de otro modo (Casos acumulados C-236/08 & C-238/08, 2010, apartado 109). Se deduce de todo lo dicho hasta ahora, que la posibilidad de llegar a la convicción de la ilegalidad 'de una forma' o 'de otro modo' son conceptos jurídicos indeterminados que generan inseguridad. Se podría subsanar esta situación con la elaboración de indicadores jurídicos, a modo de norma que lo regulara, en los cuales se especificaran los mecanismos de detección y retirada de contenidos. Ello se hace en la legislación norteamericana a través de la *Digital Millennium Copyright Act* (1998), en donde se ofrecen este tipo de aclaraciones, en la sección 512 (c) (3), lo que, sin duda, aporta confiabilidad al sistema.

Por lo que respecta a la retirada inmediata de los contenidos ilícitos alojados para sustraerse de la responsabilidad, aquella se entiende como una segunda posibilidad para esquivar la reclamación por daños. Pero para proceder a la retirada debe existir certeza de la ilicitud de los contenidos, para lo cual sería necesario precisar a quién le corresponde ponerlo de manifiesto. En situaciones dudosas, el prestador de servicios podría verse obligado a retirar una información que luego pudiera resultar lícita, por lo que también incurriría en responsabilidad por atentar contra la libertad de expresión e información. Es por ello que se necesitan mecanismos que arbitren soluciones efectivas y eficaces, pero, sobre todo, que aporten una prueba fiable o suficiente en Derecho.

Al respecto, la Directiva sobre el comercio electrónico alude en su artículo 14, apartado 3, a la posibilidad de que un tribunal o una autoridad administrativa, de conformidad con los sistemas jurídicos de los Estados miembros, exijan al prestador de servicios poner fin a una infracción o impedirla (Directiva 2000/31/CE, 2000). Pues bien, esa podría ser la opción para acreditar la ilicitud: que se encomiende esa tarea al Poder Judicial o al órgano equivalente de la administración. Tal parece ser la solución más garantista y la que se apunta en la sentencia del TJUE de 13 de mayo de 2014, en el caso *Google Spain, S.L. y Google Inc. c. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González* (Caso C-131/2012), cuando se alude a la autoridad de control o al órgano jurisdiccional. En concreto, la referencia a ambos se hace con el fin de que ordenen a Google que elimine de la lista de resultados del buscador la información relativa a una persona, de quien ha sido vulnerado su derecho fundamental a la protección de datos (Caso C-131/2012, 2014, apartado 82). De manera que se consigue contar con el filtro categórico de las instancias jurisdiccionales o gubernativas para la acreditación de la vulneración producida; sin que el prestador del servicio tenga ahora la más mínima duda de que, para librarse de la responsabilidad, debe actuar con prontitud a la hora de quitar la información controvertida.

También el Tribunal Europeo de Derechos Humanos del Consejo de Europa ha tenido ocasión de pronunciarse sobre la responsabilidad de los prestadores de servicios. En concreto, la sentencia de 16 de junio de 2015, en el asunto *Delfi AS c. Estonia,* se refirió a la responsabilidad de los portales de noticias por los contenidos difamatorios publicados por los lectores. La cuestión principal que se abordó en la resolución judicial estaba relacionada con la consideración de los portales que alojan foros. Se debatía si debían ser considerados intermediarios de servicios de la sociedad de la información o, por el contrario, debían ser equiparados a los proveedores de contenidos. En el primer caso, se podrían beneficiar de la exención de responsabilidad de la DCE; mientras que, en el segundo, tendrían la obligación de controlar los contenidos. Pues bien, la solución a la que llegó el Tribunal fue estimar que el administrador de un portal de noticias en internet tenía la consideración de editor y, por ende, asumía la responsabilidad directa por los contenidos publicados por los lectores (*Delfi AS c. Estonia*, 2015). Hay, en consecuencia, una equiparación entre estos portales de noticias en internet y los medios de comunicación tradicionales, por lo que se les impone la llamada *culpa in vigilando* por los contenidos (Departamento de Telecomunicaciones & Media de Garrigues, 2013).

Se comparte la opinión que considera discutible la respuesta ofrecida, tanto por los tribunales estonios como por el Tribunal Europeo, en relación con algunos de los comportamientos enjuiciados desde la perspectiva de su conformidad con la DCE (De Miguel Asensio, 2013). En cualquier caso, la conclusión a la que se llegó en este asunto fue la de entender que no se comprometía a libertad de expresión prevista en el artículo 10 del Convenio Europeo de Derechos Humanos, debido a la obligación del portal de suprimir los contenidos lesivos. Además, se le consideró civilmente responsable frente a la víctima por los contenidos difamatorios que terceros habían introducido en sus servicios.

Resultan también relevantes las opiniones de la doctrina respecto a la responsabilidad que debe pesar sobre los prestadores de servicios. Así, encontramos posturas que hacen referencia al estándar mayor de diligencia que se les aplicaría a los portales de noticias y a otros agregadores, como consecuencia de la sentencia del Tribunal Europeo de Derechos Humanos en el caso *Delfi AS c. Estonia.* Esta situación se produce como consecuencia de que queden al margen de la DCE y, por ende, de la imposibilidad de aplicarles la exclusión de responsabilidad propia de las reglas contenidas en dicha norma, lo cual ha sido considerado inaceptable. Al respecto, se indica que las interacciones y las relaciones de la red social con sus usuarios es muy diferente al de un medio de comunicación tradicional respecto de quienes publican en estas plataformas. Incluso se añade que, sin esta regla de exclusión, muchas de las posibilidades de negocios, pero también de expresión, asociadas a las redes sociales, simplemente, no existirían, y de forma consiguiente el pluralismo se resentiría gravemente (Boix Palop, 2016, pp. 93-94).

Por lo tanto, en la sociedad de la información la libertad de expresión adquiere una nueva dimensión, mostrándose como representante de una nueva cultura y de un nuevo modelo de vida (Teruel Lozano, 2010, p. 128). Ahora bien, no puede obviarse que para evitar resultados inopinados y divergentes en las diversas jurisdicciones, resultaría conveniente que las reglas fueran lo suficientemente homogéneas, por lo menos, en toda la Unión Europea (Peguera Poch, 2010, p. 267). En esta línea, la fórmula del Reglamento y no de la Directiva, como hasta ahora ha ocurrido con la DCE, podría ser la solución más adecuada para incrementar la seguridad en el sistema. Optar por reglas idénticas para todos, en lugar de conformarse con normas de mínimos traspuestas en los ordenamientos estatales con diferentes niveles de exigencia, parece un paso más que necesario en el momento actual de la evolución de los servicios de la sociedad de la información y del comercio electrónico.

V. COMPETENCIA JUDICIAL INTERNACIONAL POR VULNERACIÓN DE DERECHOS DE LA PERSONALIDAD Y DERECHO APLICABLE

Presupuesto necesario de la eventual adopción de medidas de retirada de contenidos con alcance mundial es que el órgano al que se solicitan tenga competencia judicial internacional para adoptarlas (De Miguel Asensio, 2019). Por lo que respecta a los litigios en los que se alegue una lesión de los derechos de la personalidad mediante el contenido publicado en un sitio de internet, la jurisprudencia del TJUE ya ha tenido ocasión de pronunciarse sobre la interpretación del instrumento jurídico que en la Unión Europea regula esta cuestión y que se circunscribe al Reglamento 1215/2012 (2012). En concreto, en los litigios relativos a la responsabilidad extracontractual por vulneración de los derechos de la personalidad, como es este caso, los tribunales de los Estados miembros correspondientes a los del domicilio del demandado, del lugar de origen del daño o del centro de intereses de la víctima pueden tener competencia con alcance general, incluyendo medidas de retirada de contenidos de internet sin limitación territorial (De Miguel Asensio, 2020b).

En efecto, de conformidad con la sentencia *eDate Advertising GmbH et al. c. X y Société MGN Ltd,* la interpretación del artículo 7.2 del Reglamento 1215/2012 permite que la persona que se considera lesionada pueda ejercitar una acción de responsabilidad por la totalidad del daño causado, ante los órganos jurisdiccionales del Estado miembro en el que se encuentra su centro de intereses (Casos acumulados C-509/09 & C-161/10, 2011, apartado 48). Se infiere de lo anterior, que los tribunales correspondientes a la residencia del perjudicado, donde con carácter general se sitúa su centro de intereses, son competentes para acordar medidas relativas a la retirada de contenidos de internet con un alcance territorial ilimitado. Además, en el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, tal y como se indica por el Abogado General en sus conclusiones (Caso C-18/18, Szpunar, 2019, apartado 84), el órgano jurisdiccional ante el que la demandante ha ejercitado la acción es el de su centro de intereses.

Las ventajas de este foro son claras, ya que potencia la buena administración de la justicia, pues dicho lugar presenta una conexión innegable con el supuesto litigioso. Además, propicia que la competencia del tribunal del lugar en el que la presunta víctima tiene su centro de intereses sintonice correctamente con el principio de previsibilidad (Calvo Caravaca & Carrascosa González, 2017, p. 1549). Esto último se logra por el conocimiento que puede tener el demandado, cuando introduce los datos lesivos, de cuáles son los centros de intereses de las personas que han sido objeto de sus comentarios. Por su parte, el demandante también se ve favorecido, porque puede averiguar sin dificultad el tribunal competente para conocer de su caso, por coincidir con el del lugar donde se encuentra su centro de intereses.

Por consiguiente, tal y como establece el Abogado General en sus conclusiones relativas al asunto *Eva Glawischnig-Piesczek c. Facebook Ireland Limited,* los tribunales de un Estado miembro pueden resolver, en principio, sobre la retirada de contenidos fuera del territorio del citado Estado miembro, pues tienen competencia territorial universal (Caso C-18/18, Szpunar, 2019). Aunque podría resultar inviable que los órganos jurisdiccionales de un Estado miembro se pronunciaran sobre la retirada a nivel mundial no ya por un tema de competencia, sino, en su caso, por una cuestión de fondo (Caso C-18/18, Szpunar, 2019, apartado 86). Esto último nos lleva inevitablemente a dedicar las líneas que siguen a la determinación de la ley aplicable a una lesión a los derechos de la personalidad en internet. El motivo de tener que hacerlo se encuentra en que la determinación de la ley aplicable en materia de derechos de la personalidad se presenta como una cuestión clave y de extremada importancia. Esto último se deduce de las frecuentísimas violaciones que en esta materia se producen a través de internet, así como de la nuclear importancia que en la construcción del Estado Social y de Derecho han tenido y tienen los bienes jurídicos protegidos por estos derechos. No en vano están protegidos como derechos fundamentales la libertad de expresión e información, así como el derecho al honor, la intimidad y la propia imagen, límite uno del otro y cuya regulación equilibrada es básica en la configuración del mismo (Ortego Ruiz, 2015, pp. 130-131).

Una dificultad añadida en el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* es que aquel va referido a una materia en la que ni el derecho material ni las reglas de conflicto están unificadas en el seno de la Unión Europea. Esta falta de regulación uniforme se deriva de la exclusión de las violaciones de derechos de personalidad del ámbito de aplicación del Reglamento 864/2007 (Roma II), en virtud de su artículo 1.2.g (De Miguel Asensio, 2019). En consecuencia, la determinación de la ley aplicable a una reclamación de ese tipo debe hacerse en los Estados miembros de la Unión Europea según las reglas nacionales del Derecho internacional privado. Sin que sea extraño, desde una perspectiva comparada, que las normas de conflicto en esa materia puedan conducir a la aplicación de una única ley, por ejemplo, la de la sede de la víctima, al conjunto de la reclamación (De Miguel Asensio, 2020b).

En cualquier caso, la ley aplicable al fondo del asunto regulará la precisión de quién es el autor de la vulneración de los derechos de la personalidad y la responsabilidad que debe imputarse al autor de la lesión referida. También deberá concretar qué otros sujetos pueden ser demandados por infracción de estos derechos en internet. Además de decidir la cuestión de la responsabilidad civil de los sujetos que administran *websites,* con enlaces de internet a otros *websites,* en los que se encuentran materiales que lesionan los derechos de personalidad (Calvo Caravaca & Carrascosa González, 2017, p. 1554). Todo ello sin olvidar que en la Unión Europea sería aplicable la DCE, con todo lo que ya hemos visto en relación con el régimen de la responsabilidad por contenidos ilícitos en el epígrafe anterior.

Lo único que nos queda ahora por determinar es el alcance territorial de los mandamientos de retirada. En concreto, abordaremos si la supresión de contenidos por una red social debe referirse solo a los datos del servicio en el Estado miembro cuyos tribunales conocen de litigio principal o también se extiende a las informaciones de cualquier lugar del mundo.

VI. LA EJECUCIÓN DE UNA OBLIGACIÓN DE RETIRADA EN TODO EL MUNDO

Resulta indubitada, de acuerdo con los planteamientos esgrimidos hasta el momento, la obligación que pesa sobre los prestadores de servicios de alojamiento de datos y, por ende, sobre Facebook Ireland, en relación con la retirada o eliminación de los datos declarados ilícitos por la autoridad competente en cuestión. Obligación, por cierto, que se extiende no solo a los datos introducidos en la red social por el autor correspondiente, sino también a los que sean idénticos a los declarados ilícitos y hayan sido difundidos por cualesquiera usuarios del servicio. Incluso abarca a los que sean similares, con independencia también de quién haya sido el autor de la información controvertida. En consecuencia, lo que procede a continuación es delimitar el alcance territorial de la orden de retirada. El motivo se encuentra en las dudas que se plantean en el litigio *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* relativas a si el mandamiento de retirada de los contenidos ilícitos se circunscribe solo a los datos correspondientes en el Estado miembro cuyos tribunales conocen del asunto o tiene también un alcance mundial.

Al respecto, el TJUE, en su sentencia sobre el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*, se pronunció con rotundidad al entender que el apartado 1 del artículo 18 de la DCE no limita en modo alguno, en particular territorialmente, el alcance de las medidas que los Estados miembros pueden adoptar con arreglo a la norma citada. Por consiguiente, concluye el TJUE, la DCE no se opone a que las referidas medidas cautelares produzcan efectos a escala mundial (Caso C-18/18, 2019, apartados 49 & 50).

Ahora bien, el principio de la razonabilidad permite cuestionar la aplicación indiscriminada de lo que parecen valores absolutos. A su vez, admite un enfoque misceláneo del derecho internacional privado sobre la base de conceptos tales como las expectativas razonables, vínculos más estrechos, el deber de evaluar y equilibrar, la distinción entre superposición en la regulación y conflicto directo y entre conflicto potencial y choque real (Lowenfeld, 1996, pp. 229-230). Por lo que, para el caso que nos ocupa, se trataría de encontrar una forma lógica y tangible de ejecutar una medida de supervisión de manera segura y efectiva. Sin pretender imponer una pléyade de controles a la red social sobre todos los contenidos vertidos en línea.

La supervisión habría de tener en cuenta, tal y como señala el Abogado General en el apartado 100 de sus conclusiones sobre el caso *Eva Glawischnig-Piesczek c. Facebook Ireland Limited* (Caso C-18/18, Szpunar, 2019), las diferencias que existen entre las leyes nacionales, por un lado, y la protección de la intimidad y de los derechos de la personalidad que dichas leyes establecen, por el otro. De tal forma que, para respetar derechos fundamentales ampliamente reconocidos, sería conveniente que dichos órganos jurisdiccionales adoptaran una postura comedida. Es más, el cumplimiento de una obligación de retirada no debería ir más allá de lo necesario para lograr la protección de la persona lesionada, so pena de ser imposible obtener el reconocimiento y la ejecución de resoluciones en terceros países cuyo orden público entre en contradicción con dichas medidas (De Miguel Asensio, 2020b).

Esta solución es la que parece imponerse de cara al futuro más inmediato con la Propuesta de Reglamento que establece la ley de servicios digitales en la Unión Europea (*Digital Markets Act*, 2020). En efecto, el artículo 8.2.b viene a decir que el alcance territorial de los mandamientos jurisdiccionales o administrativos para actuar contra los contenidos ilegales, sobre la base de las normas aplicables del Derecho estatal y de la Unión, incluida la Carta, y, en su caso, los principios generales del derecho internacional, no excederá de lo estrictamente necesario para alcanzar su objetivo (*Digital Markets Act*, 2020). Además, la propuesta en cuestión supondrá una unificación y no una armonización, como hasta ahora, de las normas que regulan la actuación de las plataformas *online*. Esta última situación se puede catalogar como muy beneficiosa, por su contribución a la seguridad jurídica de todos los participantes en el mundo digital. En efecto, entre las diferentes opciones legislativas, se ha elegido la del Reglamento, en tanto instrumento jurídico de efecto directo e inmediato en todo el territorio y que va a acompañado de una elevada dosis de precisión en la regulación, indispensable a los efectos pretendidos (Soldevila Fragoso, 2021). Por lo tanto, entre los niveles de obligatoriedad existentes en los tipos de normas de la Unión Europea, se opta por el más elevado, lo que claramente está en línea.

VII. CONCLUSIONES

No cabe duda de que internet ha supuesto una revolución sin precedentes en prácticamente todos los ámbitos de actuación del ser humano. Hay relaciones sociales que se producen a través de la red, pero también operaciones económicas, transacciones mercantiles y un sinfín de situaciones jurídicas que se llevan a cabo a través de este medio. Su peculiaridad fundamental es que se trata de una dimensión que no entiende de fronteras y presenta un carácter ubicuo, por lo que el alcance de su

proyección es, en principio, universal. La ausencia de márgenes definidos que presenta el espacio *online* mantiene una convivencia poco pacífica con la fragmentación jurídica que está presente en el mundo *offline*.

En efecto, en un planeta dividido en Estados, cada uno de los cuales regula de manera específica las actividades en línea, los problemas de Derecho internacional privado son recurrentes. Ya bien sean problemas de competencia judicial internacional, de ley aplicable o de eficacia extraterritorial de resoluciones judiciales extranjeras, se irán produciendo en la medida en que la difusión de los contenidos en línea se conecte con un gran número de ordenamientos jurídicos. A ello se une la capacidad que tienen los datos vertidos en un entorno digital para propagarse de manera inmediata y producir, cuando son ilícitos, efectos globales. En estos casos, la existencia de instrumentos jurídicos dirigidos a minimizar los efectos perniciosos de los comportamientos de tráfico jurídico externo contrarios a Derecho, se convierte en el baluarte para equilibrar los menoscabos que hayan podido sufrir los sujetos afectados.

En el contexto de la Unión Europea, la DCE es un buen ejemplo de normativa catalizadora de soluciones adecuadas para los casos de difusión en redes sociales de informaciones controvertidas. La posibilidad de adoptar mandamientos judiciales de retirada de los contenidos lesivos difundidos por los usuarios y que deben cumplir los prestadores de los servicios de alojamiento, se considera una medida muy positiva y eficaz para acabar con la vulneración de un derecho de la personalidad. Además, se impone a los prestadores de servicios de alojamiento de datos una obligación de supervisión no general, pero sí en casos específicos, sobre los datos idénticos y similares a los declarados ilícitos con anterioridad. Sin que los datos tengan que proceder únicamente del autor de los declarados ilícitos con anterioridad, sino que pueden haber sido puestos en circulación por cualquier usuario del servicio.

Incluso no se ponen puertas al campo, en el sentido de entender que las medidas cautelares que los Estados miembros pueden adoptar con arreglo a la DCE pueden surtir efectos extraterritoriales, es decir, serían susceptibles de ser emitidas con un alcance mundial, aunque para ello se pida una postura comedida y no se exija que la retirada vaya más allá de lo necesario para lograr la protección de la persona lesionada. Solución que, por otra parte, consideramos lógica, basada en el sentido común e imbuida por el principio de la razonabilidad y que, además, parece que será la respuesta ofrecida por la Unión Europea en su propuesta de *lege ferenda* para los servicios digitales. Lo contrario, que pasaría por mandamientos indiscriminados de retirada de contenidos ilícitos debe reputarse inadecuado. La necesaria ponderación de los derechos fundamentales afectados, esto es, el de libertad de expresión con el derecho a la intimidad debe permitir que se hagan públicas las informaciones objetivas y debidamente contrastadas. Pero, al mismo tiempo, tiene que impedir que los comentarios ilícitos se propaguen por la red libremente.

Las medidas de supervisión que se imponen a los prestadores de servicios, no con un alcance general, sino para casos específicos pueden catalogarse de apropiadas. Se trata de conseguir que los contenidos idénticos a los declarados ilícitos, con independencia del autor que los haya introducido, acaben desapareciendo de internet. Pero no acaba ahí la responsabilidad de los prestadores, ya que también deberán procurar la eliminación de los datos de contenido similar y aunque provengan de cualquier usuario del servicio. Esto último es lo que, quizá, pueda resultar más controvertido, desde el momento en el que se debe realizar una valoración subjetiva de lo que se pueda considerar parecido a otro comentario declarado lesivo. Para aportar confiabilidad al sistema se podría recurrir a una primera detección por las herramientas automatizadas que identifiquen contenidos afines, para pasar después de ello a la valoración final por parte de las personas competentes. Con todo, no deja de ser un enjuiciamiento humano el que decide, lo que puede conducir a interpretaciones divergentes para los mismos supuestos y, además, sin que se precise el nivel competencial del encargado de esta tarea. Es por ello que podría ser el momento oportuno de regular esta figura, aunque posiblemente se podría equiparar al *compliance officer* que se encargaría, en este caso, de supervisar el cumplimiento tecnológico de la compañía.

REFERENCIAS

Barrio Andrés, M. (2017). *Fundamentos del Derecho de Internet*. Centro de Estudios Políticos y Constitucionales.

Boix Palop, A. (2016). La construcción de los límites a la libertad de expresión en las redes sociales. *Revista de Estudios Políticos*, (173), 55-112. http://dx.doi.org/10.18042/cepc/rep.173.02.

Boyd, D., & Ellinson, N. (2007). Social Networks Sites: Definition, History and Scholarship. *Journal of Computer-Mediated Communication*, *13*(1), 210-230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Calvo Caravaca, A. L., & Carrascosa González, J. (2017). *Derecho Internacional Privado* (17ma ed., Vol. II). Editorial Comares.

Cavaliere, P. (2019). Glawischnig-Piesczek v Facebook on private enforcement of speech regulation and international jurisdiction. *European Data Protection Law Review, 5*(4), 573-578. https://dx.doi.org/10.2139/ssrn.3519389

Davara Rodríguez, M. A. (2005). *Manual de Derecho Informático*. Editorial Aranzadi.

De Miguel Asensio, P. A. (12 de octubre de 2013). Sobre el control de los comentarios de terceros en blogs y sitios webs tras el asunto Delfi. https://pedrodemiguelasensio.blogspot.com/2013/10/sobre-el-control-de-los-comentarios-de.html#more

(2015). *Derecho Privado de Internet* (5ta ed.). Editorial Aranzadi.

(13 de junio de 2019). Alcance material de los mandamientos judiciales de retirada de contenidos ilícitos frente a redes sociales [Entrada de blog]. https://pedrodemiguelasensio.blogspot.com/2019/06/alcance-material-de-los-mandamientos.html

(17 de junio de 2019). Alcance territorial de los mandamientos judiciales de retirada de contenidos ilícitos frente a redes sociales [Entrada de blog]. https://pedrodemiguelasensio.blogspot.com/2019/06/alcance-territorial-de-los-mandamientos.html

(4 de octubre de 2019). Alcance de los mandamientos judiciales de retirada de contenidos ilícitos frente a redes sociales: la sentencia Glawischnig-Piesczek [Entrada de blog]. https://pedrodemiguelasensio.blogspot.com/2019/10/alcance-de-los-mandamientos-judiciales.html

(2020a). Contratos de colaboración. En J. C. Fernández, R. Arenas García, & P. A. De Miguel Asensio, *Derecho de los negocios internacionales* (6ta ed., pp. 541-603). Iustel.

(2020b). Internet y Derecho internacional privado: Balance de un cuarto de siglo. En S. Álvarez González, R. Arenas García, P. A. De Miguel Asensio, S. Sánchez Lorenzo, & G. Stampa Casas (eds.), *Relaciones transfronterizas, Globalización y Derecho (Homenaje al Profesor Doctor José Carlos Fernández Rozas)* (pp. 211-228). Thomson Reuters-Civitas.

Departamento de Telecomunicaciones & Media de Garrigues (12 de noviembre de 2013). Sentencia del TEDH sobre la responsabilidad de los foros de internet (Caso Delfi AS v. Estonia). *Garrigues Blog*. http://blog.garrigues.com/sentencia-del-tedh-sobre-la-responsabilidad-de-los-foros-de-internet-caso-delfi-as-v-estonia/?cn-reloaded=1

Gutiérrez de Aizpuru, J. (2019). Implicaciones legales de las redes sociales. En J.F. Estévez, (coord.), *Derecho digital* (pp. 231-278). Thomson Reuters Aranzadi.

Internet (2020). En *Diccionario de la Lengua Española*. *Real Academia Española.* https://dle.rae.es/internet

Lowenfeld, A. (1996). *International Litigation and the Quest for Reasonableness - Essays in Private International Law.* Clarendon Press-Oxford.

Organización Mundial del Comercio. (1998). *Programa de trabajo sobre el Comercio Electrónico* (WT/L/274). https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=s:/WT/L/274.pdf&Open=True

Ortego Ruiz, M. (2015). *Prestadores de servicios de internet y alojamiento de contenidos ilícitos.* Editorial Reus.

(2020). *Sin miedo al Derecho a la protección de datos y derechos digitales* (2da ed.). Siglo XXII Legal.

Palao Moreno, G. (2017). Otros contratos. En C. Esplugues Mota (coord.), *Derecho del Comercio Internacional* (pp. 251-274). Tirant lo Blanch.

Peguera Poch, M. (2010). Sobre la necesidad de revisar el marco legal de exclusión de responsabilidad de los proveedores de servicios de intermediación. En L. Cotino Hueso, (ed.), *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías* (pp. 256-268). Publicaciones de la Universidad de Valencia.

Rauchegger, C., & Kuczerawy, A. (2020). Injunctions to remove illegal online content under the eCommerce Directive: Glawischnig-Piesczek. *Common Market Law Review*, *57*(5), 1495-1526. https://dx.doi.org/10.2139/ssrn.3728597

Rosati, E. (2019). Material, Personal and Geographic Scope of Online Intermediaries' Removal Obligations beyond Glawischnig-Piesczek,

C-18/18 and Defamation. *European Intellectual Property Review*, *41*(11), 672-682.

Soldevila Fragoso, S. (2021). La ley de servicios digitales: necesaria y polémica. *Actualidad Administrativa,* (3), 1-8.

Teruel Lozano, G.M. (2010). Apuntes generales sobre la libertad de expresión en internet. *Anales de derecho,* (28), 121-140.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Caso C-131/12, Google Spain S.L. & Google Inc. c. Agencia Española de Protección de Datos (AEPD) & Costeja González, ECLI:EU:C:2014:317 (may. 13, 2014).

Caso C-18/18, Eva Glawischnig-Piesczek c. Facebook Ireland Ltd, Conclusiones del Abogado General Sr. Maciej Szpunar, ECLI:EU:C:2019:458 (jun. 4, 2019).

Caso C-18/18, Eva Glawischnig-Piesczek c. Facebook Ireland Ltd, ECLI:EU:C:2019:821 (oct. 3, 2019).

Caso C-238/08, Google France SARL. c. Louis Vutton Malletier SA *et al.*, 2010 E.C.R. I-02417.

Caso C-324/09, L'Oréal SA *et al*. c. eBay International AG *et al*., 2011 E.C.R. I-06011.

Caso C-360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV, ECLI:EU:C:2012:85 (feb. 16, 2012).

Casos acumulados C-509/09 & C-161/10, eDate Advertising GmbH *et al.* c. X & Société MGN Ltd., 2011 E.C.R. I-10269.

Casos acumulados C-682/18 & C-683/18, Frank Peterson c. Google LLC *et al.*, Elsevier Inc. c. Cyando AG, Conclusiones del Abogado General Sr. Henrik Saugmandsgaard Øe, ECLI:EU:C:2020:586 (jul. 16, 2020).

Delfi AS c. Estonia, Ap. No. 64569/09, Eur. Ct. H.R (2015).

Digital Millennium Copyright Act, H.R. 2281, 105th Cong. (1998).

Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), 2000 O.J. (L 178) 1.

Directiva 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE, 2019 O.J. (L 130) 92.

Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM (2020) 842 final (dic. 15, 2020).

Propuesta de Reglamento del Parlamento Europeo y del Consejo para la prevención de la difusión de contenidos terroristas en línea, COM (2018) 640 final (sept. 12, 2018).

Reglamento 1215/2012 del Parlamento Europeo y del Consejo de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (refundición), 2012 O.J. (L 351) 1 (UE).

10.18800/themis.202101.005

EL VIRUS MÁS LETAL: LA NECESIDAD DE UNA ADECUADA REGULACIÓN SOBRE LAS *FAKE NEWS* EN EL PERÚ

THE MOST LETHAL VIRUS: THE NEED FOR AN ADEQUATE FAKE NEWS REGULATION IN PERU

Jacqueline Rose St. Laurent del Castillo*
Universidad del Pacífico

Antonio Sebastián Robles Vargas**
Universidad del Pacífico

New technologies have led to a 180 degree turn in the way society shares, consumes and accesses information. However, just as the media has contributed to personal and social development, the panorama in recent years has changed as a result of the growing wave of false information on the internet.

In this article, the authors determine the risks involved in spreading fake news about the COVID-19 pandemic and assess whether current national legislation, based on what international parameters have established, manages to mitigate this issue that has forced even the most developed legislations in the world to modify the scope and effects of their regulations.

Keywords: Fake news, international law, criminal law, freedom of expression.

Las nuevas tecnologías han supuesto un giro de 180 grados en la forma en que la sociedad comparte, consume y accede a la información. No obstante, así como los medios de comunicación han contribuido al desarrollo social y personal, el panorama en los últimos años ha cambiado a causa de la creciente ola de información falsa en internet.

En el presente artículo, los autores determinan los riesgos que conlleva la difusión de noticias falsas a propósito de la pandemia del COVID-19 y evalúan si la legislación nacional vigente, a partir de lo que disponen los parámetros internacionales, es la adecuada para combatir esta problemática que ha obligado incluso a las legislaciones más desarrolladas del mundo a modificar los alcances y efectos de su normativa.

Palabras clave: Fake news*; derecho internacional; derecho penal general; libertad de expresión.*

* Alumna de la Facultad de Derecho de la Universidad del Pacífico (Lima, Perú). Asociada de la Revista Forseti (DEREUP Editores). Colaboradora de la Clínica Jurídica de Libertades Informativas y Representante Estudiantil ante Asamblea Universitaria y Consejo de Facultad de la Universidad del Pacífico. Contacto: jr.stlaurentd@alum.up.edu.pe.

** Alumno de la Facultad de Derecho de la Universidad del Pacífico (Lima, Perú). Asociado de la Revista Forseti (DEREUP Editores). Miembro honorario del Círculo de Debate de la Universidad del Pacífico. Contacto: as.roblesv@alum.up.edu.pe.

Los autores agradecen a Betzabé Marciani y a Andrés Calderón por las enriquecedoras discusiones compartidas en el marco de este artículo.

Este artículo obtuvo el segundo puesto del Concurso de Artículos Jurídicos de Historial.pe organizado por Hiperderecho, con el apoyo de la Asociación Civil THĒMIS.

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 24 de febrero de 2021, y aceptado por el mismo el 17 de mayo de 2021.

I. INTRODUCCIÓN

En la actualidad, es sorprendente la rapidez con la que circula el contenido digital. En tan solo minutos una persona puede enterarse de información proveniente del otro lado del hemisferio, así como de cualquier tipo de contenido en redes sociales, portales de noticias o incluso en aplicaciones de mensajería instantánea.

Sin embargo, dentro de esta gran gama de plataformas, no resulta extraño ver circular información con contenido malicioso que pueda incluso atentar contra la salud pública y la integridad de los ciudadanos. Actualmente, existen estudios que demuestran lo anterior, como por ejemplo, el desarrollado por la compañía global de ciberseguridad Kaspersky, el cual determinó los riesgos que los usuarios corren cuando se conectan y navegan en internet crédulamente y sin cuestionamientos. El mismo reveló que en promedio el 70% de los latinoamericanos no sabe detectar o no está seguro de cómo reconocer una noticia falsa de una verdadera en internet (Diazgranados, 2020). Las cifras son aún más alarmantes al saber que quienes menos logran identificar una noticia falsa son los peruanos con 79%; seguidos por los colombianos (73%); los chilenos (70%); los argentinos y mexicanos (66%); y, finalmente, los brasileños (62%) (Diazgranados, 2020).

A esta problemática se le suman los riesgos de la desinformación frente a la incertidumbre que provoca el COVID-19. Ello porque la denominada 'infodemia'[1] puede apelar a nuestro lado emocional y no al racional, vulnerando incluso la capacidad de los individuos de tomar buenas decisiones como consecuencia del aislamiento social obligatorio, los sentimientos de angustia, ansiedad y muerte, que hacen al colectivo social mucho más sensible a las noticias. De esta manera, la pandemia silenciosamente ha logrado fomentar el pánico, el riesgo a la salud pública y mental[2] e incluso impulsar la desconfianza de la población frente a las medidas de prevención del Estado.

Frente a estos riesgos, el objetivo de este artículo es determinar si los Estados tienen la obligación de desmentir información falsa a partir de lo dispuesto por el derecho internacional y, de ser así, evaluar si el Perú cuenta con una regulación adecuada para poder cumplir esas disposiciones. Al mismo tiempo, dentro de este marco, analizaremos bajo qué supuesto se podría sancionar la difusión de *fake news*; para finalmente exponer las principales políticas que otros gobiernos han planteado para combatir su ejercicio.

Para ello, realizaremos una aproximación conceptual del término *fake news,* lo cual implicará desarrollar sus características y sus implicancias en los derechos humanos y la democracia. Luego, determinaremos si la difusión de información falsa configura un ejercicio legítimo del derecho a la libertad de información, para posteriormente evaluar la posibilidad de limitar este derecho e identificar si los Estados tienen la obligación de realizarlo como motivo de la crisis sanitaria. Por último, de cumplirse las premisas anteriores, analizaremos si el Perú cuenta con una adecuada regulación para combatir la difusión de información falsa, de conformidad con los estándares internacionales y, de no ser así, realizar un breve recuento de las principales regulaciones relacionadas a esta problemática con la finalidad de establecer qué aspectos deberían ser considerados en un futuro proyecto regulatorio.

II. APROXIMACIONES SOBRE LAS *FAKE NEWS* O NOTICIAS FALSAS

¿Qué tienen en común las campañas electorales de India en 2019 y Brasil en 2018 con los supuestos saqueos a un supermercado en Lima al inicio del confinamiento social? Ambos hechos se dieron en el marco de la difusión de *fake news*.

El presente acápite tiene como finalidad: (i) establecer una aproximación conceptual sobre el término *fake news*; (ii) identificar sus características más resaltantes; y (iii) determinar los principales problemas que genera para los derechos humanos y la democracia en un contexto de crisis sanitaria.

A. Conceptos iniciales

Con la finalidad de alcanzar el primer objetivo propuesto, es necesario saber diferenciar entre dos expresiones que habitualmente han sido utilizadas por los medios y la doctrina para aludir a la problemática planteada, estos son: *fake news* y *post-truth*.

---

1 Una 'infodemia' es "una sobreabundancia de información –en algunos casos precisa y en otros no– que hace que sea difícil para las personas encontrar fuentes fiables o una orientación adecuada cuando lo necesitan" (Organización Mundial de la Salud, 2020) [traducción libre].

2 Para más información, véase Naciones Unidas (2020) y Huarcaya Victoria (2020).

A falta de jurisprudencia nacional que defina el primer concepto, resulta necesario explorar el desarrollo doctrinario del mismo. De esta manera, Pauner Chulvi (2018) ofrece una primera aproximación conceptual al señalar que es el conjunto de "informaciones publicadas deliberadamente en medios digitales, que no han sido comprobadas ni verificadas, que carecen de fuentes identificadas y que no cuentan con la supervisión de un editor" (p. 300). Además, agrega que tienen por objetivo "influir en la opinión pública y crear inseguridad, sospechas, desestabilización para apoyar o desacreditar o, a veces, simplemente diversión" (Pauner Chulvi, 2018, p. 301).

Frente a lo expuesto, es de particular importancia aclarar qué debe entenderse por la expresión 'deliberadamente'. Esto se debe a que quien difunde información no necesariamente sabe que esta es falsa o verdadera, por lo cual ha de preguntarse lo siguiente: ¿la información falsa difundida culposamente debe calificar en estricto como *fake news*? La respuesta es clara: sí debería hacerlo. Es por ello que también debemos considerar este escenario dentro del universo de posibles *fake news*. Ante esta posibilidad, surge una interrogante adicional: ¿por qué se incluye la expresión 'deliberadamente' en la definición? La respuesta es histórica: las *fake news* han tenido como finalidad principal crear propaganda política malversa contra un candidato o servir como modelo de negocio para aumentar el número de visitas de una página gracias a la inserción publicitaria, por lo que bajo ambos escenarios el dolo siempre se encuentra presente.

Teniendo en cuenta lo anterior, definiremos a las *fake news* como las publicaciones o comunicaciones de cualquier naturaleza (no solo *online*) que –independientemente de su origen doloso o culposo– difundan información no real, pero que puede ser creíble dado un contexto específico, con la finalidad de influir en la opinión pública. Visto ello, es necesario advertir que su origen no constituye un fenómeno nuevo, pues desde las primeras repúblicas democráticas, la circulación de información poco verídica ha influido en la toma de decisiones de los ciudadanos. No obstante, a diferencia de tales circunstancias, resaltamos lo mencionado por Alonso González cuando cita uno de sus trabajos previos (Alonso González & García Orta, 2015), en tanto hoy las nuevas tecnologías permiten que el fenómeno cobre una dimensión nueva en la que entra en juego la "velocidad, amplitud y universalidad, vectores que potencian el auge de su difusión amparados en la participación, el anonimato, la fuente oculta y la dificultad para borrar su rastro" (2019, p. 31).

Junto al concepto de *fake news*, es necesario determinar su relación con el neologismo *post-truth*. De esta manera, constituye aquellas circunstancias en donde existe una "distorsión deliberada de la realidad, para crear y dar forma a la opinión pública e influir en las actitudes sociales, en las que los hechos objetivos son menos influyentes que las apelaciones a las emociones y creencias personales" (Flores Vivar, 2019, p. 203). En términos sencillos, este concepto se configura cuando una persona, motivada por sus emociones, califica información como subjetivamente real, aun cuando de sus hechos fácticos se evidencie que no lo es. A partir de ello, las *fake news* cobran importancia cuando influyen y fortalecen esta visión distorsionada de la realidad, dándole argumentos aparentes para que sobreexista.

Una vez aclarado todo lo anterior, no resultará sorprendente indicar que varios autores coinciden en que la proliferación de las denominadas *fake news* –y consecuentemente la construcción de una *post-truth*– alcanzan su máxima expresión en dos contextos: campañas electorales y emergencias (Calderón, 2020). Frente a lo expuesto, es menester identificar las características más resaltantes de este fenómeno.

B. Características de las *fake news*

A modo ilustrativo, detallaremos algunas de las características principales de las *fake news*, con la finalidad de encauzar mejor el análisis posterior. Es importante detallar que no existe una regla general sobre cómo se manifiestan las noticias falsas; sin embargo, es posible identificar algunas manifestaciones concurrentes.

En ese sentido, coincidimos con Blázquez-Ochado (2018) cuando señala que en las *fake news*: (i) existe un fuerte discurso emocional que busca cautivar la atención del lector con la finalidad de abstraerlo de la realidad y distraerlo a través de la provocación de una reacción intensa; (ii) se utiliza un vocabulario y recursos lingüísticos exagerados, como la exageración, hipérboles y circunloquios; (iii) los titulares suelen ser cortos pero impactantes; (iv) el texto que desarrolla la noticia es escaso; (v) existe una carencia de fuentes y noticias enlazadas en el artículo; (vi) hay un alto nivel de difusión en redes sociales; (vii) hay una ausencia de autor o fecha de publicación; entre otros.

Una vez identificadas las características que se suelen presentar en las noticias falsas, procederemos a identificar cómo es que con la propagación de *fake news* se vulneran nuestros derechos humanos y se presentan repercusiones en la democracia de todo Estado.

C. Vulneración de los derechos humanos y repercusiones en la democracia

Como anunciamos líneas arriba, para efectos del presente artículo, es imprescindible determinar los problemas que generan las *fake news* sobre (i) los derechos humanos y (ii) la democracia en un contexto de crisis sanitaria.

En primer lugar, la incertidumbre que provoca el COVID-19 hace que la sociedad esté más pendiente a la recepción de información de forma apremiante. Frente a este escenario, el artículo 19 de la Declaración Universal de Derechos Humanos (1948) (en adelante, la Declaración) garantiza el derecho fundamental a la libertad de expresión, el cual incluye el derecho de investigar, pero también de recibir información por cualquier medio de expresión. Al respecto, debemos incidir que el tipo de información al que se refiere la Declaración es aquella veraz, es decir, basada sobre "hechos o datos objetivos de la realidad" (Vallés, 2005). Siendo ello así, la difusión de *fake news* vulnera nuestro derecho humano a la libertad de información.

Por otro lado, es evidente que la cuarentena –sea obligatoria o voluntaria– ha tenido un impacto en la salud mental de la población, acentuando trastornos como la ansiedad y cambios en el estado de ánimo. En este escenario, el confinamiento nos expone a una búsqueda constante de información como consecuencia de la incertidumbre que genera el peligro de contagio, y, por tanto, al encuentro de noticias falsas que al presentarse con contenido negativo, agresivo y sensacionalista pueden llegar a alterar la calma, generar confusión, angustia e incluso estrés.

En ese marco, el artículo 25 de la Declaración prevé el derecho de toda persona a un nivel de vida adecuado que le asegure salud (Declaración Universal de los Derechos Humanos, 1948). Al respecto, como aseguran diversos expertos en la materia y la Organización Mundial de la Salud (en adelante, OMS) su definición involucra un estado de completo bienestar –físico, mental y social– y no la simple ausencia de enfermedad. En ese sentido, debemos calificar a la salud mental en plano de igualdad junto a la salud física, es decir, como un derecho humano.

Sobre esto último se debe agregar que las *fake news* podrían, incluso, configurar en prácticas que atentan contra la salud física; por ejemplo, mediante la propagación de falsos remedios sin base científica que lo respalde. Frente a estas circunstancias, el artículo 25 en la dimensión física que protege se encontraría comprometido.

Por otro lado, respecto a las repercusiones que podría generar en la democracia, consideramos importante "añadir un problema de credibilidad, fiabilidad y contaminación de las fuentes de información, así como de transparencia de los medios y empresas informativas, incluyendo las instituciones públicas y gobiernos" (Blázquez-Ochado, 2018, p. 14). A saber, de un lado, el tipo de información que un ciudadano reciba acerca de asuntos públicos influirá directamente en la credibilidad institucional, la confianza en las medidas gubernamentales implementadas y el control sobre su gestión. De otro lado, los medios de comunicación tradicionales no cuentan con una capacidad suficiente para contrarrestar las noticias falsas y –como resultado de los efectos de la *post-truth*– pierden credibilidad como fuentes fidedignas. En ese sentido, se configura una sociedad en donde la realidad parte de información falsa, donde no hay credibilidad en la institucionalidad pública o mediática y en donde no existe la capacidad de ponerse de acuerdo sobre hechos objetivos. Esto impide la construcción y el fortalecimiento de una democracia funcional[3].

Ante el incremento de este fenómeno y como consecuencia de los riesgos que puede causar la difusión descontrolada de información sin contrastar, las autoridades políticas de distintos países reclaman por la necesaria regulación del tema. Así, como bien señala Andersdotter (2017), países como Francia, Italia, y Alemania han propuesto medidas legislativas al respecto. En marzo de 2017, el Gobierno alemán propuso un proyecto de ley que prevé multas de hasta 50 millones de euros para aquellas redes sociales que no eliminen contenidos difamatorios o noticias falsas (Pauner Chulvi, 2018, p. 302); en Italia, se presentó una propuesta normativa para prevenir la manipulación de la información en línea y garantizar la transparencia en la web a través de la implementación de condenas civiles y penales para quienes difundan noticias que incluyan datos o hechos manifiestamente infundados o falsos (Parra Valero & Oliveira, 2018, p. 62); y, en Francia, el presidente Emmanuel Macron anunció el 3 de enero de 2018 la revisión de la legislación de los medios de comunicación franceses para combatir la difusión de noticias falsas en las redes sociales que supongan una amenaza para las democracias liberales (Fischer, 2018, p. 129).

[3] Asimismo, frente a estas reglas de verificación y contraste, que es un proceso lento y laborioso, "se contrapone al efecto de instantaneidad que prevalece sobre la prudencia y la verdad" (Blázquez-Ochado, 2018, p. 15).

Ahora bien, habiéndonos aproximado al concepto de las *fake news*, sus características y los problemas que genera, para efectos del presente artículo, corresponde determinar su relación con el derecho a la libertad de expresión.

III. *FAKE NEWS* Y EL DERECHO A LIBERTAD DE EXPRESIÓN

Los principales objetivos de este acápite serán dos: (i) determinar si la difusión de noticias falsas configura un ejercicio del derecho a la libertad de expresión; y, de ser así, (ii) resolver si el mismo puede admitir excepciones en el marco de una emergencia sanitaria. Para lograrlo, comenzaremos exponiendo los diferentes enfoques que defienden a la libertad de expresión para determinar su ámbito de protección y responder si, dentro del mismo, se encuentra el hecho de difundir información falsa o no.

A. Derecho fundamental a la libertad de expresión

Todas las constituciones de base democrática del mundo garantizan la libertad de expresión y la Constitución Política del Perú de 1993 no es la excepción puesto que hace muy extensiva su protección[4], debido que presenta como fundamentos –entre otros–: la limitación del ejercicio de poder del Estado; el desarrollo del ser humano y su autonomía individual; el fortalecimiento de la democracia; la formación de una opinión pública libre; la garantía de otros derechos fundamentales como el derecho a la igualdad; y la creación de un libre mercado de ideas (Huerta Guerrero, 2010).

Así como nuestro sistema constitucional avala la libertad de expresión bajo los fundamentos anteriormente expuestos, el desarrollo propio de este derecho y –por tanto– su ámbito de protección depende, en gran medida, de la importancia que cada ordenamiento le dé a determinados fundamentos. De esta manera, en la actualidad, la justificación de la protección a "la libertad de expresión descansa más que en el primigenio argumento individualista, derivado de las nociones de dignidad y autonomía, en su utilidad o garantía de los presupuestos del sistema democrático" (Marciani Burgos, 2005, p. 362).

1. Las teorías sobre la protección del derecho a la libertad de expresión

Para fines del presente artículo, es importante diferenciar entre dos enfoques: (i) el norteamericano que tiene como base el argumento democrático-político y, como consecuencia de este, la tesis de la posición preferente del derecho a libertad de expresión; y (ii) el europeo que se basa principalmente en la tesis humanista y, por tanto, da mayor énfasis a la dignidad del ser humano.

a. *El argumento democrático-político y el derecho preferente*

Este argumento parte del análisis que realiza Alexander Meiklejohn a la Primera Enmienda de la Constitución norteamericana y al reconocimiento que la misma otorga a la libertad de expresión como herramienta para el afianzamiento del sistema democrático y no como derecho público subjetivo. En efecto, Marciani Burgos citando a Meiklejohn enuncia lo siguiente:

> La Primera Enmienda no protege una "libertad para hablar". Protege la libertad de aquellas actividades de pensamiento y comunicación mediante las cuales nosotros "gobernamos". Está comprometida, no con un derecho privado, sino con un poder público, una responsabilidad gubernamental (2005, p. 354).

Como se observa, se resalta la libertad de expresión como fundamento para que cada ciudadano tenga la capacidad de desarrollar una mejor participación en su vida política. De esta manera, como consecuencia de la libre transmisión de información y el intercambio libre de ideas, los electores adquirirán mayor reflexión para realizar un voto consciente[5].

---

[4] Constitución Política del Perú, artículo 2:

> Toda persona tiene derecho a las libertades de información, opinión, expresión y difusión del pensamiento mediante la palabra oral o escrita o la imagen, por cualquier medio de comunicación social, sin previa autorización ni censura ni impedimento algunos, bajo las responsabilidades de ley (1993).

[5] Esta visión se ha visto respaldada en casos como los siguientes: Caso *New York Times c. Sullivan*, por medio del cual los jueces Black y Douglas señalaron que "la libertad de debatir sobre asuntos públicos y cargos públicos es incuestionablemente, tal y como lo dispone el Tribunal, el tipo de expresión que debe mantenerse en el área de la libre discusión a tenor con el diseño originario de la Primera Enmienda" (1964); caso *Grosjean c. American Press Co.*, en donde la Corte concluyó que "el mal que la Enmienda pretendía obviar era cualquier acción del gobierno tendente a impedir una discusión libre y general de los asuntos públicos tal como pudiera parecer absolutamente necesaria para preparar al pueblo para un ejercicio inteligente de sus derechos" (1936); caso *Mills c. Alabama*, por medio del cual el juez Black manifestó que "cualesquiera sean las diferencias existentes en las interpretaciones de la Primera Enmienda, estamos todos de acuerdo en que una finalidad fundamental de esa Enmienda era proteger la libre discusión de los asuntos de gobierno" (1966).

Estas conclusiones se han visto respaldadas, incluso, por la doctrina internacional. Por ejemplo, Bernal-Castro y Moya-Vargas, citando a Álvarez, han destacado la obligatoriedad de este derecho sobre la constitución de las democracias, desarrollando para ello tres aspectos particulares: "(i) La deliberación pública informada, (ii) El control sobre el poder público y (iii) La vigilancia sobre el creciente poder de las empresas privadas en la definición de los intereses públicos" (2015, p. 19). Vemos así que este derecho fundamental configura un medio indispensable para la existencia de una sociedad democrática en tanto su ejercicio permite la formación de una opinión pública y el más amplio acceso a la información por parte de la sociedad en su conjunto.

Por otro lado, en el derecho internacional, la Corte Interamericana de Derechos Humanos (en adelante, Corte IDH) en la Opinión Consultiva OC-5/85 ha destacado su valor primordial en la sociedad y en la formación de la opinión pública:

> **La libertad de expresión es una piedra angular en la existencia misma de una sociedad democrática. Es indispensable para la formación de la opinión pública**. Es también *conditio sine qua non* para que los partidos políticos, los sindicatos, las sociedades científicas y culturales, y en general, quienes deseen influir sobre la colectividad puedan desarrollarse plenamente. Es, en fin, condición para que la comunidad, **a la hora de ejercer sus opciones esté suficientemente informada** (1985, párr. 70) [el énfasis es nuestro].

No obstante, identificamos un problema principal con la teoría democrático-política que parte de "definir el contenido de lo «político» o de lo «público»" (Sánchez González, 1992, p. 59), puesto que como el propio Meiklejohn afirma, este se extiende a todos los campos de la actividad y conocimiento humano. Y es que la teoría, según esto último, no admitiría restricciones o algún tipo de discriminación siempre que los discursos o manifestaciones versen sobre asuntos públicos; es decir, la teoría deviene en absoluta. Por si fuera poco, los conflictos que esta enfrenta pueden ser evaluados, a su vez, con el establecimiento de la 'posición preferente de la libertad de expresión' (resultado de la recepción de la teoría norteamericana en otros sistemas).

El derecho preferente es una creación del Tribunal Norteamericano que "defiende la intangibilidad del derecho a la libertad de expresión debido al valor que este tiene, más que como derecho individual, como presupuesto necesario del sistema democrático" (Marciani Burgos, 2005, p. 365). Es decir, frente a los posibles conflictos a los que se enfrente la libertad de expresión con otros derechos (por ejemplo, al honor e intimidad), el primero de ellos se impondrá por constituir una garantía institucional de la opinión pública. Por esta razón, en sistemas como el norteamericano, se otorga un ámbito de protección mayor a la libertad de expresión, al punto de permitir marchas racistas en barrios judíos, que incluso son garantizadas por las fuerzas públicas, o los famosos *hate speeches*.

Ahora bien, antes de continuar abordando la problemática que genera este enfoque, es necesario entender la relación que existe entre garantías institucionales y derechos fundamentales. De esta manera, mientras las primeras representan la protección constitucional que reciben algunas instituciones consideradas necesarias en la organización política del Estado, los segundos comprenden un sistema de protección distinto en razón de su destinatario (una persona) y fin perseguido. Y es que la garantía institucional se presenta no solamente como una garantía de protección frente a la actuación del legislador, sino como una exigencia de promoción y de fomento de la institución en cuestión (Gallego Anabitarte, 1994).

Una vez aclarado lo anterior, es posible precisar que existen dos problemas alrededor del enfoque norteamericano: (i) ignora el aspecto objetivo o institucional de los derechos fundamentales, que los reconoce como elementos indispensables para la consecución de los fines sociales y colectivos proclamados constitucionalmente, en tanto configuran un factor esencial del Estado de derecho en cualquiera de sus manifestaciones; y (ii) devienen en inconsistencias para lo que plantea el ordenamiento jurídico peruano.

El segundo problema planteado es expuesto por la doctora Marciani Burgos en el texto La posición preferente del derecho a la libertad de expresión: un análisis crítico de sus fundamentos (2005), por medio del cual concluye –y coincidimos– en lo siguiente:

a) **La teoría de la posición preferente implica establecer una jerarquía de derechos fundamentales.** Nuestro sistema constitucional sitúa a todos los derechos fundamentales enunciados en la Carta Magna en pie de igualdad, admitiendo limitaciones en caso de conflicto con otros bienes jurídicos.

b) **La teoría de la posición preferente parte de una visión idealista de la opinión pública**.

c) **La teoría de la posición preferente facilita la vulneración de los derechos de la personalidad de los particulares por parte de**

los medios de comunicación. Al constituirse los medios de comunicación como verdaderos 'poderes privados' debido a la influencia social que ejercen, se coloca al individuo en una posición de indefensión al poder verse sus derechos lesionados a causa de informaciones difundidas por estos medios.

d) **La teoría de la posición preferente representa una concepción utilitarista de este derecho.** La libertad de expresión no se ve como un fin en sí mismo –derivado del principio de dignidad del ser humano– sino como un medio para alcanzar un fin: alcanzar el autogobierno o afirmar el sistema democrático existente.

Por todo lo expuesto, rechazamos como posición el enfoque norteamericano, en específico, el argumento democrático-político y, por sobre todo, la tesis del derecho preferente de la libertad de expresión por presentar a la libertad de expresión como directamente imperante frente a otros bienes jurídicos protegidos y como absoluta en el marco de la formación de la opinión pública y el afianzamiento del sistema democrático.

b. *La teoría humanista y el test de ponderación*

A diferencia del enfoque norteamericano, en Latinoamérica y Europa se le da un mayor énfasis a la teoría humanista, la cual sostiene que "la libertad de expresión tiene como fundamento el principio de la dignidad del ser humano y el libre desarrollo de su personalidad" (Marciani Burgos, 2005, p. 360). La misma nace como respuesta alternativa al argumento democrático-político, puesto que opiniones de diversos autores como la de Thomas Emerson y Rodney Smolla concluyen que las expresiones a las que se refiere la Primera Enmienda no tienen la finalidad de proteger un contenido político, sino por el contrario, que se garantice la 'autorrealización' del ser humano (Marciani Burgos, 2005, p. 360).

La teoría considera a la dignidad humana como valor intrínseco a la hora de analizar entre posibles conflictos de derecho, incluida la libertad de expresión. De esta manera, obliga a la adopción de métodos de ponderación, lo que a su vez refleja una mayor posibilidad de limitar a la libertad de expresión. Ejemplo de ello es la resolución de casos como el de Violeta Friedman, referente a expresiones dirigidas contra ciertos grupos. Al respecto, el Tribunal Constitucional de España consideró que Léon Degrelle –exjefe de las Waffen SS– había atentado contra el honor de Friedman y de las víctimas de los campos de concentración nazi al manifestar declaraciones en la revista Tiempo que negaban el acontecimiento del Holocausto (S.T.C. 214/1991, 1991).

En ese marco, sistemas como el constitucional peruano no han asumido una tesis de la posición preferente –si lo han hecho, ha sido descartada en los últimos años– y más bien, hacen uso del test de ponderación ante un eventual conflicto de derechos. Al respecto, si bien existen posiciones en la doctrina que resaltan la inseguridad jurídica que refleja la adopción de la ponderación como consecuencia de los resultados distintos que podría generar; coincidimos en que la ponderación –a la luz de las circunstancias de cada caso en concreto– debería producir una regla que se aplicase en casos sucesivos de naturaleza similar.

Una vez aclarado lo anterior, coincidimos en que la teoría humanista debe primar por sobre la norteamericana, con lo cual ante un conflicto de derechos será indispensable utilizar el test de ponderación. Ahora bien, cabe señalar que ello no implica que el ordenamiento jurídico peruano no considere a la libertad de expresión como fundamento para la construcción de la opinión pública y afianzamiento de la democracia (como se observará posteriormente); sino que implica considerarlo como un derecho preferente y menos como uno absoluto por sobre otros bienes jurídicos.

2. Manifestaciones de la libertad de expresión: derecho a la libertad de información y libertad de opinión

El artículo 2, inciso 4 de la Carta Magna hace alusión expresa a las dos manifestaciones de la libertad de expresión: la libertad de información (manifestación objetiva) y la libertad de opinión (manifestación subjetiva) (Constitución Política del Perú, 1993). Haciendo referencia particular sobre la primera –que es materia de este artículo–, el Tribunal Constitucional peruano (en adelante, TC) ha reconocido que las libertades de expresión e información son "dos derechos distintos y por tanto, cada uno presenta un objeto de protección distinto" (Expediente 0905-2001-AA/TC, 2002). Es así que

> [m]ientras que la libertad de expresión garantiza que las personas (individual o colectivamente consideradas) puedan tra[n]smitir y difundir libremente sus ideas, pensamientos, juicios de valor u opiniones, la libertad de información, en cambio, garantiza un complejo haz de libertades, que, conforme enuncia el artículo 13º de la Convención Americana de Derechos Humanos, comprende las libertades de buscar, recibir y difundir informaciones de toda índole verazmente (Expediente 0905-2001-AA/TC, 2002, fundamento 9).

Aclarado esto, es importante señalar que el TC ha establecido que el objeto de la libertad de información es la información veraz, motivo por el cual existe "un deber profesional del informador [de] respetar y reflejar la verdad substancial de los hechos" (Expediente 0905-2001-AA/TI, 2002, fundamento 10). A partir de ello, el TC delimitó dos dimensiones de la libertad de información:

> a) el derecho de buscar o acceder a la información, que no solo protege el derecho subjetivo de ser informado o de acceder a las fuentes de información, sino, al mismo tiempo, garantiza el derecho colectivo de ser informados, en forma veraz e imparcial, protegiéndose de ese modo el proceso de formación de la opinión pública y, en consecuencia, no solo al informante, sino también a todo el proceso de elaboración, búsqueda, selección y confección de la información.
>
> b) la garantía de que el sujeto portador de los hechos noticiosos pueda difundirla libremente. La titularidad del derecho corresponde a todas las personas y, de manera especial, a los profesionales de la comunicación. El objeto protegido, en tal caso, es la comunicación libre, tanto la de los hechos como la de las opiniones. Por ello, tratándose de hechos difundidos, para merecer protección constitucional, requieren ser veraces, lo que supone la asunción de ciertos deberes y responsabilidades delicadísimas por quienes tienen la condición de sujetos informantes, forjadores de la opinión pública (Expediente 0905-2001-AA/TI, 2002, fundamento 11).

En sencillo, la libertad de información implica buscar o acceder a información para ayudar a formar la opinión pública, por lo cual el proceso mediante el cual se produce dicha información es amparado. Sin embargo, tratándose de hechos –y no opiniones, que se encuentran sujetas a subjetividades–, estos deben ser veraces para ostentar protección constitucional. Dada su importancia, es importante puntualizar que el TC ha reconocido a este derecho no solo como uno subjetivo, es decir, con consecuencias únicamente para la persona que emite un determinado mensaje, sino como "un derecho que tiene un impacto en el resto de la sociedad, puesto que puede enriquecer el debate y el consecuente intercambio de ideas en la opinión pública" (Expedientes 012-2018-PI/TC & 013-2018-PI/TC, 2018, fundamento 54).

Ahora bien, a pesar de existir similitudes entre el derecho a la libertad de expresión e información que se aprecian en su faceta activa, al estar ambos destinados a la comunicación, "la distinción se evidencia en el contenido de lo que se transmite, pues mientras que en la libertad de expresión se exterioriza el pensamiento (concepción subjetiva), en la libertad de información se difunden datos o hechos [concepción objetiva]" (Defensoría del Pueblo, 2011, p. 9). Es así, entonces, que "[c]uando aquello que se comunica consiste en expresiones objetivas, esto es, datos o hechos que pueden ser contrastados con la realidad, estamos ante el ejercicio de la libertad de información" (Clínica Jurídica de Libertades Informativas, 2019, p. 9, fundamento 19).

Por otro lado, haciendo referencia a la libertad de opinión, es menester destacar –como se adelantó líneas arriba– que esta dimensión es subjetiva y no es materia de análisis del presente artículo. Ello debido a que, a pesar de ser una libertad necesaria en un Estado de Derecho, "en virtud de la cual las personas pueden transmitir y difundir libremente sus ideas, pensamientos, juicios de valor u opiniones" (Expediente 0905-2001-AA/TI, 2002, fundamento 9); al ser una libertad cuyo contenido es subjetivo, no puede ser sometida a un test de veracidad[6], por más perniciosa que esta pueda parecer. En esa línea, coincidimos con la postura de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos cuando señala que "únicamente los hechos, y no las opiniones, son susceptibles de juicios de veracidad o falsedad. **En consecuencia, nadie puede ser condenado por una opinión sobre una persona cuando ello no apareja la falsa imputación de hechos verificables**" (2017) [el énfasis es nuestro]. Es por ello que esta investigación versará sobre la base de la primera manifestación de la libertad de expresión: la libertad de información.

3. ¿La difusión de *fake news* configura una manifestación del derecho de información?

Sobre la base de lo anteriormente expuesto, cobra particular importancia la segunda dimensión de la libertad de información, esto es, la garantía de que el sujeto portador de los hechos noticiosos pueda difundir información libremente. Como ha señalado el TC, la protección constitucional solo abarca hechos difundidos que son **veraces**; por lo que a primera vista y de una interpretación literal, pare-

[6] Como señala la Clínica Jurídica de Libertades Informativas:

> Como lo advierte la Corte Suprema de los Estados Unidos, no se pueden censurar opiniones incorrectas o "ideas falsas", pues "por más perniciosa que una opinión pueda parecer, no dependemos de la consciencia de los jueces y jurados para valorar su corrección, sino de la competencia con otras ideas (2019, p. 7, fundamento 13).

cería que el TC entiende que la difusión de información falsa no configura el ejercicio del derecho a la libertad de información en tanto la información no es veraz. Frente a ello, es imprescindible diferenciar entre dos aspectos: (i) la propia configuración del derecho; y (ii) el ejercicio legítimo o ilegítimo de este.

A saber, la difusión de información no veraz –o falsa– constituye el ejercicio ilegítimo del derecho a la libertad de expresión o de información, pero se configura como derecho a la libertad de expresión o de información *per se.* En sencillo, toda persona tiene derecho a expresarse, y, como consecuencia de ello, a difundir todo tipo de manifestaciones que desee, ya sean estas expresiones, opiniones, ideas, o información objetiva, subjetiva, correcta o incorrecta; y es que la denominada 'expresión' configura un universo en sí mismo y como tal abarca todo aquello que pensemos, conozcamos y podamos materializar y exteriorizar. No obstante ello, existe consenso respecto a qué constituye un ejercicio legítimo o aceptable de esta libertad de expresión, al ser un uso ilegítimo aquel en donde resulte dañina o nociva y, por tanto, perjudicial para un tercero.

Sobre este análisis, Paulner Chulvi señala que

> la difusión de información y opiniones a través de internet se considera un ejercicio [legítimo] de las libertades de expresión e información y aquellas páginas web que publican contenidos informativos a través de la red están protegidas por estas libertades (2018, p. 310).

Sin embargo, hay que saber identificar qué constituye un ejercicio ilegítimo de este. Es así, que en la red habrá

> contenidos nocivos o dañinos que pueden resultar perjudiciales por atentar contra valores o principios y cuya difusión podrá ser limitada o restringida [*ex post*] de forma [excepcional y] proporcionada. Las noticias falsas son, en este sentido, contenido nocivo [ejercicio ilegítimo] **que pone en riesgo el pluralismo informativo y defraudan el derecho del público a recibir una información veraz** por lo que entendemos que son perfectamente arbitrables algunas medidas limitativas sobre aquellos que las difundan (Pauner Chulvi, 2018, p. 310) [el énfasis es nuestro].

Justamente de este hecho radica la importancia de precisar que no todo derecho es absoluto. Y es que, como se abordará a continuación, por más de que alguien pueda expresarse, eso no significa que dicha expresión constituya un uso legítimo *per se* del derecho y por tanto no admita ciertos límites.

En ese sentido, considerando que la difusión de noticias falsas constituye un ejercicio **ilegítimo** del derecho a la libertad de expresión en su manifestación como derecho de información, es menester determinar si es posible limitar la difusión de información falsa a raíz de lo que ha establecido la comunidad internacional.

B. ¿Es posible limitar la difusión de noticias?

Se dice que el peor enemigo de un gobierno corrupto es una sociedad informada. La difusión de información en una sociedad democrática permite que sus miembros se encuentren más informados y en una mejor posición para tomar una decisión racional. En efecto, mientras menos información circule, menos posibilidad habrá de cuestionar el actuar de un Estado, con lo cual, la difusión de noticias constituye una herramienta para garantizar este flujo de información. Sin embargo, como se anticipó, no toda difusión de información es siempre verdadera. A partir de ello, resulta importante cuestionarnos si es que en estos casos se debe o no limitar la difusión de *fake news*.

Como todo derecho, la libertad de expresión –y sus manifestaciones– no es absoluta, pues su coexistencia con otros derechos o bienes constitucionales puede devenir en conflictos de derecho. Frente a esta posibilidad, se admite que el legislador –en circunstancias excepcionales– restrinja el ejercicio de la libertad de expresión con el fin de proteger otros derechos fundamentales.

"Todo límite a la libertad de expresión debe cumplir con determinados requisitos, tanto de orden «formal» como «sustantivo», de modo tal que no se produzca una arbitraria restricción en su ejercicio" (Naranjo de la Cruz, 2000, pp. 35). Así, en el aspecto formal tanto en el derecho internacional de los derechos humanos (en adelante, DIDH) como en el derecho comparado, se ha optado por considerar a la ley como fuente autorizada para establecer una restricción al ejercicio de la libertad de expresión y sus manifestaciones. Por otro lado, el aspecto sustantivo –como bien lo dispone la Corte IDH– responde al análisis de los siguientes elementos: (i) fin legítimo; (ii) relación directa entre la limitación que se establece y el objetivo que se desea alcanzar; (iii) si existe una medida distinta menos lesiva pero igual de efectiva; y (iv) proporcionalidad con el derecho o bien constitucional que se desea proteger. A partir de esta posibilidad, analizaremos estas limitaciones a luz del derecho internacional.

La regulación internacional está orientada a proteger el derecho a la libertad de expresión (comprendidas también sus manifestaciones);

no obstante, admite la posibilidad de entablar restricciones siempre que estas se configuren en supuestos determinados y se encuentren bien formuladas. Es así que de acuerdo con el artículo 19 inciso 3 del Pacto Internacional de Derechos Civiles y Políticos:

> 3. El ejercicio del derecho previsto en el párrafo 2 de este artículo **entraña deberes y responsabilidades especiales**. Por consiguiente, **puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para**:
> a) Asegurar el respeto a los derechos o a la reputación de los demás;
> b) **La protección** de la seguridad nacional, el orden público o **la salud** o la moral públicas (1966) [el énfasis es nuestro].

Como se observa, esta regulación ha determinado que no nos encontramos frente a un derecho absoluto, pero sí frente a uno que "entraña deberes y responsabilidades especiales", por lo cual se admite su limitación de manera excepcional. Siguiendo esta línea, el Convenio Europeo de Derechos Humanos ha proscrito un enfoque similar en su artículo 10 inciso 2 al indicar que:

> Artículo 10 - Libertad de Expresión
>
> 2. **El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias**, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, **la protección de la salud** o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial (1950) [el énfasis es nuestro].

Vemos así que tanto el Pacto Internacional de Derechos Civiles y Políticos como el Convenio Europeo de Derechos Humanos han advertido que existen supuestos que permiten limitar la libertad de expresión, siendo uno de ellos la protección de la salud, lo cual pone en evidencia la necesidad de ponderar derechos. Sin embargo, señalan que para restringir este derecho habría que tener en cuenta qué límites no estarían permitidos.

Ahora bien, a pesar de que estos instrumentos internacionales no hayan establecido disposiciones acerca de qué límites son permisibles, la Convención Americana sobre Derechos Humanos (en adelante, la Convención) ha sido clara en prohibir la censura previa[7], al estipular en su artículo 13 inciso 2 que el derecho a la libertad de pensamiento y de expresión:

> 2. [...] **no puede estar sujeto a previa censura sino a responsabilidades ulteriores**, las que **deben estar expresamente fijadas por la ley y ser necesarias** para asegurar:
> a) El respeto a los derechos o a la reputación de los demás; o
> b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas (1969) [el énfasis es nuestro].

De esta manera, a través de esta prohibición, se buscaría "no interferir en el ejercicio del derecho hasta tanto no se haya consumado" (Ekmekdjian, 1996, p. 38). Es así que como bien señaló la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, "el hecho de que no se estipulen otras excepciones a esta disposición, indica la importancia que los autores de la Convención asignaron a la necesidad de expresar y recibir cualquier clase de información, pensamientos, opiniones e ideas" (2017). Dicho esto, es importante hacer hincapié en que las limitaciones permisibles a la libertad de expresión comprenden y resultan aplicables indistintamente a sus manifestaciones anteriormente señaladas: (i) información; y (ii) opinión, por más de que cada una proteja un bien jurídico distinto.

Asimismo, esta prohibición ha sido aún más delimitada por la Corte IDH en su Opinión Consultiva OC-5/85 del 13 de noviembre de 1985, resolución que dispuso lo siguiente:

> 38. [...] En esta materia toda medida preventiva significa, inevitablemente, el menoscabo de la libertad garantizada por la Convención.
> 39. **El abuso de la libertad de expresión no puede ser objeto de medidas de control preventivo sino fundamento de responsabilidad para quien lo haya cometido** [el énfasis es nuestro].

Es así que la Opinión Consultiva OC-5/85 dispuso que, de usarse la censura previa, "h[abría] una violación radical tanto del derecho de cada persona

[7] En palabras de Sagüés, la censura previa consiste en:
> "[...] **cualquier acto u omisión que inhabilite la publicación de algo** (incluyendo la no provisión de papel, la intervención arbitraria a una empresa periodística) **o que tienda a influir en esa publicación** (p.ej., propaganda discriminatoria del Estado o presiones sobre el medio) **o que dificulte que el producto informativo llegue normalmente a la sociedad**" (2001, p. 116) [el énfasis es nuestro].

a expresarse como del derecho de todos a estar bien informados [...]" (1985, párr. 54). Sobre ello, la Convención y la Corte IDH han optado por prohibir la censura previa, admitiendo su aplicación únicamente en los casos de acceso a espectáculos públicos, a fin de asegurar "la protección moral de niños y adolescentes" (Convención Americana de Derechos Humanos, art. 13 inciso 4).

Ahora, el Marco Jurídico Interamericano dispone que las limitaciones al derecho a la libertad de expresión (Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, 2010) deben concurrir en condiciones específicas derivadas del artículo 13 inciso 2 de la Convención y de un extenso desarrollo jurisprudencial del sistema interamericano, tras la realización del **test tripartito** o **juicio de ponderación**:

> **Principio de legalidad. Toda limitación a la libertad de expresión debe haber sido prevista en forma previa, expresa, taxativa y clara en una ley**, en el sentido formal y material. Al existir una prohibición absoluta de la censura previa, la ley que establezca una limitación a la libertad de expresión **solo puede referirse a la exigencia de responsabilidades ulteriores**.
>
> **Principio de legitimidad.** Toda limitación debe estar **orientada al logro de objetivos imperiosos autorizados por la Convención Americana**, orientados a la protección de los derechos de los demás, **la protección de la seguridad nacional**, del orden público, de la **salud pública** o de la moral pública.
>
> **Principio de necesidad y proporcionalidad.** La limitación debe ser **necesaria en una sociedad democrática para el logro de los fines imperiosos que se buscan**; estrictamente proporcionada a la finalidad perseguida; e idónea para lograr el objetivo imperioso que pretende lograr. El test de necesidad se aplica de forma estricta y exigente, requiriendo la demostración de que existe una necesidad imperiosa o absoluta de introducir limitaciones (Center for International Media Assistance & National Endowment for Democracy, 2017, p. 18) [el énfasis es nuestro].

De esta manera, vemos que estos tres requisitos necesitan concurrir para no incurrir en una vulneración frente a lo que dispone el ordenamiento interamericano. Sobre ello, la Comisión Interamericana de Derechos Humanos (en adelante, CIDH) y la Corte IDH han sostenido que el test debe ser aplicado de manera más estricta cuando las expresiones que se buscan limitar se relacionen con el Estado, asuntos de interés público, funcionarios públicos en ejercicio de sus funciones o candidatos a ocupar cargos públicos, particulares involucrados voluntariamente en asuntos públicos, y en general discursos y debates políticos.

Por otro lado, a pesar de que la limitación a un falso discurso sea necesario e incluso proporcional en determinados supuestos, esta debe estar calibrada a tal punto de evitar que ocurra un *chilling effect*, también entendido como la inhibición o desaliento del ejercicio legítimo del derecho a la libertad de expresión por miedo a repercusiones legales (Oxford, 2014). Ello porque el peligro de generar desincentivos frente a la divulgación de información podría incluso resultar hasta más peligroso que la información falsa en sí misma, pues esta no solo constituye un mecanismo de defensa frente a aquella información no verídica, sino también un medio a través del cual se genera información nueva y actualizada. Es por ello, que la responsabilidad ulterior surge como un mecanismo que permite el libre flujo de información y, al mismo tiempo, evita la generación de un *chilling effect*.

A partir de lo expuesto, se pueda afirmar que la censura previa no es admitida por el ordenamiento internacional. Así, el mismo formula como solución la imposición de responsabilidades ulteriores, las cuales se configuran una vez que se haya consumido una conducta. Ello ha sido reconocido por el ordenamiento peruano a partir de pronunciamientos del TC, al señalar que, aunque este derecho no sea susceptible de una autorización previa ni puede ser objeto de censura o impedimento:

> [...] ello no debe interpretarse en el sentido de que la libertad de expresión sea absoluta, de ahí que **el legislador cuente con competencia para determinar cuáles son los mecanismos de responsabilidad ulterior cuando las expresiones o datos que han sido difundidos terminan por vulnerar otros principios o derechos reconocidos en la Constitución** (Expediente 012-2018-PI/TC, 2018, fundamento 168) [el énfasis es nuestro].

Asimismo, se evidencia la necesidad de cumplir el test tripartito antes citado, a fin de restringir el ejercicio del derecho a la libertad de expresión bajo determinados escenarios.

En otras palabras, podemos afirmar que un Estado que se rige bajo lo que dispone la comunidad internacional, se encuentra en la obligación de realizar este test si es que quiere limitar el derecho a la libertad de expresión, pudiendo hacerlo de manera excepcional sin que ello signifique la posibilidad de establecer una censura previa.

En concordancia con la posibilidad de limitar el derecho a la libertad de expresión, la comunidad

internacional ha establecido además la obligación para los Estados de proteger, asegurar y salvaguardar los derechos humanos de los ciudadanos que se encuentren en su territorio o dentro de su jurisdicción[8]. De esta manera, esta obligación se traduce en un *due diligence*, es decir, un deber de conducta, pero no necesariamente de resultado. Dicho de otra manera, un Estado debe llevar a cabo todos los esfuerzos para prevenir daños que puedan afectar la salud o vida de sus ciudadanos, pero dentro de lo razonablemente posible (Coco & De Souza Dias, 2020). En el contexto de la pandemia, esta obligación implicaría que un Estado realice los esfuerzos necesarios para proteger a su población del virus[9], pero también implicaría sumar esfuerzos contra la difusión de información falsa, en tanto –como se anunció en los acápites anteriores– podrían atentar contra la salud pública y la integridad, además de afectar el propio sistema democrático debido a los riesgos y consecuencias de la desinformación y consiguiente desconfianza y seguridad de la población.

IV. LAS OBLIGACIONES DE LOS ESTADOS SEGÚN EL DERECHO INTERNACIONAL FRENTE A LA CRISIS SANITARIA

Así como en el Pacto Internacional de Derechos Civiles y Políticos, el Comité de Derechos Económicos, Sociales y Culturales ha indicado que los Estados tienen una **obligación positiva** de proteger la salud de sus ciudadanos, en donde deben tomar todas las medidas necesarias para salvaguardarla (2000)[10]. De acuerdo con Milanovich y Schmitt (2020), esta obligación positiva se cumpliría con los siguientes requisitos:

1. Los estados deben tomar todas las medidas posibles para evitar que las operaciones cibernéticas hostiles afecten negativamente a sus sistemas y capacidades de atención de la salud cuando dichas operaciones pueden causar daños a la vida o la salud humana o interrumpir la respuesta del estado a la pandemia. Es irrelevante si la operación cibernética maliciosa proviene de un actor no estatal o de otro estado.

2. **Los estados deben tomar todas las medidas posibles para promover información precisa relacionada con COVID-19 y facilitar el acceso a dicha información.**

3. **Los estados tienen el deber de suprimir la información errónea, estrictamente sujeto a los requisitos de necesidad y proporcionalidad para limitar legalmente la libertad de expresión**. Por ejemplo, el estado tendría el deber de suprimir el discurso que afirma que ingerir metanol es una cura para la COVID-19. Y en un conjunto de casos algo más amplio, a los estados se les permitiría suprimir dicha información errónea.

4. Los Estados deben tomar medidas razonables para regular y cooperar con los actores corporativos que administran plataformas digitales, como las empresas de redes sociales, que albergan la mayor parte de la expresión en línea de particulares (pp. 272-273) [traducción libre] [el énfasis es nuestro].

Resulta evidente, entonces, que los Estados tienen la obligación de proteger la salud de sus ciudadanos –y más aún en el contexto de una pandemia– a través de dos vías: (i) la promoción de información precisa; y (ii) la supresión de información errónea, respetando el test tripartito. Sin embargo, para lograrlo es de suma importancia que no se vulneren derechos como la libertad de expresión (comprendidas también sus manifestaciones), pues este resulta indispensable para luchar contra la difusión falsa de información y, con ello, garantizar una sociedad más transparente y democrática.

Frente a la obligación de proteger la salud mediante la supresión de información falsa, es necesario tomar en consideración que aquellas limitaciones a la libertad de expresión deben ocurrir en supuestos excepcionales y su limitación no debe ser ambigua, tal y como señalamos en el acápite anterior. Es así que mediante la Declaración Conjunta sobre Libertad de Expresión y "Noticias Falsas" ("Fake News"), Desinformación y Propaganda se señaló que:

> a. **Las prohibiciones generales de difusión de información basadas en conceptos imprecisos y ambiguos**, incluidos "noticias falsas" ("*fake news*") o "información no objetiva", **son incompatibles con los estándares internacionales sobre restricciones a la libertad de expresión**, conforme se indica en el párrafo 1(a), y deberían ser derogadas (Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, 2017) [el énfasis es nuestro].

[8] Véase el artículo 2 inciso 1 del Pacto Internacional de Derechos Civiles y Políticos (1966).

[9] Véase Öneryıldız c. Turquía (2004).

[10] Véase Comité de Derechos Económicos, Sociales y Culturales (U.N. Doc. E/C.12/2000/4, 2000).

En ese sentido, y en relación con lo anteriormente expuesto, es posible afirmar que dentro de la obligación positiva que tiene un Estado de velar por la salud de sus ciudadanos, esta comprende suprimir aquella información errónea o falsa, sin que ello signifique vulnerar el derecho a la libertad de información con la promulgación de leyes ambiguas o indeterminadas, cumpliendo con los requisitos de legalidad, legitimidad, necesidad y proporcionalidad previstos en el test tripartito antes mencionado. Frente a esta regulación internacional, a continuación, analizaremos si el Perú ha cumplido con establecer adecuadamente las limitaciones a este derecho en lo referente a la difusión de información falsa.

V. PREVISIÓN LEGISLATIVA PERUANA RELACIONADA A LA DIFUSIÓN DE *FAKE NEWS*

Frente a lo discutido en acápites anteriores, resulta necesario plantearnos las siguientes interrogantes: ¿las *fake news* se encuentran reguladas en el Perú? Y, de ser así, ¿cumplen con lo dispuesto en los parámetros internacionales? A partir de una revisión a la producción legislativa peruana y a las iniciativas legislativas vinculadas con el ejercicio de la libertad de expresión, encontramos que la modificación introducida en el Código Penal mediante la Ley 30076 (2013)[11], resulta ser la única previsión que puede llegar a regular en específico la figura de difusión de noticias falsas.

Esta modificación fue introducida en el 2013 con el fin de combatir la inseguridad ciudadana. De esta manera, se creó un nuevo delito denominado de 'grave perturbación de la tranquilidad pública' en el artículo 315-A del Código Penal peruano (2013).

Al respecto, el 8 de abril de 2020, el Ministerio de Justicia y Derechos Humanos (en adelante, MINJUS) publicó en sus cuentas oficiales que con motivo de la circulación de noticias falsas sobre la COVID-19, se procedería a actuar conforme a lo establecido en los artículos 438 y 315-A del Código Penal. Es así que el comunicado señalaba que:

> **Quien crea y/o difunda información falsa para obtener provecho o generar perjuicio a terceros,** será reprimido con: 2 o 4 años de pena privativa de libertad. **Si al difundir noticias falsas el autor genera pánico y perturba la tranquilidad pública**, estará sujeto a una denuncia penal y una pena de: 3 a 6 años de pena privativa de libertad (El Peruano, 2020) [el énfasis es nuestro].

Ahora, si bien el MINJUS hizo referencia expresa al artículo 438 del Código Penal como previsión legal capaz de sancionar la divulgación de noticias falsas, consideramos que el uso de este tipo penal no termina de encajar con la figura de *fake news,* a diferencia del posible debate que pueda existir en torno al artículo 315-A. En efecto, el texto legal del artículo 438 dispone lo siguiente:

> El que de cualquier otro modo que no esté especificado en los Capítulos precedentes, **comete falsedad simulando, suponiendo, alterando la verdad intencionalmente y con perjuicio de terceros**, por palabras, hechos o usurpando nombre, calidad o empleo que no le corresponde, (...) será reprimido con pena privativa de libertad no menor de dos ni mayor de cuatro años (Código Penal, 1991) [el énfasis es nuestro].

Como se observa, el artículo antes citado se refiere al delito denominado 'falsedad genérica' y forma parte del Título XIX del Libro Segundo, Parte Especial, que regula los delitos contra la fe pública (Código Penal, 1991). *Grosso modo,* este bien jurídico tutelado "comprende dos hechos: (i) la confianza del público en un documento de materialización de relaciones jurídicas; y (ii) la facilidad de este [documento] para ser falsificado" (Bramont Arias, 2003). De esta manera, se busca proteger la certeza jurídica en todo tipo de documentos, sean públicos o privados.

De esta manera, el supuesto de hecho normativo que busca sancionar este delito gira en torno del "agente cuyo comportamiento está dirigido a otorgar, expedir u ofertar certificados, diplomas u otras constancias que atribuyan falso grado académico, título profesional, título de segunda especialidad profesional, nivel de especialización u otra capacidad análoga" (López Cantoral, 2018) o, en su defecto, a sancionar la difusión de "supuestos documentos oficiales como comunicados, mensajes e incluso comunicaciones entre autoridades" (Guerrero, 2020).

Ahora bien, teniendo en cuenta que el presente apartado busca evaluar si la vía penal adoptada en la legislación peruana es la ideal para evitar la propagación de noticias falsas, consideramos que el uso del artículo que tipifica el delito de falsedad genérica resulta irrelevante para dicho propósito, pues este no tiene como finalidad jurídica evitar la difusión masiva de una noticia falsa; sino por el contrario, preservar la confianza en la documentación oficial, sea esta pública o privada.

[11] Ley que modifica el Código Penal, Código Procesal Penal, Código de Ejecución Penal y el Código de los Niños y Adolescentes y Crea Registros y Protocolos con la finalidad de combatir la inseguridad ciudadana.

Asimismo, en el supuesto negado de que el artículo sí busque evitar la difusión masiva de una noticia, consideramos pertinente evaluar el margen de acción del mismo, y es que desde la redacción de este se evidencia que no cumple con suplir todo el conjunto de causas y consecuencias que engloba a la definición de *fake news* y sus modalidades de posible difusión, en tanto este solo prevé a la documentación como único medio de difusión de falsedad. Frente a este razonamiento, corresponde, entonces, analizar el delito tipificado en el artículo 315-A del Código Penal: la grave perturbación de la tranquilidad pública.

A. El delito de grave perturbación de la tranquilidad pública

El delito de grave perturbación de la tranquilidad pública se encuentra tipificado en el artículo 315-A del Código Penal[12] y sanciona con 3 a 6 años de prisión a quien "perturbe gravemente la paz pública usando cualquier medio razonable capaz de producir alarma" (Ley 30076, 2013).

Desde una primera aproximación, surgen varias confusiones a partir de la redacción, puesto que la conducta tipificada descrita en el primer párrafo del artículo deviene en imprecisa. En efecto, los medios razonables capaces de producir alarma pueden ser variados. Asimismo, ¿qué debe entenderse como perturbación grave de la paz pública? Si bien parecería que el texto penal logra definir el concepto "perturbación grave" en su segundo párrafo, consideramos que la redacción trae consigo mayores dudas que respuestas:

> Se considera como perturbación grave a todo acto por el cual se difunda o ponga en conocimiento de la autoridad pública, medios de comunicación social o de cualquier otro por el cual pueda **difundirse masivamente la noticia**, la inminente realización de un **hecho o situación falsa o inexistente**, relacionado con un **daño o potencial daño a la vida e integridad** de las personas o de bienes públicos o privados (Código Penal, 2013, art.315-A) [el énfasis es nuestro].

En esta tipificación se logra identificar tres elementos necesarios para que un acto sea considerado de perturbación grave: (i) la difusión masiva de la noticia; (ii) la noticia debe abarcar un hecho o situación falsa o inexistente; y (iii) la noticia debe relacionarse a un hecho referido a potencial daño contra las personas y bienes. De inmediato se presentan más subjetividades en el concepto y sobre todo se generan los siguientes cuestionamientos: ¿cuándo una noticia califica como masiva? ¿cómo sé que una noticia en específico fue la causante de un daño y no otra?

Esta ambigüedad se torna aún más complicada al conocer el bien jurídico protegido por la tipificación de este delito: la tranquilidad pública. En palabras de Peña Cabrera Freyre (2016), esta debe ser entendida como:

> Un bien jurídico de orden espiritual e inmaterial a la vez, al definirse como un estado de percepción cognitiva, que tiende a formarse en la psique de los ciudadanos, a partir del cual tienen **una sensación de seguridad sobre el marco social donde han de desenvolverse**, de sentir tranquilidad, de que sus bienes jurídicos fundamentales no han de verse lesionados por ciertos actos de desvalor [...] (p. 431) [el énfasis es nuestro].

Como se observa, el concepto es tiene una pluralidad de significados, debido a que si la tranquilidad pública ha de entenderse como un estado de percepción cognitiva (sensación de seguridad), esta variará dependiendo del tipo de persona que uno es, la nacionalidad que tiene, las experiencias que haya vivido, entre otros aspectos. Es decir, la sensación de seguridad que uno pueda percibir no es igual a la sensación que otra persona pueda sentir.

Teniendo en cuenta los elementos antes descritos y antes de presentar los riesgos e impresiones que la norma causa al momento de concebirse como una especie del género de delitos de expresión, debemos advertir algunos componentes referentes al derecho penal.

---

[12] El artículo 315-A dice:

> El que perturbe gravemente la paz pública usando cualquier medio razonable capaz de producir alarma, será sancionado con pena privativa de libertad no menor de tres ni mayor de seis años.
> Se considera perturbación grave a todo acto por el cual se difunda o ponga en conocimiento de la autoridad pública, medios de comunicación social o de cualquier otro por el cual pueda difundirse masivamente la noticia, la inminente realización de un hecho o situación falsa o inexistente, relacionado con un daño o potencial daño a la vida e integridad de las personas o de bienes públicos o privados.
> Si el agente actúa en calidad de integrante de una organización criminal que, para lograr sus fines, cualesquiera que sean, utiliza como medio la amenaza de la comisión del delito de terrorismo, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años (Ley 30076, 2013).

La grave perturbación de la tranquilidad pública es un delito de resultado. Para entender su contenido, Olave Albertini (2018) nos ofrece un ejemplo a propósito del delito de homicidio:

> Si A dispara su arma contra B en un tiempo t1, causando su posterior muerte por desangramiento en un tiempo t2, A ha finalizado la ejecución de su acción en t1, a pesar de que al momento de disparar (i.e. al momento de jalar el gatillo), la muerte de B no se haya producido. Así, B muere en un tiempo distinto de aquel en que la acción de A fue ejecutada (p. 189).

De esta manera, observamos que el resultado es producido por el ejercicio de una acción específica determinable, incluso si la concreción de la misma haya terminado en un tiempo distinto.

Ahora bien, el delito de resultado exige –efectivamente– un resultado. Sin embargo, a comparación del delito de homicidio, el delito de grave perturbación de la tranquilidad pública puede desencadenar en problemas relacionados a la causalidad entre el delito base, el cual sería la difusión de noticias falsas, y el resultado; esto es, el posible daño que esta cause. Y es que una de las principales características de las *fake news* es la dificultad para determinar el origen de la noticia, con lo cual, es complicado –e incluso improbable– identificar si una noticia en específico fue la que causó realmente un daño cuando existen muchas otras noticias falsas que pudieron haber perjudicado con la misma significatividad a la ciudadanía. De esta manera, haciendo una analogía con el caso anteriormente descrito, no se podría determinar si es que A ha producido B –en un tiempo t2–, pues la noticia que puede haber provocado el daño puede haber sido una distinta a aquella que A publicó.

Por otro lado, este tipo penal debe calificarse como uno eminentemente doloso, toda vez que si se tratase de una acción culposa el tipo penal no podría castigarlo[13]. Frente a ello, la tipificación de este delito no termina por responder preguntas como ¿qué sucede si divulgo cierta información bajo la creencia de que esta es verdadera, finalmente no lo es y como consecuencia perjudico a alguien?

Ahora bien, hemos podido corroborar que dichos cuestionamientos trascienden lo conceptual y han sido materializados en la práctica. En 2017, durante el fenómeno de del Niño Costero, se anunció que quienes compartían reportes sobre saqueos inexistentes serían denunciados por la propagación de *fake news* (Ministerio del Interior, 2017). Sin embargo, a raíz de una solicitud de acceso a la información pública presentada por la Clínica Jurídica de Libertades Informativas de la Universidad del Pacífico (Arroyo *et al.*, 2020), se pudo constatar que desde el 2017 hasta la fecha no se ha encontrado proceso alguno que verse sobre el delito y/o falta contra la tranquilidad pública ni por la difusión de información falsa como delito contra el orden público. Frente a esta ausencia de información, la Clínica Jurídica presentó dos solicitudes de acceso a la información pública adicionales al Ministerio de Justicia y del Interior con la finalidad de confirmar que efectivamente no hubieran denuncias sobre la materia en el lapso de tiempo consultado, y el resultado fue el mismo: "no existe data sobre proceso penal alguno con referencia a la difusión de información falsa en el periodo señalado" (Arroyo *et al.*, 2020). Con ello, demostramos una vez más no solo la ambigüedad con la que el delito en cuestión ha sido tipificado, sino también su inaplicabilidad evidenciada en la ausencia de casos iniciados a partir de esta causal.

Hasta este punto hemos demostrado la ambigüedad y subjetividad que presenta este tipo penal desde el bien jurídico que tutela hasta la forma en la que define 'grave perturbación' y las dificultades que emergen de sus componentes penales: delito de resultado y dolo. A continuación, corresponde evaluar si la difusión de noticias falsas puede configurar un delito de grave perturbación de la tranquilidad pública.

B. ¿Las *fake news pueden* configurar un supuesto de delito de "grave perturbación de la tranquilidad pública"?

Como se ha indicado anteriormente, las noticias falsas en el contexto de una pandemia pueden generar una grave afectación a la sociedad. Como se mencionó, el MINJUS se ha pronunciado acerca de la necesidad de condenar a aquellos que difundan información falsa, en aras de cumplir con su obligación internacional de proteger la salud pública (2020). Así, busca que el delito de grave perturbación a la tranquilidad pública sea aquel aplicable en caso se incurra en este supuesto. Sin embargo, a partir del análisis expuesto cabe preguntarse ¿hasta qué punto la regulación actual permite cumplir con esta obligación internacional?

A partir del comunicado oficial publicado por el MINJUS, se ha confirmado que el delito de grave perturbación de la tranquilidad pública resulta aplicable a aquel que difunda información falsa sobre la pandemia y genere pánico. Como motivo de ello, a continuación, realizaremos el test tripartito descrito en acápites anteriores, recogido en el artículo 13 inciso 2 de la Convención y en un extenso desarrollo jurisprudencial del sistema

interamericano, a fin de demostrar que la delimitación del tipo penal no cumple con lo que la doctrina penal estipula y la comunidad internacional considera.

1. Estricta formulación de la norma que consagra la limitación o restricción (legalidad penal)

La Corte IDH ha tenido oportunidad de cuestionar el uso de normas penales en la limitación de derechos humanos (como lo es el derecho a la libertad de expresión y sus manifestaciones). De esta manera, ha postulado que las mismas, por su carácter subjetivo, "disuaden a las personas de emitir opiniones críticas respecto de la actuación de las autoridades, dada la amenaza de sanciones penales y pecuniarias" (*Kimel c. Argentina*, 2008, párr. 59). Asimismo, ha señalado que, de existir una limitante al ejercicio de este tipo de derecho, es preciso "observar los estrictos requerimientos característicos de la tipificación penal para satisfacer en este ámbito el principio de legalidad. Así, deben formularse en forma expresa, precisa, taxativa y previa" (*Kimel c. Argentina*, 2008, párr. 53).

En esa línea, en el Caso *Castillo Petruzzi c. Perú*, la Corte dispuso que en la elaboración de los tipos penales era "**preciso utilizar términos estrictos y unívocos, que acoten claramente las conductas punibles, dando pleno sentido al principio de legalidad penal**"[13] (1999, párr. 121) [el énfasis es nuestro] y que "la ambigüedad en la formulación de los tipos penales genera dudas y abre el campo al arbitrio de la autoridad" (1999, párr. 121).

En suma a ello, es menester recordar que el derecho penal se define solo por mandato legal (reserva de ley) y tiene una doble función garantista[14]: el Estado debe señalar el hecho punible y la pena aplicable. Frente a ello, Feuerbach ha señalado reiteradas veces que la esencia de este principio es *nullum crimen nulla poena sine lege certa,* es decir, "ningún delito, ninguna pena sin ley previa" (LP Pasión por el Derecho, 2018).

De esta manera, siendo la reserva de ley el principio materia de análisis más relevante para efectos del test, debemos referirnos a la característica de *lex certa* en la norma penal. De acuerdo con Roxin (citado en Simaz, 2014), la manifestación de ley cierta del principio de legalidad está dirigida hacia el legislador, a quien se le exige que formule las leyes penales –conducta prohibida y sanción– con la mayor precisión posible. Dicho autor agrega que esta garantía impone un mandato de certeza al legislador en tanto las normas que este tipifique no deben devenir en confusas, vagas e indeterminadas, sino, por el contrario, en precisas. Y es que la razón de ser de la *lex certa* justifica su razonamiento en evitar que el ciudadano común encuentre inseguridad sobre qué conducta sería pasible de una sanción.

Siendo ello así, en capítulos anteriores advertimos la ambigüedad que se desprende de la norma, así como las dificultades que emergen de sus componentes penales: dolo y derecho de resultado. Por lo que, al no cumplir con utilizar términos estrictos y unívocos que acoten claramente las conductas punibles y al no realizar la doble función garantista, el Perú estaría incurriendo en un incumplimiento de la obligación de adoptar medidas contempladas en el artículo 2 de la Convención Americana, porque no se respetarían los siguientes derechos reconocidos en la Convención: artículo 9 (principio de legalidad y de retroactividad) y artículo 13 inciso 1 (libertad de pensamiento y expresión). A pesar del incumplimiento de este punto, continuaremos con el análisis por fines académicos.

2. Idoneidad y finalidad de la restricción

En esta parte del test corresponde determinar "si la restricción constituye un medio idóneo o adecuado para contribuir a la obtención de una finalidad compatible con la Convención" (*Kimel c. Argentina*, 2008, párr. 70). La finalidad de esta medida es clara: evitar la circulación de información falsa que pueda 'perturbar la tranquilidad pública'. En ese sentido, en efecto, una sanción penal es una medida que evita la circulación de información falsa. Sin embargo –y como será analizado líneas abajo– dicha prohibición no solo desincentivará la difusión de información falsa, sino de información en general. Recordemos que una medida puede ser idónea

[13] En palabras de la Corte en *Kimel c. Argentina* (2008),

> este **implica una clara definición de la conducta incriminada**, que fije sus elementos y permita deslindarla de comportamientos no punibles o conductas ilícitas sancionables con medidas no penales. **La ambigüedad en la formulación de los tipos penales genera dudas y abre el campo al arbitrio de la autoridad**. [...] Normas como las aplicadas en el caso que nos ocupa, que no delimitan estrictamente las conductas delictuosas, **son violatorias del principio de legalidad establecido en el artículo 9 de la Convención Americana** (párr. 63) [el énfasis es nuestro].

[14] Sobre ello, Villavicencio Terreros (2013) también ha indicado que es:

> [...] esencialmente garantista; ya con él el Estado de derecho especifica el contenido y fundamento de las intervenciones que ha de realizar sobre los ciudadanos con el mayor rigor posible, y que estos tengan la posibilidad real y efectiva de conocerlo. **En tal sentido, este principio cumple una doble función garantista: el Estado debe señalar el hecho punible y la pena** (p. 135) [el énfasis es nuestro].

para obtener una finalidad prevista, pero esto no implica que la misma sea necesaria y proporcional.

3. Necesidad de la medida utilizada

En *Kimel c. Argentina*, "la Comisión [Interamericana] consideró que el Estado tuvo otras alternativas [...] menos restrictivas que la aplicación de una sanción penal" (2008, párr. 72). Con ello la Corte ha sido reiterativa en su decisión de considerar al derecho penal como el medio más restrictivo y severo para establecer responsabilidades respecto del ejercicio de un derecho de expresión al "resultar contraria al principio de intervención mínima y de **ultima ratio** del derecho penal" (*Kimel c. Argentina*, 2008, párr. 76) [el énfasis es nuestro].

En esa línea, se puede afirmar que "el poder punitivo solo se [debe] ejerce[r] en la medida estrictamente necesaria para proteger los bienes jurídicos fundamentales de los ataques más graves que los dañen o pongan en peligro" (*Kimel c. Argentina*, 2008, párr. 76) lo que no sucede en el caso en concreto de la difusión de noticias falsas, al poder adoptarse alternativas menos lesivas para proteger el bien jurídico de la salud, que serán discutidas con mayor profundidad en el siguiente acápite. Un ejemplo de ello sería la adopción de medidas de promoción que concedan herramientas a las personas para aprender a detectar si una noticia es falsa, sin que ello signifique vulnerar aspectos como control de información, censurar información, el uso de medidas penales desproporcionadas, etc. Con ello, esta medida no sería necesaria para obtener el fin anhelado.

4. Estricta proporcionalidad de la medida

En este último paso, "se considera si la restricción resulta estrictamente proporcional, de tal forma que el sacrificio inherente a aquella no resulte exagerado o desmedido frente a las ventajas que se obtienen mediante tal limitación" (*Chaparro Álvarez y Lapo Íñiguez c. Ecuador*, 2007, párr. 93). Es en línea con ello que la Corte ha indicado que "[...] la restricción debe ser proporcional al interés que la justifica y ajustarse estrechamente al logro de ese legítimo objetivo, interfiriendo en la menor medida posible en el efectivo ejercicio del derecho a la libertad de expresión" (*Kimel c. Argentina*, 2008, párr. 83)[15].

En el caso en concreto, para determinar si la restricción logra una importante satisfacción en cuanto al derecho a la salud, sin hacer nugatorio el derecho a la libertad de expresión, se tendrá que analizar:

> (i) el grado de afectación de uno de los bienes en juego, determinando si la intensidad de dicha afectación fue grave, intermedia o moderada; (ii) la importancia de la satisfacción del bien contrario y (iii) si la satisfacción justifica la restricción del otro (*Kimel c. Argentina*, 2008, párr. 84).

Al respecto, anteriormente la Corte ha considerado que "las consecuencias del proceso penal en sí mismo, la imposición de la sanción, [...] y el efecto estigmatizador de la condena penal" (*Kimel c. Argentina*, 2008, párr. 85) constituyen una afectación grave de la libertad de expresión. Si bien no cabe duda de que el bien jurídico que se busca proteger es de vital importancia, pues la preservación de la salud es prioritaria –sobre todo en un contexto como este–, la limitación de su ejercicio no lo justifica, pues en línea con lo señalado en el caso *Kimel c. Argentina*, "el recurso penal genera un fuerte efecto inhibidor" (2008, párr. 73), con lo cual esta medida produce más daños que beneficios, al provocar un *chilling effect* sobre quienes buscarán difundir información verdadera.

De lo expuesto, corresponde precisar que, aunque se cumpla con el requisito de idoneidad, existe un claro incumplimiento con los requisitos de legalidad, necesidad y proporcionalidad. En ese sentido, queda claro que esta disposición normativa no cumple de manera concurrente con los requisitos que el test tripartito dispone ni con los principios sobre los cuales se fundamenta el derecho penal. Por ello y por lo expuesto, coincidimos en que se debe modificar la previsión legal por ser insuficiente, indeterminada e ilegal desde un punto de vista internacional.

VI. REGLAS ESTATALES SOBRE LA REGULACIÓN DE LAS FAKE NEWS

Hasta el momento, se ha evidenciado que no existe una regulación legal específica sobre *fake news* en el Perú y que, por el contrario, encontramos una regulación penal imprecisa e indeterminada que atenta contra lo dispuesto por la regulación internacional. En ese sentido, acorde con la obligación de los Estados a proporcionar acceso adecuado a información precisa según lo prescrito por el DIDH y más aún, ser vías de promoción de información precisa relacionada al COVID-19, es necesario contar con una adecuada regulación

[15] Véase también Opinión Consultiva OC-5/85 (1985); *Herrera Ulloa c. Costa Rica* (2004, párrs. 121 & 123); *Palamara Iribarne c. Chile* (2005, párr. 85); y *Claude Reyes y otros c. Chile* (2006, párr. 91).

legal que esté impedida de usar medidas desproporcionadas para combatir la desinformación –como la censura– y que cumpla con la evaluación del test tripartito.

En ese sentido, consideramos pertinente realizar un breve recuento de las principales regulaciones vigentes sobre las *fake news* a fin de establecer qué aspectos deben ser considerados en un futuro proyecto de política pública. Al respecto, consideramos pertinente mencionar tres en específico: Reino Unido, España y Colombia. Las razones que giran alrededor de esta decisión son cuatro: (i) estos países, al igual que el Perú, no cuentan con una legislación aplicable a las *fake news*; (ii) sus propuestas no entran en conflicto con el principio de neutralidad de red; (iii) sus acciones no solo están dirigidas a las entidades públicas sino también al comportamiento de la ciudadanía; y, (iv) en el caso de Colombia, la realidad regulatoria se encuentra más próxima a la del ordenamiento peruano[16].

A. Reino Unido

Reino Unido si bien no cuenta con legislación específica aplicable a la figura de *fake news*, ha desarrollado políticas públicas que abarcan, por un lado, el uso de respuestas preventivas destinadas a combatir información errónea que rodea eventos predecibles; y, por otro lado, respuestas que siguen un plan predeterminado para eventos imprevistos.

En efecto, en el año 2018, el Cabinet Office –ministerio dedicado a crear políticas sobre innovación en los servicios del Estado– promulgó el Rapid Response Unit, un programa destinado a combatir la propagación de noticias falsas en tiempos de crisis (Bartosch, 2018). De esta forma, en el año 2020, con la ayuda de la National Security Communications Team*, se* desarrolló el Plan FACT[17], plan que busca: (i) monitorear en línea fuentes de noticias y redes sociales públicas para identificar temas, discusiones o historias que promuevan noticias e información falsa; (ii) valorar el nivel de riesgo identificado y establecer medidas al respecto si fuese necesario; (iii) crear contenido apropiado con el objetivo de rebalancear la narrativa y promover información oficial; y (iv) asegurarse de que el contenido creado en el punto anterior sea altamente visible y accesible.

A diferencias de otras regulaciones[18], el ordenamiento inglés ha planteado soluciones que no involucran obligaciones, sanciones o el control directo de plataformas digitales como –entre otros aspectos– eliminar contenido de manera inmediata o dentro de un límite de tiempo mínimo, promover incentivos a los proveedores de las plataformas para la reducción de difusión de contenido nocivo o dañino o disponer de lineamientos que vulneren principios como el de neutralidad de red.

En primer lugar, el Plan FACT busca realizar un análisis que permite identificar, analizar, contrastar y comprobar información calificada como falsa, para luego realizar actividades de comunicación digital dirigidas a audiencias clave. Este enfoque dista del que busca únicamente eliminar contenido 'aparentemente falso' que se ha venido gestando ante la apremiante necesidad de obtener información veraz.

En segundo lugar, la dinámica del Plan FACT no obliga a los portales a eliminar contenido como motivo de una eventual multa basada en el falso discurso de estar frente a una regulación 'legítima'. Frente a ello, cabe preguntarse: ¿qué consecuencias trae consigo la imposición de sanciones o, de otro lado, incentivos? Implicaría que las plataformas eliminen, mas no revisen, evalúen o comprueben el contenido que se ha solicitado eliminar. Como se observa, la solución inglesa trabaja a partir de hechos ya difundidos y no configura una presencia censuradora *ex ante*.

En tercer lugar, la naturaleza abierta del internet ha generado que los gobiernos e incluso empresas proveedoras de servicios de internet opten por preferir que se legisle en el sentido de favorecer el surgimiento de redes no neutrales. Existe regulaciones que se inmiscuyen en el universo de control propio de cada plataforma, contraviniendo principios

[16] Como señala Carpizo,

> En este amplio campo se encuentran esfuerzos de integración económica y también política; tribunales, cortes y parlamentos supranacionales, así como mecanismos de consulta en los más diversos aspectos y cuestiones. Asimismo, se han venido desarrollando instituciones constitucionales que adquieren dimensión o perspectiva latinoamericana. En tal virtud, se hace referencia al juicio o recurso de amparo latinoamericano o al ombudsman criollo (2005, p. 952).

[17] Véase Government Communication Service (2018).

[18] Por ejemplo,

> Por disposición del Gobierno Alemán los grandes agentes de internet están sometidos a la NetzDG, normativa que obliga a plataformas con más de dos millones de usuarios en el país a retirar contenidos que pudieran ser constitutivos de delitos en menos de 24 horas desde la recepción de la denuncia por parte de un usuario (Magallón Rosa, 2019, pp. 334-335).

como el de neutralidad de red que, según un informe de la Organización de los Estados Americanos, busca proteger la libertad de acceso y elección de los usuarios, de modo que los contenidos en internet no estén direccionados, condicionados o restringidos por privados o gobiernos (2013, p. 500). En contraposición, el Plan FACT busca desmentir y luego, a través de su Comité, no eliminar inmediatamente el contenido de la información en red u obligar a las plataformas a determinadas regulaciones que pueden devenir en subjetivas e incluso limitantes. Y es que cabe hacer la precisión que una posterior eliminación de información una vez identificada como falsa sí sería necesaria.

Al respecto, el Reino Unido, además, ha creado el Comité Rapid Response Unit que trabaja como un órgano especializado para reprimir la información errónea en línea sobre el COVID-19. Esta unidad también coordina con los departamentos del gobierno de manera inmediata con el propósito de implementar una respuesta activa. Tales coordinaciones pueden involucrar una refutación directa en las redes sociales, trabajar con las mismas plataformas digitales para eliminar contenido dañino o garantizar que las campañas de salud pública se promuevan a través de fuentes confiables.

Por otro lado, consideramos importante traer a colación la implementación de un código ético obligatorio para las empresas de tecnología, tal y como se realizó en el Reino Unido. Y es que

> en un momento en el que muchos actores políticos parecen creer que la solución a la desinformación en internet es una ley contra las *fake news*, el informe [final del grupo de expertos de la UE sobre *fake news* y desinformación digital] claramente especifica que no lo es, instando a la cautela y señalando su escepticismo hacia cualquier regulación de contenido [de esta naturaleza] (Magallón Rosa, 2019, p. 329).

A diferencia de una ley en sentido estricto, un código de ética se configura como una medida de carácter social en donde existe autovinculación y autorregulación. El objetivo de su implementación es excluir el control del Estado sobre la toma de decisiones directas de las plataformas digitales, pero también que estos sean los que determinen sus sanciones, independientemente del proceso civil al que podrían ser citados.

Por último, consideramos que "medidas como la alfabetización digital deberían entrar dentro de cualquier iniciativa promovida por los países" (Magallón Rosa, 2019, p. 341). De esta manera, al igual que el Plan FACT, actualmente existen otros planes en desarrollo como el denominado RESIST Model[19] y la campaña Don't Feed the Beast[20] que buscan instaurar en la ciudadanía una cultura dirigida a contrarrestar la difusión de noticias falsas, la cual se basa en el fomento de la capacidad, enseñanza y libertad de la ciudadanía de detectar por sí misma si una noticia o grupo de noticias es falsa y así decidir difundirla o no.

B. España

En 2018 la Comisión de Seguridad Nacional del Congreso de los Diputados aprobó una propuesta que obligaba al Gobierno español a reforzar los medios materiales y humanos dedicados a combatir las campanas de desinformación e instaba al mismo a:

1. Participar de manera activa en el proceso de construcción de la estrategia de la UE para detener la difusión de noticias falsas en línea.
2. Impulsar que, sin perjuicio de los objetivos actualmente asignados a la East Stratcom Task Force, se ampliara su rango de acción a las campañas de desinformación que pudieran ser detectadas respecto a los Estados miembros.
3. Desplegar las acciones necesarias para proceder al refuerzo inmediato en medios humanos y materiales del East Stratcom Task Force perteneciente al Servicio de Acción Exterior Europeo (Magallón Rosa, 2019, p. 338).

Como se observa, la propuesta califica como una regulación que busca elaborar métodos especializados para determinar la veracidad de la información y contrastar las mismas con hechos objetivos.

C. Colombia

En Colombia, al igual que en Perú, Reino Unido y España, no existe una regulación expresa que regule las *fake news*; no obstante, es menester mencionar que existe un proyecto de ley que busca aumentar la alfabetización digital de su población.

El Proyecto de Ley 027/2020C, como lo adelantamos, tiene como objetivo establecer un modelo educativo a favor de la alfabetización mediática y digital dentro del territorio colombiano (2020). De esta manera, busca crear programas para que los ciudadanos tengan la capacidad de evaluar

[19] Véase Government Communication Service (2019).

[20] Véase Law Library – Library of Congress (2019).

críticamente los contenidos de los medios de información y tomen decisiones fundamentadas a partir de criterios objetivos, pero también controlados por ellos mismos.

De esta manera, el Proyecto propone que las instituciones educativas públicas y privadas deban incluir contenidos y temas sobre el fenómeno de la desinformación, las noticias falsas, y la importancia de reconocer los criterios de veracidad en la búsqueda, selección y utilización de información contenida en internet, siendo los criterios mínimos de veracidad los siguientes: contexto, credibilidad de la fuente, construcción del contenido, corroboración y comparación.

VII. REFLEXIONES FINALES

En los últimos tiempos ha aumentado de manera exacerbada la producción y difusión de *fake news* o noticias falsas, situación que se agrava ante contextos de crisis o de emergencia sanitaria, lo que puede atentar contra la salud pública y la integridad de las personas, además de afectar el propio sistema democrático debido a los riesgos y consecuencias de la desinformación y consiguiente desconfianza y seguridad de la población.

Ante esta situación, el Estado ostenta una obligación positiva de garantizar que la información que se difunda en el marco de la pandemia sea veraz, motivo por el cual requiere adoptar medidas que promuevan la difusión de información veraz y supriman o desmientan información errónea y falsa, siempre que superen el test de proporcionalidad y estén conforme a los estándares internacionales que garantizan una sociedad realmente democrática, a fin de evitar una limitación arbitraria de las libertades de expresión y de información. A partir de ello, se admite una limitación a la libertad de expresión –en su manifestación de libertad de información– en el caso de difusión de noticias falsas, al ser este un ejercicio ilegítimo del derecho a la libertad de expresión.

Sobre la base de esta obligación, coincidimos en que el Perú ha transgredido las disposiciones internacionales sobre la adecuada y permitida limitación al derecho a la libertad de expresión, a través de su –intento de– regulación penal, al ser esta manifiestamente imprecisa y ambigua, y por no respetar a la vía penal como última ratio. Por ello, instamos a que los parámetros internacionales sobre la regulación de la libertad de expresión sean respetados e incorporados al cuerpo normativo peruano, además de que se inutilice la vía penal como mecanismo de lucha contra la difusión de noticias falsas. Por el contrario, resulta indispensable que se opte por mecanismos alternativos para desmentir y posteriormente eliminar información falsa, así como políticas que busquen aumentar la alfabetización digital en la población.

REFERENCIAS

Access Now (2020). *Recomendaciones para los estados para combatir la desinformación y defender la libre expresión durante COVID-19*. https://www.accessnow.org/cms/assets/uploads/2020/05/Combatiendo-Desinformacion-Defendiendo-Libre-Expresion.pdf

Alonso González, M. (2019). Fake News: desinformación en la era de la sociedad de la información. *Ámbitos. Revista Internacional de Comunicación*, (45), 29-52. http://dx.doi.org/10.12795/AMBITOS

Alonso González, M., & García Orta, M. J. (2015). Noticias falsas en Internet: difusión viral a través de las redes sociales. En A.I. Reis, F. Zamith, H. Bastos & P. Jerónimo (orgs.), *Livro de Atas do IV Congresso Internacional de Ciberjornalismo* (pp. 394-405). Observatório de Ciberjornalismo. http://dx.doi.org/10.12795/Ambitos.2019.i45.03

Álvarez, J.D. (2011). *Libertad de expresión y litigio de alto impacto*. Universidad de los Andes.

Andersdotter, K. (2017). Fatti alternativi e *fake news*: La verificabilità nella società dell'informazione. *AIB Studi*, *57*(1), 5-6. http://doi.org/10.2426/aibstudi-11618

Arroyo, T., Montero, P., Ruiz, G., & St. Laurent, J. (4 de enero de 2021). #INFODEMIA: ¿Informar o condenar? [Entrada de blog]. https://clinicajuridica.up.edu.pe/category/blog/

Bartosch, F. (17 de octubre de 2018). How the Rapid Response Unit actually works (and why it's important). *Prweek Regions*. https://www.prweek.com/article/1496346/rapid-response-unit-actually-works-and-why-its-important

Bernal-Castro, C. A., & Moya-Vargas, M. F. (2015). Democracia y libertad de expresión. En C. A. Bernal-Castro & M. F. Moya-Vargas, *Libertad de expresión y proceso penal* (pp. 13-24). Universidad Católica de Colombia.

Blázquez-Ochado, M. (mayo de 2018) *El problema de las noticias falsas: detección y contramedidas* [documento de conferencia]. XV Seminario Hispano-Mexicano de Investigación en Biblioteconomía y Documentación, Ciudad de México, México.

Bolton, D. M., & Yaxley, J. (2017). Fake news and clickbait – natural enemies of evidence-based medicine. *BJU International*, (119), 8-9. http://doi.org/10.1111/bju.13883

Bramont Arias, L. A. (2003). *Código Penal anotado* (4ta ed.). Editorial San Marcos.

Calderón, A. (16 de marzo de 2020). El virus de la desinformación. *El Comercio*. https://elcomercio.pe/opinion/columnistas/el-virus-de-la-desinformacion-por-andres-calderon-noticia/

Carpizo, J. (2005). Derecho constitucional latinoamericano y comparado. *Boletín mexicano de derecho comparado*, *38* (114), 949-989. http://dx.doi.org/10.22201/iij.24484873e.2005.114.3851

Center for International Media Assistance & National Endowment for Democracy (2017). *Estándares internacionales de libertad de expresión: Guía básica para operadores de justicia en América Latina*. https://www.corteidh.or.cr/tablas/r37048.pdf

Chilling effect (2014). En *Dictionary of Journalism*. Oxford. https://www.oxfordreference.com/view/10.1093/acref/9780199646241.001.0001/acref-9780199646241-e-228

Coco, A., & De Souza Dias, T. (24 de marzo de 2020). Part I: Due Diligence and COVID-19: States' Duties to Prevent and Halt the Coronavirus Outbreak. *EJIL: Talk!.* https://www.ejiltalk.org/part-i-due-diligence-and-covid-19-states-duties-to-prevent-and-halt-the-coronavirus-outbreak/

Defensoría del Pueblo (2011). *Situación de la libertad de expresión en el Perú setiembre 1996 – setiembre 2000, Informe Nº 48*. https://www.defensoria.gob.pe/wp-content/uploads/2018/05/informe_48.pdf

Diazgranados, H. (4 de febrero de 2020). 70% de los latinoamericanos desconoce cómo detectar una fake news. *Kaspersky daily*. https://latam.kaspersky.com/blog/70-de-los-latinoamericanos-desconoce-como-detectar-una-fake-news/17015/

Ekmekdjian, M.A. (1996). *Derecho a la información. Reforma constitucional y libertad de expresión. Nuevos aspectos.* Depalma.

El Peruano (9 de abril de 2020). Seis años de cárcel por difundir noticias falsas. *El Peruano*. https://elperuano.pe/noticia/94165-seis-anos-de-carcel-por-difundir-noticias-falsas

Fake News (2020). En *Oxford English Dictionary*. https://www.oed.com/

Fischer, T. (2018). Editorial: IA, alternative facts and fake news – Is the post-factual turn starting to turn?. *Impact Assessment and Project Appraisal*, *36*(2), 129-130, https://doi.org/10.1080/14615517.2018.1426846

Flores Vivar, J. M. (2019). Inteligencia artificial y periodismo: diluyendo el impacto de la desinformación y las noticias falsas a través de los bots. *Doxa Comunicación Revista interdisciplinar de estudios de comunicación y ciencias sociales*, (29), 197-212. http://dx.doi.org/10.31921/doxacom.n29a10

Gallego Anabitarte, A. (1994). *Derechos Fundamentales y garantías institucionales: análisis doctrinal y jurisprudencial (derecho a la educación: autonomía local, opinión pública).* Civitas.

Government Communication Service [Reino Unido] (2019). *Government Communication Plan 2019/20*. https://communicationplan.gcs.civilservice.gov.uk/wp-content/uploads/2019/04/Government-Communication-Plan-2019.pdf

(2018). *5 Trends in Leading-Edge Communications*. https://perma.cc/4BDP-JTRN

Guerrero, C. (13 de abril de 2020). Combatiendo las noticias falsas durante la crisis del COVID-19. *Hiperderecho*. https://hiperderecho.org/2020/04/combatiendo-las-noticias-falsas-durante-la-crisis-del-covid-19/

Huarcaya Victoria, J. (2020). Consideraciones sobre la salud mental en la pandemia del COVID-19. *Revista peruana de medicina experimental y salud pública*, *37*(2), 327-334. https://doi.org/10.17843/rpmesp.2020.372.5419

Huerta Guerrero, L. (2010). Libertad de expresión: fundamentos y límites a su ejercicio. *Pensamiento Constitucional*, *14*(14), 320-344.

Jiménez Ulloa, A. C. (2010). *La libertad de expresión en la jurisprudencia de la Corte Interamericana y del Tribunal Europeo de Derechos Humanos*. Universidad Externado de Colombia.

Law Library of Congress [Estados Unidos] (2019). *Government Responses to Disinformation on Social Media Platforms*. Global Legal Research Directorate. https://www.loc.gov/law/help/social-media-disinformation/social-media-disinformation.pdf

López Cantoral, E. (23 de octubre de 2018). El delito de falsedad genérica agravada. *LP Pasión por el Derecho*. https://lpderecho.pe/delito-falsedad-generica-agravada/

LP Pasión por el Derecho (22 de marzo 2018). Von Feuerbach, el autor de la fórmula «nullum crimen, nulla poena sine praevia lege poenali». *LP Pasión por el Derecho*. https://lpderecho.pe/paul-johann-anselm-von-feuerbach-autor-la-maxima-nullum-crimen-nulla-poena-sine-praevia-lege-poenali/

Magallón Rosa, R. (2019). La (no) regulación de la desinformación en la Unión Europea. *Revista de Derecho Político*, (106), 319-347. https://doi.org/10.5944/rdp.106.2019

Marciani Burgos, B. (2005). La posición preferente del derecho a la libertad de expresión: un análisis crítico de sus fundamentos. *Pensamiento Constitucional*, *11* (11), 352-378.

Milanovic, M., & Schmitt. M. (2020). Cyber Attacks and Cyber Misinformation Operations during a Pandemic. *Journal of National Security Law,* (11), 247-284.

Ministerio del Interior [@MininterPeru]. (20 de marzo de 2017). *El ministro del Interior, @CarlosBasombrio, anunció que denunciarán a más de 20 personas por difundir rumores sobre saqueos en Lima* [Tweet]. Twitter. https://twitter.com/i/status/843809476100657152

Naciones Unidas (2020). *Policy Brief: COVID-19 and the Need for Action on Mental Health*. https://www.un.org/sites/un2.un.org/files/un_policy_brief-covid_and_mental_health_final.pdf

Naranjo de la Cruz, R. (2000). *Los límites de los derechos fundamentales en las relaciones entre particulares: la buena fe*. Centro de Estudios Políticos y Constitucionales.

Olave Albertini, A. (2018). El delito de hurto como tipo de delito de resultado. *Política Criminal*, *13*(25), 175-207.

Organización de los Estados Americanos [OEA] (2020). *Informe sobre la libertad de expresión e internet.* http://www.oas.org/es/cidh/expresion/docs/informes/internet/informe_fe_internet_2013.pdf

Organización Mundial de la Salud (2020). *Novel Coronavirus(2019-nCoV) Situation Report - 13*. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf

Orgaz, C. (15 de abril de 2020). Dióxido de cloro, el peligroso químico que se promociona como cura para el covid-19 y sobre el que advierten los expertos. *BBC News.* https://www.bbc.com/mundo/noticias-52303363

Parra Valero, P., & Oliveira, L. (2018). Fake news: una revisión sistemática de la literatura. *Observatorio,* (1), 54-78.

Pauner Chulvi, C. (2018). Noticias falsas y Libertad de Expresión e Información - El control de los contenidos informativos en la red. *Revistas UNED*, (41), 297-318.

Peña Cabrera Freyre, A.R. (2016). *Derecho Penal - Parte Especial* (tomo IV). Idemsa.

Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (2010). Marco jurídico interamericano sobre el derecho a la libertad de expresión. *Organización de los Estados Americanos.* http://www.oas.org/es/cidh/expresion/docs/cd/sistema_interamericano_de_derechos_humanos/index_MJIAS.html

(2017). Declaración Conjunta Sobre Libertad De Expresión Y "Noticias Falsas" ("Fake News"), Desinformación Y Propaganda. http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1056&lID=2

(24 de abril de 2017). *La Relatoría Especial manifiesta preocupación ante nueva condena penal por difamación contra columnista y defensor de derechos humanos en Perú* [Comunicado de prensa R50/17]. https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1061&lID=2

Sagüés, N. (2001). *Teoría de la Constitución*. Astrea.

Sánchez González, S. (1992). Sobre la Libertad de Expresión en el mundo anglosajón. *Revista de Administración Pública*, (127), 45-83.

Simaz, A. (2014). Principio de Legalidad e Interpretación en el Derecho Penal: Algunas consideraciones sobre la posibilidad de interpretar extensivamente la ley sustantiva. *Revista de derecho Penal y Criminología*, (7), 49-72.

Vallés, A. (2005). *Curso de Derecho de la Comunicación Social*. Editorial Tirant lo Blanch.

Villavicencio Terreros, F. (2013). *Derecho penal - Parte general* (4ta ed.). Grijley.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Castillo Petruzzi y otros c. Perú, Fondo, Reparaciones y Costas, Inter-Am. Ct. H.R. (ser. C) No. 52 (may. 30, 1999).

Chaparro Álvarez y Lapo Íñiguez c. Ecuador, Excepciones Preliminares, Fondo, Reparaciones y Costas, Inter-Am. Ct. H.R. (ser. C) No. 170 (nov. 21, 2007).

Claude Reyes y otros c. Chile, Fondo, Reparaciones y Costas, Inter-Am. Ct. H.R. (ser. C) No. 151 (sep. 19, 2006).

Código Penal [CP], Decreto Legislativo 635, Diario Oficial *El Peruano*, 8 de abril de 1991 (Perú).

Constitución Política del Perú [Const.] (1993).

Convención Americana Sobre Derechos Humanos (Pacto de San José), nov. 22, 1969, O.A.S.T.S. No. 36.

Convenio Europeo de Derechos Humanos para la Protección de los Derechos Humanos y de las Libertades Fundamentales, 4 de noviembre de 1950, 213. U.N.T.S. 221.

Declaración Universal de los Derechos Humanos, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (10 de diciembre de 1948).

General Comment No. 14: The right to the highest attainable standard of health (article 12 of the International Covenant on Economic, Social and Cultural Rights), Rep. of the ESCOR, Comm. on Economic, Social and Cultural Rights, 22nd Sess., U.N. Doc. E/C.12/2000/4 (ago. 11, 2000).

Grosjean c. American Press Co., Inc., 297 US 233 (1936).

Herrera Ulloa c. Costa Rica, Excepciones Preliminares, Fondo, Reparaciones y Costas, Inter-Am. Ct. H.R. (ser. C) No. 107 (jul. 2, 2004).

Infectious Disease Control and Prevention Act, Act. No. 14286, 2 de diciembre, 2016 (Corea del Sur). *Traducido por* Korea Legislation Research Institute. https://elaw.klri.re.kr/kor_service/lawView.do?hseq=40184&lang=ENG

Informe jurídico de la Clínica Jurídica de Libertades Informativas de la Universidad del Pacífico como Amicus Curiae en defensa de Paola Ugaz, 10 de junio de 2019, Eguren Anselmi c. Ugaz Cruz, Quinto Juzgado Penal Unipersonal de Piura, Expediente 4772-2018-0-2001-JR-PE-05 (Perú).

Informe Nº 11/96-Caso 11.230-Chile (Martorell), Rep. Inter-Am. Ct. H.R. 11 (may. 3, 1996).

Kimel c. Argentina, Fondo, Reparaciones y Costas, Inter-Am. Ct. H.R. (ser. C) No. 177 (may. 2, 2008).

Ley 30076, Ley que modifica el Código Penal, Código Procesal Penal, Código de Ejecución Penal y el Código de los Niños y Adolescentes y Crea Registros y Protocolos con la finalidad de combatir la inseguridad ciudadana, Diario Oficial *El Peruano,* 19 de agosto de 2013 (Perú).

Mills c. Alabama, 384 US 214 (1966).

New York Times c. Sullivan, 376 US 254 (1964).

Öneryıldız c. Turquía, App. No. 48939/99 Eur. Ct. H. R. (2004).

Opinión Consultiva OC-5/85, Inter-Am. Ct. H.R. (ser. A) No. 5 (nov. 13, 1985).

Pacto Internacional de Derechos Civiles y Políticos, dic. 16, 1966, 999 U.N.T.S. 171.

Palamara Iribarne c. Chile, Fondo, Reparaciones y Costas, Inter-Am. Ct. H.R. (ser. C) No. 135 (nov. 22, 2005).

Proyecto de Ley 027/2020C, Por medio del cual se establecen las bases para un modelo de educación digital y flexible y se promueve la alfabetización mediática y digital para la identificación de noticias falsas, fomentar un uso responsable de las redes sociales desde la educación básica y media, y se dictan otras disposiciones, 20 de julio de 2020 (Colombia).

S.T.C., nov. 11, 1991 (No. 214/1991) (Esp.).

Tribunal Constitucional [T.C.], 14 de agosto de 2002, sentencia recaída en el Expediente 0905-2001-AA/TI (Perú).

Tribunal Constitucional [T.C.], 27 de junio de 2008, Resolución 01578-2008-PHC/TC (Perú).

Tribunal Constitucional [T.C.], 11 de septiembre de 2012, sentencia recaída en el Expediente 00015-2010-PI/T (Perú).

Tribunal Constitucional [T.C.], 11 de octubre de 2018, sentencia recaída en los Expedientes 012-2018-PI/TC y 013-2018-PI/TC (Perú).

Observatorio Peruano de Cibercriminalidad

cibercrimenperu
cibercrimenperu.com
hola@cibercrimenperu.com

Construyendo juntos un entorno digital seguro.

- LITIGIO PENAL
- CONSULTORÍAS
- CAPACITACIÓN

/eliaspuelles
@eliaspuelles
@estudio.eliaspuelles
eliaspuelles.com

ESTUDIO ELÍAS PUELLES
ESPECIALISTAS EN DERECHO PENAL & PROCESAL

Telf: (01) 400-5181
contacto@eliaspuelles.com
Av. Javier Prado Este No. 596, oficina 602 - San Isidro, Lima

10.18800/themis.202101.006

EL EXTRACTIVISMO DE GRANDES DATOS (PERSONALES) Y LAS TENSIONES JURÍDICO-POLÍTICAS Y TECNOLÓGICAS VINCULADAS AL VOTO SECRETO

(PERSONAL) BIG DATA EXTRACTIVISM AND THE POLITICAL-LEGAL AND TECHNOLOGICAL TENSIONS RELATED TO THE SECRET VOTE

Ariel Hernán Vercelli*
Consejo Nacional de Investigaciones Científicas y Técnicas

The power, scope and technological capacity of certain States and their corporations bring new and complex challenges for democracies in the 21st century. The extraction of personal big data, the creation of citizens psychographic profiles and the sending of microsegmented political propaganda can affect the secret ballot and weaken democracy.

This article reviews the case of Facebook Inc. – Cambridge Analytica in order to analyze how the extraction of personal big data, the violation of privacy and the use of psychography can favor the manipulation of people, groups, communities and populations. The article is part of a larger investigation that seeks to rethink internet regulations and strengthen democracies in the digital age.

Keywords: Extractivism; personal data; secret ballot; Facebook Inc.; Cambridge Analytica; psycography.

El poder, alcance y capacidad tecnológica de ciertos Estados y sus corporaciones plantea nuevos y complejos desafíos para las democracias del siglo XXI. El extractivismo de grandes datos personales, la creación de perfiles psicográficos de los ciudadanos y el envío de propaganda política microsegmentada pueden afectar el voto secreto y debilitar la democracia.

En este artículo se retoma el caso Facebook Inc. – Cambridge Analytica con el objeto de analizar como el extractivismo de grandes datos personales, la violación de la privacidad y el uso de psicografía pueden favorecer la manipulación de personas, grupos, comunidades y poblaciones. El artículo forma parte de una investigación mayor que busca repensar las regulaciones de internet y fortalecer las democracias en la era digital.

Palabras clave: Extractivismo; datos personales; voto secreto; Facebook Inc.; Cambridge Analytica; psicografía.

* Doctor en Ciencias Sociales y Humanas. Consejo Nacional de Investigaciones Científicas y Técnicas de Argentina (CONICET) (Buenos Aires, Argentina). Contacto: arielvercelli@arielvercelli.org

El artículo se desarrolló gracias al apoyo del Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), la Universidad Nacional de Mar del Plata (UNMdP) y Bienes Comunes A. C. La investigación se desarrolla dentro del Instituto de Humanidades y Ciencias Sociales (INHUS/CONICET - UNMdP) y el Grupo de Investigación 'Ciencia, Tecnología, Universidad y Sociedad' (CITEUS), OCA 347/05, Facultad de Humanidades, UNMdP.

Nota del editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 10 de enero de 2021, y aceptado por el mismo el 30 de mayo de 2021.

I. INTRODUCCIÓN: LOS PROBLEMAS DEL EXTRACTIVISMO DE GRANDES DATOS (PERSONALES)

El uso masivo de las tecnologías digitales, las redes electrónicas distribuidas y las redes móviles ha generado (y está generando) profundos cambios en las sociedades contemporáneas. Muchos de estos cambios representan beneficios claros, ostensibles y masivos. Otros, sin embargo –más allá de las atractivas tecno-utopías–, profundizan injusticias socioeconómicas, generan asimetrías jurídico-políticas y contribuyen al deterioro de institutos clave para la vida democrática. Las crecientes y, muchas veces, compulsivas capacidades de extracción (recolección, procesamiento, archivo y explotación) de grandes datos alcanzadas por algunos Estados y sus corporaciones tecnológicas están planteando nuevos y complejos desafíos para los derechos humanos y las democracias representativas en el siglo XXI.

En la era digital, al igual que las piezas de un rompecabezas que aún no logran mostrar una figura completa, es posible advertir que el derecho humano a la privacidad (de personas, comunidades o poblaciones) se convirtió en un elemento central de la vida democrática. Al igual que otros sistemas complejos, los sistemas jurídico-políticos se caracterizan por conformar redes de relaciones: no hay forma de afectar (positiva o negativamente) alguno sin que otros derechos también resulten reconfigurados. Hace décadas se advierte que el exponencial aumento en las capacidades de extracción u explotación de grandes datos (personales, comunitarios y poblacionales) iba a afectar directamente el derecho a la privacidad y la protección de datos personales. Ahora bien, ¿la violación masiva y sistemática de estos derechos, su reconfiguración, o bien, su desaparición, podrían también acarrear consecuencias imprevistas?

Al respecto, es posible observar que los profundos cambios sobre el derecho humano a la privacidad comienzan a afectar también, de forma negativa e imprevista, la interpretación y el ejercicio de otros derechos y garantías constitucionales. ¿Es posible identificar casos recientes que evidencien estas tensiones jurídicos-políticas y tecnologías? Una de las hipótesis que atraviesa el artículo (y la investigación mayor en la que este se inserta) es que ciertos modelos tecnológicos corporativos están afectando negativamente las democracias representativas. Puntualmente, la violación masiva y sistemática del derecho humano a la privacidad –producto de la extracción y gestión tecnológica que llevan adelante algunos Estados y sus corporaciones tecnológicas– afecta la garantía constitucional del voto secreto y, con ello, se debilitan las democracias.

Es por ello por lo que, a los problemas ya suscitados por las modernas máquinas de votar y el voto electrónico[1], ahora es posible agregar nuevos problemas vinculados al extractivismo de grandes datos personales, la violación masiva y sistemática de la privacidad y ciertos diseños tecnológicos que degradan las libertades políticas y el sufragio universal. En el artículo se retoma el caso Facebook Inc. – Cambridge Analytica/Strategic Communications Laboratories (vinculado a las elecciones presidenciales de los Estados Unidos y el referéndum del Reino Unido en 2016) con el objetivo de analizar como el extractivismo de grandes datos personales y el uso de psicografía[2] pueden favorecer la manipulación de personas, comunidades y poblaciones y afectar negativamente las libertades políticas y las democracias en el siglo XXI.

II. LA RELEVANCIA DE LA PRIVACIDAD Y DE LA PROTECCIÓN DE LOS DATOS PERSONALES

El derecho humano a la privacidad es reconocido y garantizado ampliamente en las Constituciones Nacionales y en numerosos instrumentos internacionales (por ejemplo, el artículo 12 de la Declaración Universal de los Derechos Humanos de 1948)[3]. La privacidad es reconocida a cada ser humano individualmente, a grupos y comunidades específicas y, por cierto, también a las poblaciones. Se trata de un derecho que puede (y debe) interpretarse de forma amplia y respetando la di-

[1] Los numerosos intentos 'modernizadores' de los votos electrónicos (y de sus recuentos provisorios y definitivos) parecen no estar orientados a colaborar y fortalecer las democracias: el voto electrónico, telefónico, *online*, por computadora, por celular, entre otros, representan casos de retrocesos y vulnerabilidad para los sistemas y formas de votar. A través de estos sistemas, el voto podría dejar de ser secreto y/o se los podría identificar con facilidad (Hao & Ryan, 2017).

[2] La psicografía combina datos demográficos y psicológicos de las poblaciones (Nix, 2016). Se desarrolló como una herramienta del marketing (Samuel, 2016): releva si a los consumidores les gusta (o no) un producto o acuerdan (o desacuerdan) con alguna situación. Así se construyen perfiles de los ciudadanos (estilos de vida, rutinas y preferencias de consumo). Ver apartados IV y V en este artículo.

[3] El artículo 12 de la Declaración Universal de Derechos Humanos expresa que:

> Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (1948).

versidad de cada cultura (Francis & Francis, 2017). Tiene la particularidad de articularse con una red densa de otros derechos fundamentales: entre ellos, derechos políticos, libertades intelectuales (conciencia, creencias, pensamiento), libertad de expresión, protección del cuerpo, intimidad, confidencialidad, bienes materiales, autonomía, autodeterminación, domicilio y correspondencia.

A pesar de ser un derecho multiforme y de reciente reconocimiento mundial, el derecho a la privacidad reconoce a las personas la posibilidad de gozar de espacios de reserva, que, según diversidad de formas y alcances, pueda garantizar la intimidad, anonimidad o no intromisión por parte de los Estados, corporaciones u otras personas (sean estas físicas o jurídicas). Esta esfera de reserva, por fuera de las autoridades estatales y/o corporativas, ha recibido numerosos nombres y definiciones a lo largo de la historia. Entre otras, y con diferencias conceptuales y de alcances, se pueden mencionar conceptos tales como privacidad, vida privada, intimidad, confidencialidad, secreto, secretismo (Riofrío, 2015), olvido, reserva, no registro, anonimato y protección de datos sensibles.

A su vez, los cambios tecnológicos han ido afectando la codificación, configuración e interpretación del derecho a la privacidad a través de los años. Entre otras adecuaciones pueden citarse las tensiones generadas por las fotografías, las videocámaras, la telefonía fija o, más recientemente, el uso masivo de dispositivos móviles. El aumento exponencial de las capacidades tecnológicas de registro y archivo han resultado en la proliferación de todo tipo de información sobre las personas, grupos o poblaciones. En particular, formando parte del derecho a la privacidad, pero también de otros derechos fundamentales (intimidad, honor, identidad, integridad, libertades políticas), la era digital se caracteriza por haber regulado, a partir de la década del setenta y con mayor intensidad en los noventa, los principales aspectos del tratamiento de la información personal y de la protección de los datos personales.

Se han creado, con algo más de precisión, nuevos derechos orientados a resguardar la información personal (sensible), contenida en cualquier soporte (archivos, registros, bancos de datos u otros medios), frente a la gestión (más o menos automática) por parte de terceras personas (Estados, corporaciones comerciales, personas jurídicas sin fines de lucro)[4]. Aunque se trata de un derecho 'nuevo', de reciente construcción, todavía no existe a nivel mundial un estándar o posiciones uniformes sobre protección de datos personales. No obstante, más allá de las especificidades nacionales o regionales, por ejemplo, las de la Unión Europea (Hijmans, 2016; Reglamento 2016/679, 2016)[5], es posible identificar en las regulaciones algunos de los que podrían definirse como sus elementos comunes. A continuación, se describen los tres más relevantes para el presente análisis:

a) **Dato personal** es toda información sobre una persona (identificada o identificable) relacionada con, entre otros aspectos, nombres, documentos, origen étnico/racial, biometría, consumos, emociones, vida familiar/afectiva, domicilios, teléfonos, patrimonio, ideología, posiciones políticas, creencias (religiosas, morales), educación, salud, sexualidad;

b) Salvo excepciones legales, para la colecta de cualquier información o dato personal siempre se debe contar con el **consentimiento expreso** de la persona directamente afectada/involucrada (es decir, con su autorización expresa) obtenida a través de un medio que sea, entre otros requisitos exigibles, accesible, gratuito, comprensible, claro en sus términos y condiciones legales;

c) Estas **autorizaciones nunca podrán interpretarse de forma amplia, extensa o genérica**: es decir, los datos personales solo podrán usarse para los fines expresa y previamente autorizados. Las regulaciones nacionales e internacionales prohíben otros usos (sean por parte de quienes los colectaron o por parte de terceras personas).

[4] Se reconocen nuevos derechos a la ciudadanía para gestionar sus datos, saber dónde se almacenan, quiénes pueden acceder a ellos, con qué fines pueden usarlos o por cuánto tiempo se conservarán. En algunos países (como Argentina y Uruguay) los ciudadanos disponen de una acción específica (judicial) de *habeas data* orientada a poder conocer (rectificar, eliminar) los datos que constan en una base de datos del Estado o de personas privadas (con o sin fines de lucro).

[5] La Unión Europea (en adelante, UE) busca regular qué hacen algunas corporaciones extranjeras (Facebook Inc., Google Inc. Uber Inc., entre otras) con los datos de los ciudadanos europeos. El Reglamento General de Protección de Datos de la UE (Reglamento 2016/679, en vigor desde el 25 mayo de 2016 y aplicable desde el 25 de mayo de 2018), plantea reforzar el derecho a la privacidad, restringir la gestión automática de datos personales sin consentimientos expresos y ofrecer, entre otros puntos, mayor capacidad a las agencias europeas de inspeccionar, limitar y sancionar a las corporaciones que no cumplan con sus estándares: por ejemplo, las nuevas 28 autoridades de protección de datos podrán imponer multas de hasta 20 millones de EUROS o del 4 % del volumen de negocios. A partir de la aplicación del nuevo reglamento en la Unión Europea es posible advertir una creciente complejidad en el tratamiento de datos personales (Troncoso Reigada, 2021).

III. LA VIOLACIÓN MASIVA Y SISTEMÁTICA DEL DERECHO HUMANO A LA PRIVACIDAD

Más allá de lo expresado en las diferentes leyes de protección de datos personales y, sobre todo, de sus interpretaciones legales y tecnológicas, es importante resaltar que la extracción de todo tipo de datos personales se ha transformado en una de las formas más rentables y lucrativas de explotar la experiencia e interacción humana en la era digital. De allí que la privacidad y la protección de datos personales se hayan convertido en una zona álgida, de conflictos y tensiones, sobre qué se puede o no se puede hacer con la información de los ciudadanos. La problemática fue denunciada a través de numerosos informes y documentos internacionales (United Nations Educational, Scientific and Cultural Organization [UNESCO], 2014). Alemania y Brasil impulsaron la Resolución 68/167 (aprobada el 18 de diciembre de 2013 por Asamblea General de Naciones Unidas) sobre el derecho a la privacidad en la era digital.

A nivel internacional existen fuertes presiones de Estados y sus corporaciones tecnológicas para reconfigurar la regulación hacia sus propios intereses. Las corporaciones que se dedican a extraer y explotar datos personales de los usuarios pasaron a producir sus propias interpretaciones jurídico-tecnológicas sobre qué es y cómo se ejercen estos derechos. Esto ha tenido resultados negativos: muchas de las condiciones de uso de servicios, plataformas y redes sociales se han transformado en imposiciones abusivas e ilegales (o paralegales) sobre el tratamiento estos datos. Muchas de estas corporaciones tecnológicas, incluso, rechazan el sentido protectivo de estas regulaciones. De allí que la protección de datos personales, lejos de convertirse en un ejercicio ciudadano directo y efectivo, se haya convertido en algo dudoso, confuso, atrasado, costoso, técnico, solo para expertos.

Estas situaciones han favorecido que, a escala global, se produzca un tipo de violación masiva y sistemática de la privacidad (en general) y de los datos personales de los usuarios (en particular). Estas tensiones entre las regulaciones de los datos personales de los usuarios y las tecnologías digitales que se usan para extraerlos y explotarlos es posible identificarlas a partir de, al menos, dos fuertes tendencias a nivel mundial. Por un lado, la vigilancia masiva y el ciberespionaje: de público conocimiento a través de las filtraciones de Chelsea Manning[6] y Edward Snowden[7] (Assange, 2013; Poitras, 2014; Greenwald, 2014; Lefébure, 2014). Por el otro, los modelos de negocios y la comercialización de la publicidad/propaganda que llevan adelante las corporaciones tecnológicas más poderosas a nivel mundial (Reischl, 2008; Vaidhyanathan, 2011; Assange, 2014; Bartlett, 2018).

Los entornos digitales están siendo diseñados para extraer valor de todo tipo de experiencias humanas. Dentro de estos diseños tecnológicos y arquitecturas los seres humanos pasan a ser considerados recursos naturales, una fuente más para extraer valor. Las imágenes de la vigilancia y del panóptico devienen penetrantes. Similar a como Michel Foucault (1991) describía el panóptico de Jeremías Bentham, las redes electrónicas (internet, la red de redes) se convirtió en un (ciber)espacio donde se distribuyen asimétricamente las capacidades de ver y ser visto. Algunos pueden verlo todo, un gran panóptico electrónico distribuido, otros –disociados, atomizados, sujetos a máquinas digitales de extracción, producción y control–, no pueden siquiera verse a sí mismos como personas, comunidades o poblaciones.

Este panóptico, ahora electrónico, captura e intenta extraer valor de la totalidad de la vida humana. Se caracteriza por recombinarse con arquitecturas, disciplinas, tecnologías, regulaciones, algoritmos, ciencia de datos, inteligencias artificiales, análisis predictivos. Estos dispositivos, en suma, siguen funcionando como una especie de laboratorio de poder. Permiten observar un tipo de extractivismo que utiliza la experiencia humana como material crudo, lo traduce en 'datos conductuales' (en conductas) y lo ofrece como dispositivos de predicción (sobre lo que puede ocurrir ahora, pronto o después). Aquello que Zuboff (2019) define como un mercado de conductas futuras. Se trata de un tipo

[6] Chelsea Elizabeth Manning (llamada al nacer Bradley Edward Manning) es una soldado de inteligencia del ejército de los Estados Unidos de Norteamérica (fuera de servicio). Fue quién filtró al sitio WikiLeaks.com cables diplomáticos (sobre embajadas) y documentos de la inteligencia de EE. UU sobre las guerras de Afganistán e Irak. Entre otros, el video filtrado más reconocido fue Collateral Murder (Asesinato Colateral) (Assange, 2013). Desde 2014 cumple condena a 35 años de prisión en los EE. UU.

[7] Edward Snowden es un experto en tecnologías de información norteamericano, actualmente asilado en Rusia, que trabajó para la CIA (Agencia Central de Inteligencia), la DIA (Agencia de Inteligencia en Defensa), la empresa Dell y la firma Booz Allen Hamilton (trabajando para la National Security Agency, en Hawaii), que filtró en 2013 miles de documentos clasificados sobre los sistemas de vigilancia masiva de la Agencia Nacional de Seguridad de EE.UU (NSA) a los medios de comunicación y, específicamente, al periódico inglés The Guardian (a través de los periodistas Glenn Greenwald y Laura Poitras). Al respecto se puede ver el documental Citizenfour (Poitras, 2014).

de extractivismo compulsivo, invasivo, violatorio de derechos, oculto y antidemocrático.

IV. FACEBOOK INC. – CAMBRIDGE ANALYTICA: A LA CAZA DE LOS DATOS (PERSONALES)

A mediados de marzo del año 2018, Channel 4[8], The New York Times[9] y The Observer (The Guardian)[10] comenzaron a publicar material de investigación sobre como algunas corporaciones favorecían el uso masivo de los datos personales de la ciudadanía con fines electorales. Las investigaciones periodísticas –que incluyeron cámaras ocultas, entrevistas a exempleados y documentos oficiales– dejaron entrever una trama oscura entre la red social norteamericana Facebook Inc.[11] y, entre otras, la empresa británica Cambridge Analytica (en adelante, CA), parte de Strategic Communications Laboratories (en adelante, SCL)[12]. El tema no era nuevo[13], pero sí escandaloso. Las investigaciones revelaron como CA/SCL ofrecía 'innovadoras' campañas electorales a través del uso intensivo de tecnologías digitales, datos personales y perfiles psicológicos de millones de usuarios[14].

Los informes periodísticos denunciaban que CA/SCL había utilizado estas novedosas herramientas en más de 200 campañas en todo el mundo: en particular, y más cercanas en el tiempo, en las elecciones norteamericanas de 2016 (con una participación a favor de Donald Trump) y, en el mismo año, en el referéndum del Reino Unido (donde apoyaron activamente la posición del Brexit)[15]. Al tomar estado público rápidamente surgieron campañas en su contra[16] y varias investigaciones en todo el mundo[17]. A los pocos días se fueron conociendo algunos detalles operativos. Los datos y perfiles de los usuarios de Facebook Inc. habían sido recolectados por CA/SCL a través de la empresa Global Science Research (GSR)[18]. Esta última fue fundada por Aleksandr Kogan, un psicólogo social ruso que trabajaba en la Universidad de Cambridge (Reino Unido).

[8] Canal público de televisión comercial del Reino Unido, controlado por Channel Four Corporation (C4C), una corporación pública dedicada a televisión, cine e internet, y relacionada con la Oficina de Comunicaciones (Ofcom) del Reino Unido.

[9] Diario norteamericano fundado en 1851.

[10] Es el diario dominical más viejo del mundo. Fue publicado por primera vez en 1791.

[11] Facebook Inc. es una corporación norteamericana dueña de la red social más grande del mundo (Facebook) y otras empresas (Instagram, Messenger, Oculus, Whatsapp). Sus oficinas centrales están en Menlo Park, California. La red social vio la luz el 4 de febrero de 2004 y comenzó a cotizar en bolsa en 2012. La plataforma Facebook se caracteriza por enlazar gente 'amiga' (o conocidos) mostrando sus actividades sociales (es decir, textos, fotos, videos sobre qué hacen). Sus principales ingresos se deben al rubro publicidad. Se estima que a principios de 2018 Facebook tenía cerca de 2 200 millones de usuarios en todo el mundo. En promedio, los usuarios activos le dedican a Facebook unos cincuenta minutos diarios (Stewart, 2016). Facebook Inc. es considerado, según criterios de uso y adopción, el negocio más exitoso en la historia de la humanidad (Galloway, 2017).

[12] Cambridge Analytica (en adelante, CA) era una empresa británica (con oficinas en Londres, New York y Washington D.C.) dedicada a las consultorías de mercado y campañas electorales. Pertenecía a la familia Mercer (Robert y Rebekah) y fue presidida por Steve Bannon (director de campaña de Donald Trump en 2016). CA fue fundada en 2012 como una filial de Strategic Communications Laboratories (en adelante, SCL). SCL provee datos, análisis y estrategia para gobiernos y organizaciones militares: se dedica a colectar y analizar cuál es la opinión sobre los servicios militares y diplomáticos de Estados Unidos y el Reino Unido en todo el mundo. Trabaja principalmente con los ministerios de defensa de los países de la Organización del Tratado del Atlántico Norte (OTAN) (Briant, 2018). SCL se describe a sí misma como la primera empresa privada proveedora de operaciones psicológicas. Entre sus técnicas, se destacaban la propaganda política y la posibilidad, en tiempos de crisis, de sobreescribir las transmisiones de los medios de comunicación, además, la colecta de grandes datos y de su duplicación y segmentación.

[13] En julio de 2015 la Revista Politico publicó una nota sobre la estrategia de campaña de Ted Cruz: resaltaban la promiscua relación de la familia Mercer (financista de Cruz) y empresas de su propiedad (CA/SCL) que lo asesoraban (Vogel & Parti, 2015). En diciembre de 2015, The Guardian ya denunciaba el uso de datos personales y la creación de perfiles psicológicos para la campaña en los EE. UU. (Davies, 2015). En 2017, The Intercepter denunciaba algo similar (Schwartz, 2017).

[14] Las cámaras ocultas mostraban a directivos de CA/SCL ofreciendo campañas de desprestigio: escándalos sexuales, noticias falsas (*fake news*), sobornos, trabajos de inteligencia.

[15] Se denomina así a la campaña del año 2016 en el Reino Unido para influir en el referéndum del 23 de junio por la salida de Gran Bretaña de la Unión Europea. Al respecto ver Glenncross (2016).

[16] El 22 de marzo uno de los fundadores de Whatsapp, Brian Acton, se manifestó contra la Facebook Inc. y llamó a un boicot en su contra: *#DeleteFacebook* y *#BoycottFacebook*.

[17] Se iniciaron múltiples investigaciones (políticas, administrativas y judiciales) sobre violaciones a la protección de datos personales y a las leyes electorales. En EE. UU. denunciaron a CA/SCL ante la Comisión Federal Electoral y el Departamento de Justicia. En el Reino Unido las investigaciones fueron tomadas principalmente por la Cámara de los Comunes (Digital, Culture, Media and Sport Committee, 2018; 2019). En Brasil estuvieron a cargo del Ministerio Público del Distrito Federal y Territórios (Brito, 2018; Ministério Público, 2018). En Argentina se encargaron la Cámara Nacional Electoral y la Dirección Nacional de Protección de Datos Personales (Carelli, 2018). También hay investigaciones iniciadas en Israel, Perú e India.

[18] La página web de Global Science Research fue dada de baja. La información solo es disponible a través de Internet Archive: https://web.archive.org/web/20160317171729/http://www.globalscienceresearch.com

El tema de investigación de Aleksander Kogan era 'felicidad y amabilidad' (*happiness and kindness*) en las redes sociales y usaba desarrollos del Centro de Psicometría de la Universidad de Cambridge. Entre otras, investigaciones sobre psicografía[19] y predicción de la personalidad provenientes de los trabajos de Michal Kosinski y David Stillwell (Youyou *et al.*, 2015; Sumpter, 2018)[20]. Estos investigadores (Kosinski *et al*., 2013), habían advertido que la personalidad de un usuario podía predecirse fácilmente a través de los datos públicos que se extraían de sus rutinas de navegación (páginas web, redes sociales, etc). En CA/SCL estaban interesados en poder usar los datos personales y los perfiles psicográficos de los usuarios de Facebook Inc. para diseñar campañas electorales microsegmentadas.

Inicialmente, Kogan desarrolló una aplicación (un cuestionario de personalidad llamado *this is my digital life* [esta es mi vida digital]), validada en la *application programming interface* (en adelante, API) de Facebook Inc.[21], a través de la cual los usuarios consentían hacer un estudio psicográfico. Al hacerlo, permitieron voluntariamente que la aplicación recolecte todo tipo de información sobre su perfil (ubicación, género, cumpleaños, preferencias, me gusta). Incluso, al aceptar el cuestionario, por la configuración de Facebook Inc., también permitieron que la aplicación recolecte los perfiles de sus amigos (contactos)[22]. Cerca del 80% de los voluntarios ofrecieron sus datos (y los de sus amigos) por un dólar (tenían en promedio 353 amigos). Entre 2014 y 2015, aceptaron participar unos 857 usuarios de Facebook Inc. y, gracias a los 'permisos de los amigos', se recolectaron más de 287 000 perfiles (Sumpter, 2018).

En un segundo momento CA/SCL le ofreció a Aleksandr Kogan ampliar la muestra. Esta vez el contrato fue hecho por fuera de la Universidad y se usó Qualtrics (un servicio en línea de encuestas para consumidores) (Sumpter, 2018). Según afirma Kogan, en ese momento se solicitaron todas las autorizaciones correspondientes a los encuestados y también se cumplió con la normativa de Facebook Inc. (Sumpter, 2018; Stahl, 2018). En esta oportunidad el cuestionario fue respondido por cerca de 200 000 norteamericanos (Sumpter, 2018). Según datos estimados de Facebook Inc., los perfiles recolectados a través de esta segunda encuesta podrían alcanzar entre 70 y 87 millones de usuarios (inicialmente se supuso que eran 50, luego 70 y, finalmente, 87 millones). Se estimó también que, de los 87 millones, 71 millones vivían en EE. UU. (una cantidad significativa que permitió esquematizar los rasgos psicológicos de la población norteamericana).

Es importante resaltar que los datos anteriores son solo estimaciones provisorias: no existen datos oficiales ni de Facebook Inc. ni de CA/SCL, ni de ningún Estado. ¿Es posible que el número de damnificados sea superior? Es posible. Brittany Kaiser, una exempleada de Cambridge Analytica, declaró el 17 de abril 2018 ante el Parlamento Británico que –más allá de las desarrolladas por Kogan– existían dentro de la red social numerosas encuestas con similares características: por ejemplo, "sex compass [brújula sexual]" (Collins, 2018). Incluso, el mismo Aleksandr Kogan, entrevistado por Lesley Stahl (2018), expresó que dentro de Facebook existían decenas de miles de estas aplicaciones que recolectaban datos personales. Facebook Inc. reconoció (tal vez como parte de su estrategia legal) que no podían certificar (calcular) la cantidad real de usuarios afectados.

Incluso, su representante legal, Mike Schroepfer, llegó a afirmar a la prensa que en Facebook Inc. nunca revisaban los términos y condiciones incluidos en las aplicaciones que los desarrolladores cargaban a la red (Romm, 2018). No obstante, el informe final de la investigación llevada adelante

---

19 Para la psicometría todas las personalidades humanas pueden clasificarse según rasgos. El uso de PCA (*Principal Component Analysis*) permitió sintetizar cinco grandes grupos (*big five*), el modelo OCEAN (por sus siglas): *Openness* (apertura), *Conscientiousness* (responsabilidad), *Extroversion* (extroversión), *Agreeableness* (amabilidad) y *Neuroticism* (inestabilidad).

20 Michal Kosinski y David Stillwell desarrollaron (dentro de la Universidad de Cambridge) el proyecto myPersonality recolectando, con permisos explícitos, más de tres millones de perfiles de usuarios de Facebook Inc. Muchos de estos usuarios tomaron un test de psicometría (medición de inteligencia, personalidad, alegría, orientación sexual, uso de drogas, etc.). El estudio les permitió analizar como aquello que es escrito, compartido y evaluado a través de un simple 'me gusta' permite describir la personalidad y, en parte, predecir conductas (Sumpter, 2018).

21 En 2007, la red social comenzó a ofrecer un espacio para el desarrollo de aplicaciones. Esta plataforma articuló HTML, SQL (*styled query language*), JavaScript y una serie de librerías de clientes de programación. A este espacio de desarrollo se lo llamó genéricamente API (*application programming interface*). Esta plataforma le permitió a Facebook Inc. que otros desarrolladores crearan aplicaciones (externas) para mejorar la interacción entre los usuarios.

22 Es decir, los 'amigos' no aceptaban explícitamente los términos legales de la aplicación. Esta característica, llamada 'permisos de amigos' (*friend permissions*), no era un permiso especial concedido a Kogan (u otros), sino que era una de las principales 'funcionalidades' de la plataforma orientada a desarrolladores y empresas afiliadas-asociadas. Según Kogan, era una característica general de la plataforma y no un error: "It was a feature, not a bug" (Stahl, 2018). Estas características, debido a diferentes problemas legales de Facebook Inc., fueron restringidas a partir del año 2015.

por la Cámara de los Comunes del Reino Unido desmintió a Facebook Inc. y dejó en claro que la corporación sí sabía (internamente) cuantas aplicaciones corrían en la red social y bajo qué condiciones legales lo hacían (Digital, Culture, Media and Sport Committee, 2018; 2019). Facebook Inc. nunca hizo públicos estos datos. Es importante resaltar que, si bien los perfiles de los usuarios provenientes de Facebook Inc. fueron la fuente más importante para extraer datos personales, la red social norteamericana no fue la única fuente para la empresa CA/SCL[23].

CA/SCL articuló los datos personales provenientes de Facebook Inc. con otras fuentes de información de ciudadanos de los EE. UU.: entre otras, encuestas telefónicas, cuestionarios en línea, consumo de tarjetas de crédito, datos de otras redes sociales, bases de datos de las Iglesias evangélicas de los EE. UU. (Kriel & Gellein, 2020) e, incluso, datos públicos provenientes de padrones del Partido Republicano. La triangulación de las diferentes fuentes de datos le permitió a CA/SCL alcanzar perfiles más sólidos e integrados de la población norteamericana. Se estima que estas bases de datos contenían más de sesenta campos de información sobre aproximadamente 191 millones de ciudadanos norteamericanos (Kriel & Gellein, 2020). Estos datos son los que fueron retroalimentando los algoritmos predictivos que CA/SCL utilizó en la campaña de EE. UU. en 2016 y, con ajustes poblacionales, en otras campañas electorales alrededor del mundo.

V. EL USO DE PSICOGRAFÍA EN LAS PRESIDENCIALES DE EE. UU. Y EL BREXIT DEL REINO UNIDO

El uso intensivo de las tecnologías digitales para campañas electorales no es nuevo. El presidente Barack Obama también las usó en las elecciones de 2008 para promover y financiar su llegada a la Casa Blanca[24]. Algo similar ocurrió con las campañas electorales de 2016 en EE. UU. (elecciones presidenciales a favor de Donald Trump) y también en el Reino Unido (referéndum Brexit: Vote.Leave y Leave.EU). En ambas campañas se registró un uso intensivo de redes sociales (en especial Facebook Inc.[25]), de datos personales y perfiles de Facebook Inc. (entre otros) y de herramientas psicográficas. Así lo confirmó Theresa Hong, Directora de Contenidos de la Campaña de Trump (Rampling, 2017) y los exempleados de Cambridge Analytica, Christopher Wylie y Brittany Kaiser (Cadwalladr & Graham-Harrison, 2018; Metcalf, 2018; Digital, Culture, Media and Sport Committee, 2018; 2019; Kaiser, 2019).

Específicamente, CA/SCL en los EE. UU. comenzó a trabajar en 2015 para las campañas republicanas de pequeña escala (alcaldías y legisladores). En un segundo momento, para las presidenciales de 2016 en EE. UU. comenzaron asesorando a Ted Cruz (candidato republicano) y, luego de la interna, pasaron a la campaña del también candidato republicano Donald Trump. Para la elección general el centro de operaciones se ubicó en San Antonio, Texas, y la campaña fue bautizada como Proyecto Álamo (Rampling, 2017). La estrategia de CA/SCL para influir el voto popular fue compleja y ambiciosa. Entre otros elementos, presentes también en el Brexit, buscaron articular: (i) el uso de grandes datos (personales); (ii) con desarrollos de psicometría (y su poder predictivo); y (iii) diseñar y enviar mensajes políticos micro-segmentados. Específicamente, articularon:

a) El uso de grandes datos (personales), tal y como se analizó anteriormente, obtenidos y recolectados desde diferentes fuentes (aunque, principalmente, de Facebook Inc.), para construir diferentes bases de datos y algoritmos que permitan definir y redefinir audiencias específicas para (o solo en función de) los intereses políticos de las campañas electorales que tenían por delante;

b) Los últimos desarrollos de psicometría (y su potencial para poder predecir la conducta

[23] Para Christopher Wylie, uno de los miembros de Cambridge Analytica, según declaración ante la Comisión de Asuntos Digitales, Cultura, Medios de Comunicación y Deportes de la Cámara de los Comunes (Parlamento Británico), los datos personales recolectados de la red social fueron la base sobre la que se fundó la empresa y sobre la que se apoyaron los algoritmos utilizados (Cadwalladr & Graham-Harrison, 2018). Algo similar puede haber ocurrido con AggregateIQ (AIQ), empresa canadiense que aportó modelos psicográficos para las campañas en EE. UU. y en el Brexit del Reino Unido (Digital, Culture, Media and Sport Committee, 2018; 2019).

[24] En esa oportunidad fue Google Inc. La corporación que demostró grandes capacidades de gestión para las campañas y para acompañar en la misma gestión del gobierno demócrata en EE.UU. (incluso, volviendo porosos los límites entre lo público y lo privado) (Zuboff, 2019).

[25] Según el informe corporativo de Facebook Inc. del 2016, Year in Review (Neman, 2016), ambas elecciones tuvieron la máxima relevancia. Los diez temas más hablados a nivel global del año 2016 fueron: 1) US Presidential Election, 2) Brazilian Politics, 3) Pokemon Go, 4) Black Lives Matter, 5) Rodrigo Duterte & Philippine Presidential Election, 6) Olympics, 7) Brexit, 8) Superbowl, 9) David Bowie, 10) Muhammad Ali. Es decir, cuatro de los diez temas más 'compartidos' en Facebook Inc. involucraron campañas políticas y elecciones: EE. UU., Reino Unido, Brasil y Filipinas (Neman, 2016).

política de los ciudadanos)[26]: CA/SCL creó y configuró modelos psicográficos de comportamientos de la población según rasgos de personalidad similares (grupos de votantes o audiencias). Estos modelos se desarrollaron antes del Proyecto Álamo[27]. Podrían considerarse una creación intelectual alcanzada por derechos intelectuales (Metcalf, 2018);

c) Para diseñar y enviar todo tipo mensajes microsegmentados con la intención de afectar (influir, asegurar, modificar o evitar) el voto popular. Los modelos psicográficos permitieron definir (interactuar, controlar) las audiencias (grupos de votantes) y decidir estrategias (y medios) para enviarles mensajes microsegmentados adecuados a su perfil psicológico (ansiedades, temores, solidaridad, escepticismo, etc.).

Por tanto, a partir de la estrategia implementada por CA/SCL es posible observar un punto relevante para el presente análisis. Los datos personales de carácter político de la ciudadanía tuvieron la máxima relevancia al momento de definir y conducir las campañas. Los datos personales de carácter político fueron usados para definir, construir y enviar mensajes a las diferentes audiencias. Al respecto, la Directora de Contenidos de la Campaña de Donald Trump en 2016, Theresa Hong, señaló cuál de los atributos era el más relevante para definir el universo de personas a las que dirigir la campaña microsegmentada (Rampling, 2017). Puntualmente, entre otros datos políticos relevantes, la directora expresó que para la campaña se consideraba central conocer (de personas/grupos/poblaciones): "[…] when was the last time they voted?, who did they vote for?" (Rampling, 2017)[28].

Incluso, a partir de las investigaciones de la Cámara de los Comunes del Reino Unido (Comisión de Asuntos Digitales, Cultura, Medios de Comunicación y Deportes; en adelante, la Comisión), Chris Vickery (Director de Investigaciones sobre Cyber Risk, Upguard), entregó a la Comisión un disco externo con datos personales de 191 millones de ciudadanos norteamericanos (Kriel & Gellein, 2020). La información de cada persona estaba compuesta por aproximadamente unos 60 campos. La base de datos, según afirmó Vickery, fue expuesta públicamente (accesible vía registración) a través de la organización religiosa evangelista United in Purpose (una coalición de pastores). Se estima que originalmente podría haber sido una base datos de los afiliados al Partido Republicano (llamada *Data Trust voter vault*). Entre otros campos de datos relevantes se destacan: "[…] likely swing voter … this person is likely to vote based on this issue … kind of one-position voter based on abortion […]" (Kriel & Gellein, 2020, 20:15)[29].

El gerente general de Cambridge Analytica, Alexander Nix, en su declaración ante la Cámara de los Comunes del Reino Unido, reconoció que la consultora buscaba alcanzar una adecuación de la información similar a la antes descrita. En su testimonio, tomado antes de que se desate el escándalo internacional en marzo de 2018, describe y defiende la microsegmentación implementada por CA/SCL de la siguiente forma:

> We are trying to make sure that voters receive messages on the issues and policies that they care most about, and we are trying to make sure that they are not bombarded with irrelevant materials. That can only be good [...] for democracy [...] (Digital, Culture, Media and Sport Committee, 2018, p. 27)[30].

---

[26] Para medir la personalidad antes se usaban test o cuestionarios. En la era digital se usan las huellas digitales de navegación o uso de redes sociales. Son los pequeños datos acumulados en el tiempo los que hacen la diferencia predictiva. Este es un trabajo que las computadoras hacen mejor que los seres humanos. Los algoritmos pueden identificar detalles valiosos dentro de grandes cantidades de pequeños rastros digitales. Los perfiles de comportamiento son muy buenos para estimar datos demográficos como las tendencias políticas, el género, la ubicación y la raza (Kosinski *et al*., 2013). Los análisis, predicciones y juicios sobre la personalidad hechos por computadoras son más adecuados que los hechos por seres humanos (Youyou *et al*., 2015). Las computadoras ven lo que los psicólogos, médicos o policías no ven. Un perfil de comportamiento basado en 'me gusta' (aparentemente inofensivos) junto con otros datos crean un mapa lo suficientemente bueno para obtener mucha más información sobre una persona: a mayor cantidad de dimensiones mayor el poder para clasificación (Kosinski *et al*., 2016).

[27] Según Alexander Nix (Rampling, 2017), para la campaña de Trump no se crearon modelos psicográficos específicos. La psicografía que tenían los datos utilizados en campaña fue heredada de los modelos de datos que se venían usando en las anteriores campañas (dos o tres años atrás).

[28] Traducción libre: "[…] ¿cuándo fue la última vez que votaron?, ¿por quién votaron?".

[29] Traducción libre: "[…] votante con probable cambio […] esta persona es probable que vote a partir de este tema […] tipo de votante que posiciona en primer lugar el aborto […]" .

[30] Traducción libre:

> Estamos tratando de asegurar que los votantes reciban los mensajes sobre los tópicos y las políticas que más les interesan y estamos tratando de asegurar que ellos no sean bombardeados con materiales irrelevantes. Esto solo puede ser bueno ... para la democracia […].

Los testimonios mencionados permiten observar que los perfiles psicográficos y los datos personales de carácter político, sobre todo los vinculados al voto, resultaron de máxima relevancia para las campañas. En 2016, para la campaña presidencial de EE.UU., se llegaron a enviar más de cien avisos diarios a través de las redes sociales (entre otras, Facebook, Youtube, Twitter) (Rampling, 2017). Según Christopher Wylie, la psicometría se usó para despertar los 'demonios internos' (*inner demons*) de cada persona (Cadwalladr & Graham-Harrison, 2018). Para ciertas 'audiencias' estas campañas pueden haberse convertido en un indeseable y abusivo bombardeo de todo tipo de mensajes: incluyendo, desde noticias falsas (*fake news*), hasta noticias más 'emocionales' orientadas a despertar ansiedad, temor, empatía, desagrado, desesperanza, escepticismo, etc.[31]

A partir del escándalo desatado en 2018 por el caso de Facebook. Inc. – Cambridge Analytica, la legalidad y legitimidad de este tipo de campañas micro-segmentadas, que apuntan a audiencias según perfiles psicográficos, que solo llegan a 'las pantallas' de los votantes (sin ningún control público-comunitario) y que buscan un cambio de conducta en la población, comenzaron a ser fuertemente cuestionadas en todo el mundo. A pesar de la gravedad, aún no se avizoran soluciones. Estas no aparecieron en EE. UU., tampoco en el Reino Unido. Incluso, en muchos países regular estas situaciones podría resultar una tarea casi imposible y con serias dificultades jurídico-políticas, económicas y tecnológicas. Finalmente, más allá de las vanas promesas de autoregulación corporativa, las posibles soluciones tampoco emergieron desde las mismas corporaciones tecnológicas.

VI. ZUCKERBERG PIDE DISCULPAS PÚBLICAS, PERO FACEBOOK INC. SIGUE SU CAMINO

En medio del escándalo, Facebook Inc. intentó esquivar responsabilidades legales. En primera instancia, acusó a Aleksandr Kogan de fraude, de haber 'vendido' los datos a CA/SCL y, sin mediación, suspendió su cuenta. Por su parte, Kogan se defendió alegando que solo recopilaba la información con fines académicos y que actuó con honestidad (aunque con cierta ingenuidad). En segunda instancia, Facebook Inc. también suspendió la cuenta de CA/SCL bajo la acusación de haber violado su política de privacidad (prohibiéndole operar publicidad). Por su parte, CA/SCL también negó haber actuado de forma ilegal. No obstante, apartó a Alexander Nix. El 2 de mayo de 2018 la empresa anunció su cierre definitivo alegando pérdida de clientes y altos costos legales (Ballhaus & Gross, 2018). La empresa CA fue rápidamente transformada en otra, llamada Emerdata.

Finalmente, Mark Zuckerberg tuvo que pedir disculpas públicas por la forma en que Facebook Inc. había manejado los datos personales de sus usuarios. Sin embargo, fueron disculpas genéricas, ambiguas, sin ofrecer información válida sobre los hechos denunciados (Zukerberg, 2018). Se comprometió a realizar una investigación interna sobre CA/SCL y sobre otras aplicaciones que podrían haber minado datos personales de la red social (Zukerberg, 2018). Sin mucha relevancia, también se pusieron a disposición de los usuarios herramientas para saber si sus perfiles habían sido recolectados por CA/SCL (Facebook Newsroom, 2018). A principios de abril de 2018 Facebook Inc. presentó una nueva 'actualización' de sus términos de servicio y de su política de datos. Sin embargo, en nada modificaron sus políticas de datos personales ni su posición frente a la privacidad.

A mediados de abril de 2018 sí pudo observarse un movimiento brusco. La negativa de adecuar su gestión de datos personales a las nuevas regulaciones de la Unión Europea llevó a que Facebook Inc. cambie repentinamente su domicilio legal (la jurisdicción) de Irlanda hacia los EE.UU. Esto afectó los derechos de millones y millones de usuarios (cerca de dos tercios de sus clientes). El cambio de jurisdicción estuvo motivado por la entrada en vigencia del nuevo Reglamento General de Protección de Datos de la Unión Europea (Reglamento 2016/679, 2016). Sin mayores explicaciones Facebook Inc. regresó a su casa matriz en los EE. UU. (Agencia Telam, 2018). Los movimientos de Facebook Inc. dejaron en claro al menos dos puntos relevantes para el análisis. Por un lado, que a Facebook Inc. poco le importa la privacidad de sus usuarios y que algunas corporaciones parecen funcionar al margen de la ley. Por el otro, tal vez lo más importante, que a nivel internacional el derecho a la privacidad vale menos de lo que podía suponerse.

Los movimientos de Facebook Inc. mostraron que, a pesar de los escándalos vinculados a CA/SCL y de sus responsabilidades jurídicas, la red social

[31] Al respecto se puede revisar los informes (provisorio y final) de la Cámara de los Comunes (Digital, Culture, Media and Sport Committee, 2018; 2019) sobre desinformación (*disinformation*) y noticias falsas (*fake news*). En Argentina, según Acordada Extraordinaria 66-18, la Cámara Nacional Electoral (CNE) creó un "registro de cuentas de redes sociales y sitios web de los candidatos, agrupaciones políticas y máximas autoridades partidarias" con la intención de concientizar a la población sobre el peligro de las noticias falsas (*fake news*) (Acordada Extraordinaria 66-18, 2018).

norteamericana no tiene pensado adecuar su modelo de gestión de datos personales ni sus configuraciones de privacidad. Mucho menos revisar su modelo de negocio de publicidad y propaganda por microsegmentación de audiencias. La materia prima de Facebook Inc. son los perfiles de usuarios y su capacidad (amplia y detallada) para poder gestionarlos según sus intereses comerciales. Día a día, segundo a segundo, Facebook Inc. interroga a millones usuarios '¿qué estás pensando?'. Sus algoritmos registran cada movimiento. Facebook Inc. devino en una plataforma comercial que, lejos de ser una inocente red social de intercambio de fotos, videos o textos, adquirió una relevancia política insospechada.

En los próximos años, cada día más, Facebook Inc. (pero también Alphabet, Amazon y otras) seguirán colectando datos personales de sus usuarios. Estas corporaciones son, claramente, máquinas de disparar con publicidades y propagandas. Una vez que el relacionamiento social pasa a estar mediado solo por intereses comerciales, resulta factible que estas corporaciones se transformen en máquinas de manipulación social y afecten la autoconciencia y la autodeterminación de las personas y poblaciones[32]. El primer objetivo de Facebook Inc. como corporación es funcionar como máquina predictiva: su modelo de desarrollo, instrumentos e inteligencias artificiales (FBLearnerFlow) van creando un mercado de "futuros conductuales" (Zuboff, 2019, p. 264) sobre la base de predecir (poder anticipar) las conductas de los individuos, grupos sociales y poblaciones.

VII. LAS TENSIONES POR EL VOTO 'OBLIGATORIAMENTE SECRETO' EN LA ERA DIGITAL

El recorrido propuesto en el artículo permite observar que la era digital no ha traído solo cambios tecnológicos favorables. La extracción y explotación de datos personales por parte de Estados y sus corporaciones tecnológicas tiene consecuencias negativas. A partir de la constante retroalimentación de los flujos de datos personales y, sobre todo, del aprendizaje circular y recursivo en la construcción de perfiles a través de tiempo, es que las conductas de los ciudadanos, comunidades y poblaciones se pueden conocer (directamente) o predecir (deducir, inferir, presumir). Entonces, ¿qué ocurre con el secreto del voto cuando algunos Estados y sus corporaciones tecnológicas pueden saber o predecir por quién/es ha votado, vota o podría votar un/a ciudadano/comunidad/población? ¿Por qué el sufragio universal fue también construyéndose como una práctica secreta?

El sufragio universal se ha transformado, desde mediados del siglo XIX, y a partir de diferentes luchas jurídico-políticas, en una de las piezas clave en la organización de poder del Estado. En la actualidad es uno de los pilares que sustenta la soberanía popular, los sistemas de representación política y los sistemas democráticos. Puede definirse como un derecho político de todos y cada uno de los ciudadanos/as para participar (elegir y ser elegido) en la organización y en las actividades del poder en el Estado. Es por ello que, a través del voto popular, logran expresarse tanto intereses individuales como colectivos: se manifiestan tanto la voluntad política individual de cada ciudadano (a favor de algún candidato o decisión política) como la voluntad colectiva de todo un pueblo/comunidad (como mayorías y minorías).

El recorrido histórico vinculado a las formas de participación política de los últimos siglos permite identificar gran cantidad y variedad de regulaciones, tecnologías y sistemas de votación: desde los más públicos –con votos a '*viva voce*', a la vista de todos–, hasta los sistemas que garantizan el voto como un 'acto secreto'. Tal y como afirma Elster (2015), todos los sistemas electorales, con semejanzas y diferencias, combinan elementos públicos y secretos. Entre las instancias públicas es posible mencionar, entre otros, los padrones electorales, el lugar y el horario y los resultados alcanzados (por mesa, distrito, provincia, etc.). Entre sus elementos más reservados se destaca, obviamente, el voto individual. En la actualidad, la mayoría de las elecciones de representantes de los cuerpos políticos se realiza a través del voto secreto[33].

En los últimos siglos se fueron construyendo las condiciones temporales, espaciales y tecnológicas específicas para garantizar el sufragio universal, igual, secreto y obligatorio[34] (Kropf, 2016). Así lo expresa el artículo 21(3) de la Declaración Univer-

[32] La autoconciencia y la autodeterminación se relacionan con las capacidades de pensar, elegir, criticar, reflexionar, empatizar, aprender, innovar y muchas de otras capacidades necesarias para el relacionamiento social.

[33] Elster (2015) afirma que, si el secreto es la norma para elecciones de representantes y la publicidad es la norma para las asambleas, la situación entre secreto y publicidad del voto pasa a ser menos clara para jurados, cortes con múltiples miembros, agencias administrativas o en votaciones de comités de expertos. En la práctica es posible observar gran variedad de casos.

[34] El voto es obligatorio solo en algunos países del mundo y no es la regla: es obligatorio votar en la mayoría de los países de América Latina (Argentina, Brasil, Bolivia, Chile, Ecuador, Perú, Panamá, Costa Rica, República Dominicana, Venezuela), y en algunos pocos de Europa y el resto del mundo (Bélgica, Luxemburgo, Grecia, Tailandia, Egipto, Australia, entre otros).

sal de los Derechos Humanos de 1948[35]. Uno de los primeros países en reconocer y sistematizar el voto secreto fue Australia[36] (Brett, 2019). Al respecto, también pueden revisarse las experiencias de Francia, Países Bajos, Grecia, Colombia o Argentina[37]. Además del reconocimiento jurídico-político, el secreto del voto también tuvo que ser garantizado tecnológicamente: el diseño de espacios específicos y reservados para votar (cuartos oscuros y cabinas), el uso de urnas cerradas (para evitar la individualización del voto) o la designación de autoridades de mesa (para el cumplimiento de las leyes electorales).

De esta manera, con similitudes y diferencias, entre los siglos XIX y XX el voto fue construyéndose como una práctica regulada, protegida, atravesada por la dualidad público-privada. Por un lado, una práctica pública (y en muchos países obligatoria) vinculada a las capacidades de participación política democrática. Por el otro, el contenido del voto fue construyéndose como algo privado, secreto, reservado y oculto a la mirada de otros (sean pocos, muchos o todos). El voto secreto se orientó a proteger la libertad política que tiene cada ciudadano de participar en la selección de candidatos (o en la toma de otras decisiones políticas) sin que medien amenazas, influencias o presiones (de cualquier tipo y forma)[38]. Según Rosanvallón (1999; 2015), en la experiencia francesa, el secreto del voto se orientó a democratizar las elecciones y evitar la 'presión partidista' sobre la opinión popular.

El secreto del voto procura que una decisión (por un/a candidato/a A, B o C, o por una consulta popular) se mantenga solo reservada al individuo que ejerce el derecho (a su esfera íntima, privada, exclusiva). Si bien el resultado general de una elección es público, el voto secreto procura evitar que se pueda identificar el contenido del voto con cada votante. Incluso, un momento clave en esta historia, es que el voto devino también una práctica obligatoriamente secreta (es decir, no alcanzó con que el voto sea optativamente secreto). El voto obligatoriamente secreto se transformó así en una de las más simples, elegantes y extendidas medidas regulativas que se construyeron para garantizar que las decisiones y/o preferencias políticas sean solo conocidas por el votante (excluyendo a otras/os, los Estados y las corporaciones). Esta situación parece haber cambiado radicalmente.

VIII. CONCLUSIONES: LAS TENSIONES POR EL CONTROL DEL VOTO POPULAR

El extractivismo de todo tipo de datos personales que llevan adelante algunos Estados y sus corporaciones tecnológicas y la violación masiva y sistemática de la privacidad están afectando seriamente algunas libertades políticas y debilitando a la democracia representativa. En particular, el extractivismo de datos personales políticos vinculados al voto está generando una doble violación de derechos. La información política sobre a quién/es votó, vota o votará un ciudadano, un grupo social o la población, es un dato personal sensible alcanzado tanto por el derecho a la privacidad y la protección de datos personales como por la garantía del voto secreto-obligatorio. El análisis del caso Facebook Inc. – Cambridge Analytica/Strategic Communications Laboratories (entre otras empresas) permite observar claramente este doble proceso.

---

35 El artículo 21(3) de la Declaración Universal de Derechos Humanos expresa que:

> 3. La voluntad del pueblo es la base de la autoridad del poder público; esta voluntad se expresará mediante elecciones auténticas que habrán de celebrarse periódicamente, por sufragio universal e igual y por voto secreto u otro procedimiento equivalente que garantice la libertad del voto (1948).

En igual sentido, el artículo 23 del Pacto de San José de Costa Rica expresa que

> Todos los ciudadanos deben gozar de los siguientes derechos y oportunidades: [...] b) de votar y ser elegidos en elecciones periódicas auténticas, realizadas por sufragio universal e igual y por voto secreto que garantice la libre expresión de la voluntad de los electores [...] (Convención Americana de Derechos Humanos, 1969).

36 En la segunda parte del siglo XIX, Victoria, Australia, fue uno de los primeros lugares donde se garantizó la anonimidad en la relación voto-votante y en alcanzar el voto obligatorio y secreto. El secreto del voto se transformó en una de las formas fáciles y efectivas de limitar el poder de intimidación que tenían las aristocracias terratenientes de sur de Australia (Brett, 2019).

37 En la República Argentina el sufragio no fue reconocido explícitamente en la Constitución de 1853 (aunque sí de forma implícita a través de su artículo 33). Este fue regulado, por primera vez, en la Ley Sáenz Peña (Ley 8.871, 1912), donde se estableció el voto universal, secreto y obligatorio. A su vez, la Ley 13.010 (1947) otorgó el derecho de voto a las mujeres. La Reforma Constitucional de 1949 continuó con el reconocimiento "implícito" (artículo 36 de la Constitución Nacional de 1949 con redacción idéntica al artículo 33 de la Constitución Nacional de 1853). Con la reforma constitucional de 1994, artículo 37, el sufragio fue incluido explícitamente como derecho político: "[...] El sufragio es universal, igual, secreto y obligatorio" (Const. Nac., 1994).

38 Explica Elster (2015) que la razón para que el voto sea secreto (tanto en elecciones de gobierno como en votos emitidos por tribunales) es la protección de los votantes de posibles sobornos, intimidaciones o venganzas. El voto secreto se basó en el deseo de proteger a los votantes que se oponían al poder de pequeños concejos en manos de las oligarquías. Los votos en asambleas, por el contrario, no son secretos sino (en su gran mayoría) públicos.

A partir del análisis realizado es posible afirmar que las campañas electorales microsegmentadas, que usan perfiles psicográficos (y que incluyen datos personales políticos referidos al voto) están atravesadas por esta doble violación de derechos humanos. En momentos en que las leyes electorales están peligrosamente desactualizadas a nivel global, este tipo de campañas electorales se están transformando en una guerra de datos e información orientadas a la manipulación y el control del voto popular. Cada dispositivo (computadora, teléfono, televisor, etc.) conectado a internet comienza a ser un punto de intercambio de datos que, lejos de recibir mensajes (de candidatos) políticos, está siendo bombardeado con todo tipo de mensajes generados por computadoras (y por algoritmos) de acuerdo con perfiles psicológicos, estados de ánimo o predicciones de votos.

La publicidad indirecta, opaca, engañosa, microsegmentada, los anuncios oscuros (*dark ads*), las noticias falsas (*fake news*), no tienen puntos de comparación con las antiguas campañas electorales (por televisión, radio, carteles en la vía pública o prensa escrita). Los mensajes políticos enviados a través de Facebook Inc. son intencionalmente opacos: solo pueden ser vistos por usuarios finales, no se sabe quién/es los financian y, además, son imposibles de auditar (por Estados, ciudadanos y organizaciones comunitarias). La microsegmentación psicográfica favorece la construcción de conciencias políticas atomizadas, fragmentadas, divididas y agrietadas. Estas campañas atentan contra la autodeterminación, la construcción del espacio público-común y la democracia. Adecuar y fortalecer los sistemas electorales se presenta como una tarea urgente e imprescindible.

Esta adecuación va a requerir que las diferentes autoridades electorales tengan la capacidad de poder auditar, entre otros elementos clave, cuáles son los algoritmos que se usan para realizar esas campañas. Es necesario poder auditar y discutir sus diseños internos (por lo general, están ocultos, son cajas negras, de código privativo, cerrados). Muchos de estos algoritmos se están diseñando para conocer en profundidad y poder predecir las conductas de individuos, grupos, comunidades y poblaciones. Como tales representan un serio problema político. Por ello, es necesario que el diseño y uso de estos algoritmos respeten las leyes nacionales e internacionales, los derechos humanos, y que su diseño se produzca de forma abierta, cerca de los controles público-comunitarios y a través del conocimiento libre y compartido.

En sociedades democráticas los ciudadanos tienen que poder ejercer libremente su derecho al voto. Tienen que poder votar libres de amenazas, coacciones, propaganda oculta o campañas que operan subrepticiamente para modificar y condicionar sus conductas. El voto obligatoriamente secreto se construyó (se conquistó), justamente, para evitar este tipo de presiones políticas. Lamentablemente, en la era digital, esta solución simple, elegante e inteligente comienza a desvanecerse. Por ello, es necesario que la garantía constitucional del voto obligatoriamente secreto amplíe su cobertura espacio-temporal y pase a interpretarse de forma abierta, amplia y extendida. Es necesario que esta garantía proteja el secreto del voto antes, durante y con posterioridad al ejercicio del voto. Para ello, también es necesario volver a proteger los datos personales políticos de la ciudadanía.

Las democracias representativas se encuentran frente a un punto de no retorno. Si las capacidades de conocer o predecir el voto se fortalecen en algunos Estados y sus corporaciones tecnológicas, entonces, el voto popular podría pasar a ser secreto solo para los ciudadanos entre sí (es decir, entre quienes no poseen las máquinas de extraer datos e información de la población). El escenario futuro, en este caso, no es muy alentador. El voto popular podría estar migrando rápida y peligrosamente hacia un voto de 'secreto selectivo'. Es decir, un voto que, si bien no adquiere publicidad inmediata, su secreto pasa a depender de lo que 'otros' decidan sobre la información disponible. Estas intrusiones extractivistas y predictivas anticipan un aumento de la manipulación y los fraudes electorales y una disminución de las libertades políticas y de la vida democrática.

REFERENCIAS

Agencia Telam (19 de abril de 2018). Un cambio en Facebook hará que 1.500 millones de usuarios estén menos protegidos que los demás. *La Voz*. https://www.lavoz.com.ar/tecnologia/un-cambio-en-facebook-hara-que-1500-millones-deusuarios-esten-menos-protegidos-que-los-d/

Assange, J. (2013). *Criptopunks: La libertad y el futuro de internet*. Marea. Trilce.

(2014). *Wikileaks: When Google Met Wikileaks*. OR Books.

Ballhaus, R., & Gross, J. (2 de mayo de 2018). Cambridge Analytica Closing Operations Following Facebook Data Controversy. *The Wall Street Journal*. https://www.wsj.com/articles/cambridge-analytica-closing-operations-following-facebook-data-controversy-1525284140

Bartlett, J. (2018). *The People Vs Tech: How the internet is killing democracy (and how we save it)*. Penguin Random House.

Brett, J. (2019). *From Secret Ballot to Democracy Sausage: How Australia Got Compulsory Voting.* Swann House.

Briant, E. (4 de mayo de 2018). As Cambridge Analytica and SCL Elections shut down, SCL Group's defence work needs real scrutiny. *OpenDemocracy.Net*. https://www.opendemocracy.net/uk/emma-l-briant/as-cambridge-analytica-and-scl-elections-shut-down-scl-groups-defence-work-needs-re

Brito, R. (21 de marzo de 2018). Brazil prosecutors open investigation into Cambridge Analytica. *Reuters*. https://www.reuters.com/article/us-facebook-cambridge-analytica-brazil/brazil-prosecutors-open-investigation-into-cambridge-analytica-idUSKBN1GX35A

Cadwalladr, C., & Graham-Harrison, E. (17 de marzo de 2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Carelli, A. (22 de marzo de 2018). El Gobierno niega haber utilizado los servicios Cambridge Analytica. *Diario Perfil*. http://www.perfil.com/noticias/politica/el-gobierno-niega-haber-utilizado-los-servicios-cambridge-analytica.phtml

Collins, K. (17 de abril de 2018). Cambridge Analytica gathered Facebook data with 'sex compass' quiz. *CNET Internet Services*. https://www.cnet.com/news/cambridge-analytica-gathered-facebook-data-with-sex-compass-quiz-brittany-kaiser/

Davies, H. (11 de diciembre de 2015). Ted Cruz using firm that harvested data on millions of unwitting Facebook users. *The Guardian*. https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data

Digital, Culture, Media and Sport Committee (2018). *Disinformation and 'fake news': Interim Report* (Fifth Report of Session 2017-19). House of Commons. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf

(2019). *Disinformation and 'fake news': Final Report* (Eighth Report of Session 2017-19). House of Commons. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf

Elster, J. (2015). *Secrecy and Publicity in Votes and Debates*. Cambridge University Press.

Facebook Newsroom (4 de abril de 2018). Hard Questions: Q&A with Mark Zuckerberg on Protecting People's Information. *Facebook Newsroom*. https://newsroom.fb.com/news/2018/04/hard-questions-protecting-peoples-information/

Foucault, M. (1991). *Vigilar y Castigar: nacimiento de la prisión*. Siglo XXI.

Francis, L., & Francis, J. (2017). *Privacy: What Everyone Needs To Know*. Oxford University Press.

Galloway, S. (2017). *The four: the hidden DNA of Amazon, Apple, Facebook and Google*. Penguin.

Glencross, A. (2016). *Why the UK Voted for Brexit: David Cameron's Great Miscalculation*. Palgrave Macmillan.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the Surveillance State*. Metropolitan.

Hao, F., & Ryan, P. (2017). *Real-World Electronic Voting: Desing, Analysis and Development*. CRC Press.

Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*. Springer.

Kaiser, B. (2019). *The Cambridge Analytica Whistleblower's Inside Story of How Big Data, Trump, and Facebook Broke Democracy and How It Can Happen Again*. Harper Collins.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of the United States of America*, *110*(15), 5802-5805.

Kosinski, M., Wang, Y., Lakkaraju, H., & Leskovec, J. (2016). Mining big data to extract patterns and predict real-life outcomes. *Psychological methods*, *21*(4), 493-506.

Kriel, C., & Gellein, K. (realizadores) (2020). *People You May Know* [documental]. Metrotone Media.

Kropf, M. (2016). *Institutions and the Right to Vote in America*. Palgrave Macmillan.

Lefébure, A. (2014). *El caso Snowden: Así espía Estados Unidos al mundo*. Capital Intelectual.

Metcalf, J. (16 abril de 2018). Los efectos del escándalo de Facebook para el futuro de la democracia. *MIT Technology Review*. https://www.technologyreview.es/s/10138/los-efectos-del-escandalo-de-facebook-para-el-futuro-de-la-democracia

Neman, S. (8 de diciembre de 2016). Facebook's 2016 Year In Review. *Facebook Newsroom*. https://newsroom.fb.com/news/2016/12/facebook-2016-year-in-review/

Nix, A. (2016). Cambridge Analytica – The Power of Big Data and Psychographics. *Concordia Annual Summit in New York*. https://codingvideos.net/cambridge-analytica-the-power-of-big-data-and-psychographics/

Poitras, L. (realizadora). (2014). *Citizenfour* [documental]. Praxis Films, Participant Media, HBO Films. https://citizenfourfilm.com/.

Rampling, J. (realizador) (2017). *Secrets of Silicon Valley (I and II)* [documental]. BBC and The Open University. http://www.bbc.co.uk/programmes/b0916ghq

Reischl, G. (2008). *El engaño Google: una potencia mundial incontrolada en Internet*. Medialive Content.

Riofrío Martínez-Villalba, J.C. (2015). El derecho al secreto y la teoría del cono. *Revista Derecom*, (19), 137-163.

Romm, T. (26 de abril de 2018). Facebook didn't read the terms and conditions for the app behind Cambridge Analytica. *The Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2018/04/26/facebook-didnt-read-the-terms-and-conditions-for-the-app-behind-cambridge-analytica/?noredirect=on&utm_term=.a0e590fccda2

Rosanvallón, P. (1999). *La Consagración del Ciudadano: Historia del sufragio universal en Francia*. Instituto de Investigaciones Dr. José María Luis Mora.

(2015). *El buen gobierno*. Manantial.

Samuel, A. (11 de marzo de 2016). Psychographics Are Just as Important for Marketers as Demographics. *Harvard Business Review*. https://hbr.org/2016/03/psychographics-are-just-as-important-for-marketers-as-demographics

Schwartz, M. (30 de marzo de 2017). Facebook Failed to Protect 30 Million Users From Having Their Data Harvested by Trump Campaign Affiliate. *The Intercept*. https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/

Stahl, L. (22 de abril de 2018). Aleksandr Kogan: The link between Cambridge Analytica and Facebook. *CBS News*. https://www.cbsnews.com/news/aleksandr-kogan-the-link-between-cambridge-analytica-and-facebook/

Stewart, J. (5 de mayo de 2016). Facebook Has 50 Minutes of Your Time Each Day. It Wants More. *New York Times*. https://www.nytimes.com/2016/05/06/business/facebook-bends-the-rules-of-audience-engagement-to-its-advantage.html

Sumpter, D. (2018). *Outnumbered: From Facebook and Google to fake news and filter-bubbles -the algorithms that control our lives*. Bloomsbury Sigma

Troncoso Reigada, A. (2021). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales*. Civitas-Thomson Reuters.

United Nations Educational, Scientific and Cultural Organization [UNESCO]. (2014). *Fostering Freedom Online: The Role of internet Intermediaries. United Nations Educational, Scientific and Cultural Organization (UNESCO) y internet Society*. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

Vaidhyanathan, S. (2011). *The googlization of everything (And Why We Should Worry)*. University of California.

Vogel, K., & Parti, T. (7 de julio de 2015). Cruz partners with donor's 'psychographic' firm. *Politico*. https://www.politico.com/story/2015/07/ted-cruz-donor-for-data-119813

Youyou, W., Kosinski, M., & Stillwell, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Science of the United States of America*, *112*(4), 1036-1040. https://doi.org/10.1073/pnas.1418680112

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Furure at the New Frontier of Power*. Public Affairs Books.

Zuckerberg, M. (21 de marzo de 2018). Muro de Mark Zuckerberg. *Facebook*. https://www.facebook.com/zuck/posts/10104712037900071

NORMATIVA, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Acordada Extraordinaria No. 66-18. Ag. 16, 2018, A.L.J.A (Arg.).

A.G. Res. 68/167, Derecho a la privacidad en la era digital (18 de diciembre de 2013).

Constitución Nacional [Const. Nac.] 1949 (Arg.).

Constitución Nacional [Const. Nac.], 23 de agosto de 1994, B.O. (Arg.).

Convención Americana de Derechos Humanos (Pacto de San José), 22 de noviembre de 1969, O.A.S.T.S. No. 36.

Declaración Universal de los Derechos Humanos, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (10 de diciembre de 1948).

Ley 8.871, Ley Sáenz Peña, 26 de marzo de 1912, B.O. (Arg.).

Ley 13.010, Ley del voto femenino, 27 de septiembre de 1947, B.O. (Arg.).

Portaria No. 02/2018, Inquérito Civil Público - ICP - Cambridge Analytica / Facebook, 20 de marzo de 2018 (Bras.).

Reglamento 2016/679, del Parlamento Europeo y Consejo de la Unión Europea del 27 de abril de 2016 relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), 2016 O.J. (L 119) 1 (UE).

10.18800/themis.202101.007

LA FUNCIÓN PUBLICITARIA DE LAS *COOKIES*: MECANISMOS DE PREVENCIÓN Y CAUTELA EN EL DERECHO ESPAÑOL

THE ADVERTISING FUNCTION OF COOKIES: PREVENTION AND PRECAUTIONARY MECHANISMS IN SPANISH LAW

Juan Flaquer Riutort*
Universitat de les Illes Balears

The Internet increasingly radiates its essentialness in relationships, and in the different areas and activities of people. However, as we make a greater use of it, we expose our personal data to be stored and processed by third parties for commercial purposes. This is made possible by a tool that is present in most of the websites we browse on a daily basis: cookies.

In this article, the author assesses the risks involved in the use of cookies for advertising purposes without an adequate legal framework. Furthermore, he analyzes the prevention and precautionary mechanisms to follow in order to ensure a balance that respects the rights of users.

Keywords: Behavioral advertising; internet; cookies; privacy; consent

El internet cada vez más irradia su esencialidad en las relaciones, y en los diferentes ámbitos y actividades de las personas. No obstante, a medida que hacemos un mayor uso de este, nos exponemos a que nuestros datos personales sean almacenados y tratados por terceros con fines comerciales. Ello es posible a través de una herramienta que está manifiesta en gran parte de los sitios web que navegamos diariamente: las cookies*.*

En el presente artículo, el autor evalúa los riesgos que supone el empleo publicitario de las cookies sin un marco legal adecuado. Asimismo, analiza cuáles serían los mecanismos de prevención y cautela a seguir para garantizar un equilibrio que respete los derechos de los usuarios.

Palabras clave: Publicidad comportamental; internet; cookies; privacidad; consentimiento

* Abogado. Doctor en Derecho por la Universitat de les Illes Balears. Docente de Derecho Mercantil de la Universitat de les Illes Balears (Islas Baleares, España). Investigador de Derecho y Nuevas Tecnologías (CEDIB). Contacto: j.flaquer@uib.es

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 30 de noviembre de 2020, y aceptado por el mismo el 24 de marzo de 2021.

I. INTRODUCCIÓN

La importancia del internet en nuestra sociedad actual es una realidad incuestionable. Su proyección en la vida de los ciudadanos no hace sino crecer exponencialmente, manifestándose en la mayor parte de sus ámbitos, relaciones y actividades, sin que el sector económico constituya una excepción a ello. De hecho, cada vez son más las compras que se llevan a cabo en la red y buena parte de la publicidad que desarrollan las empresas se efectúa ya hoy en día de modo digital, hasta el punto de que la inversión en este sector se multiplica año a año y las empresas dedican buena parte de sus esfuerzos a asegurarse una presencia destacada en internet.

En este contexto, una de las formas en que esa publicidad se manifiesta es precisamente a través de la utilización de *cookies* o tecnologías de naturaleza similar. El objeto de este trabajo es justamente profundizar en dicha cuestión, tratando de analizar los evidentes riesgos que, en lo referido a la privacidad de las personas, puede plantear dicha técnica publicitaria, así como los mecanismos de prevención y cautela que pueden adoptarse en tal sentido.

Para ello, procederemos, en primer lugar, a explicar en qué consisten las *cookies* y las diferentes modalidades bajo las que se pueden presentar. Seguidamente, nos referiremos específicamente a su función publicitaria y al marco legal básico de referencia en el que se desenvuelve la materia objeto de estudio en nuestro país. Para finalizar, abordaremos los mecanismos de cautela y de prevención que pueden ser utilizados en la práctica, detallando las obligaciones y la responsabilidad en las que pueden incurrir las partes en la utilización de las *cookies*.

II. CONCEPTO Y CLASES DE *COOKIES*

Se conoce con dicho término aquellos archivos o dispositivos que se descargan al acceder a un determinado sitio web en el equipo terminal del destinatario de un servicio de la sociedad de la información, con la finalidad de almacenar datos que podrán ser actualizados y recuperados por la entidad que las instala, o incluso por un tercero, en el momento en que ese usuario vuelva a conectar con ese sitio o con otro que forma parte de la misma red. En otras palabras, por medio de las *cookies*, los prestadores de servicios obtienen datos relacionados con los usuarios, susceptibles de ser utilizados para diversos y variados fines.

Existen diversos tipos de *cookies*, las cuales se clasifican en función de la entidad que las gestiona (propias y de terceros), del plazo en que permanecen activas en el equipo terminal del usuario (de sesión y persistentes) y también de la finalidad o propósito que persiguen (técnicas, de análisis y publicitarias). Además, es destacable que una misma *cookie* puede ser incluida en más de una categoría (*cookies* polivalentes).

Las *cookies* propias son archivos que se envían al equipo o terminal del usuario desde el equipo gestor de la página web visitada y desde el que se presta el servicio solicitado, mientras que las *cookies* de terceros son aquellas otras que se envían desde otro terminal distinto al del gestor de la web visitada, con independencia de que será siempre el titular de la *cookie* el responsable del tratamiento de los datos personales por ella obtenidos.

Por su parte, las *cookies* de sesión o de entrada son aquellas que se mantienen solamente durante el tiempo que el usuario accede a un sitio web, siendo un ejemplo característico de ellas las utilizadas por los portales de comercio electrónico para recordar los productos añadidos al carrito de compra. Por otra parte, las *cookies* persistentes son almacenadas en el equipo del usuario de modo permanente, es decir, por un periodo de tiempo superior al de la simple sesión en que fueron instaladas.

Sin embargo, la distinción que nos interesa destacar especialmente ahora es aquella otra que fija su atención en la finalidad perseguida a través de su uso. Desde esta perspectiva, en un primer momento, las *cookies* tuvieron un carácter eminentemente técnico. Su propósito esencial era facilitar la prestación del servicio al usuario de internet, sirviendo de claro ejemplo aquellas que permiten recordar una contraseña al efecto de que la misma no tenga que proporcionarse de nuevo en cada conexión ulterior.

Con carácter más general, dentro de este grupo de *cookies* denominadas técnicas, la doctrina ha identificado las siguientes: (i) *cookies* de autenticación o identificación de usuario, que sirven para identificar al usuario desde el momento en que inicia la sesión; (ii) *cookies* de sesión de reproductor multimedia, que almacenan datos técnicos necesarios para reproducir el contenido de videos o audios; (iii) *cookies* de sesión para equilibrar la carga, que permiten distribuir el tratamiento de las solicitudes de un servidor web entre varios terminales en lugar de uno solo; (iv) *cookies* de personalización de la interfaz del usuario, que permiten al usuario navegar con unas características predefinidas, como puede ser la lengua de preferencia; y, finalmente, (v) *cookies* de complemento para intercambiar contenidos sociales o *plug-in*, cuya finalidad esencial es que los usuarios de una misma

plataforma social puedan intercambiar los contenidos que deseen o publicar comentarios (Navas Navarro, 2015, pp. 4 & ss).

Con todo, la finalidad de las *cookies* no se detiene en estos aspectos meramente técnicos, sino que el paso del tiempo ha demostrado que su instalación permite, asimismo, conseguir utilidades que van mucho más allá de esa primigenia finalidad. Así, puede hablarse también de *cookies* de análisis o de medición, que son aquellas cuyo propósito esencial es el de permitir al responsable de su instalación el seguimiento y análisis del comportamiento del usuario en la red. Es decir, ya no se trata solo de mejorar la prestación del servicio y, más específicamente, de facilitar su uso al destinatario, sino que se va más allá: se pretende utilizar la huella o los datos que deja cada sesión para comprender mejor, por medio de estadísticas, el perfil de los distintos usuarios, lo que podrá ser empleado, entre otras cosas, para mejorar los sitios web, aplicaciones, productos, servicios y anuncios visitados.

Pero, ahondando aún más en esa capacidad de las *cookies* para servir a finalidades más allá de las puramente técnicas, puede hablarse también de *cookies* publicitarias y de publicidad comportamental (*behavioural advertising*), que tienen como objetivo último una gestión más eficaz de los espacios publicitarios que aparecen en un sitio web, sobre la base de criterios como el contenido editado o la frecuencia en la que se muestran los anuncios. Se comprende de inmediato la extraordinaria importancia que tiene este tipo de herramientas, en la medida que todo el entramado construido en torno a la red y a esa gran aldea global en la que consiste internet, solo puede entenderse, y lo que sin duda es más relevante sostenerse, sobre la base de los ingresos publicitarios que genera todo este mercado virtual.

III. LA FUNCIÓN PUBLICITARIA DE LAS *COOKIES*

Es precisamente en esa sede que podemos percibir claramente la distinción entre dos conceptos que se revelan esenciales en este campo de la publicidad digital. Por un lado, el de editor, que se corresponde con aquella entidad prestadora de servicios de la sociedad de la información titular de una página web a la que puede acceder un usuario y para cuya prestación se utilizan *cookies*. Por otro lado, el de anunciante, que será aquel sujeto que pretende servirse de los soportes ofrecidos por el editor en su página web a efecto de publicitar sus productos o servicios.

Pues bien, es en este contexto en el que cobra trascendencia la finalidad publicitaria de las *cookies*, habida cuenta que el aprovechamiento de sus utilidades permite al anunciante asegurarse una publicidad mucho más personalizada y eficaz en los canales que pone a su disposición el editor. Dicho de otro modo, la posibilidad de ofrecer una publicidad ajustada al gusto y la preferencia de cada usuario constituye uno de los aspectos básicos que permiten sostener el mercado de la publicidad digital.

Naturalmente, este tipo de *cookies* publicitarias entraña un riesgo evidente para la privacidad del usuario, toda vez que tienen como finalidad detectar los gustos y las preferencias de este por medio del análisis y de la observación continuada de sus hábitos de navegación en la red. Se trata, por consiguiente, de una técnica especialmente intrusiva, aunque, como decíamos, absolutamente necesaria en el contexto del *marketing* digital y en el desarrollo consiguiente de lo que ha venido a denominarse publicidad comportamental, puesto que permite a las empresas anunciantes realizar un rastreo o *tracking* de las acciones de los usuarios de internet (palabras clave utilizadas, sitios web visitados y su frecuencia, etcétera). Esto facilita, a su vez, la configuración de perfiles predictivos susceptibles de ser utilizados posteriormente como publicidad a medida o personalizada.

El Dictamen 2/2010, emitido el 22 de junio de 2010 por el Grupo de Trabajo de Protección de Datos del Artículo 29 (en adelante, GT29), sobre publicidad comportamental en línea, define este tipo de publicidad como aquella

> basada en la observación continuada del comportamiento de los individuos, que busca estudiar las características de dicho comportamiento a través de sus acciones (visitas repetidas a un sitio concreto, interacciones, palabras clave, producción de contenidos en línea, etc.) para desarrollar un perfil específico y proporcionar así a los usuarios anuncios a medida de los intereses inferidos de su comportamiento (p. 5).

Con relación a ello, el GT29 no cuestiona los beneficios económicos que la publicidad comportamental pueda aportar a los que la practican, pero cree firmemente que esta práctica no debe realizarse a expensas de los derechos a la intimidad y a la protección de datos de las personas.

En una época como la actual, en que la navegación por medio de internet, a través de un sinfín de sitios web, constituye una práctica casi diaria de la mayor parte de los ciudadanos, se comprende fácilmente que la posibilidad de almacenar, recopilar, clasificar y, en última instancia, utilizar los datos o, si se prefiere, la huella que deja el usuario en la red, constituye un elemento de incalculable valor

para cualquier empresa cuyo objetivo último sea la producción de bienes o servicios en el mercado. Mas en particular, su propósito esencial se dirige a un objetivo claro: el envío posterior de publicidad *online* al destinatario sobre la base del perfil previamente trazado con arreglo a la información que las *cookies* han permitido generar y almacenar.

El GT29, en el ya citado Dictamen 2/2010, nos explica el funcionamiento de este tipo de *cookies*, denominadas **de rastreo**:

> el proveedor de redes de publicidad coloca una *cookie* de rastreo [que será distinta para cada buscador] en el terminal del usuario, la primera vez que este visita un sitio de internet que exhibe un anuncio de su red. […] el cookie así instalado permitirá al proveedor de la red de publicidad reconocer a un antiguo visitante que vuelve a dicho sitio o visita cualquier otro sitio asociado de la red publicitaria. La repetición de visitas permitirá al proveedor de la red publicitaria construir un perfil del visitante que se utilizará para producir publicidad personalizada (2010, p. 6).

De esta forma, como advertíamos anteriormente, se consigue una gestión mucho más eficiente de los espacios publicitarios que aparecen en cada sitio web, puesto que los mismos se verán personalizados conforme a los gustos y las preferencias de cada específico usuario, tomados, a su vez, de los datos que han sido almacenados y tratados previamente por medio de las *cookies* publicitarias instaladas en ese terminal. De tal modo, se logra que dos usuarios que visiten el mismo sitio web, el mismo día y a la misma hora, no vean el mismo contenido, ya que este va a depender del perfil particular de cada uno de los usuarios (Navas Navarro, 2015, p. 68).

Esta idea aparece definida de modo muy claro en cualquier sitio web que haga uso de este tipo de técnicas publicitarias. Tomemos como ejemplo de ello el caso de eBay, una conocida plataforma de compraventa a disposición de los particulares, en cuya página web, en la sección o pestaña dedicada precisamente a *cookies*, balizas web y tecnologías similares, puede leerse lo siguiente:

> [c]uando usas nuestros Servicios, nosotros, en colaboración con proveedores externos autorizados, utilizamos cookies y tecnologías similares. Utilizamos cookies y tecnologías similares que no se guardarán en tu dispositivo o que solo lo harán durante el tiempo que tu navegador esté activo (p. ej., cookies de sesión). Además, usamos cookies y tecnologías similares que se guardarán en tu dispositivo durante un período más largo (p. ej., cookies persistentes). Siempre que es posible, tomamos medidas de seguridad adecuadas para evitar el acceso no autorizado a nuestras cookies y tecnologías similares. Un identificador único (ID) garantiza que solo nosotros y proveedores externos autorizados tengamos acceso a los datos que se han recopilado por medio de cookies y tecnologías similares.
>
> Las cookies y las tecnologías similares que usamos cuentan con diversas funciones:
> - Pueden ser (técnicamente) necesarias para el aprovisionamiento de nuestros Servicios.
> - Nos ayudan a mejorar técnicamente nuestros Servicios (p. ej., supervisando los mensajes de error y tiempos de carga).
> - Nos ayudan a mejorar tu experiencia de usuario (p. ej., guardando el tamaño de fuente y los datos escritos en los formularios web).
> - Nos permiten mostrarte anuncios más pertinentes (eBay, 2020).

Observamos pues que se advierte expresamente al usuario del sitio web de la existencia de la finalidad específicamente publicitaria del uso de las *cookies*, ya sean propias o de terceros. Se ofrece también la posibilidad de desactivar la misma por medio de una conducta activa de aquel, de manera que se le devuelve el control referido al tratamiento que se haga de la huella que va dejando en su navegación por internet[1].

De lo expuesto hasta el momento, se deduce inmediatamente la importancia que adquiere este tipo de herramienta en el contexto de la publicidad y el *marketing* digital, constituyendo la información y los datos conseguidos y almacenados mediante este tipo de dispositivos un elemento de incalculable valor para las empresas en el desarrollo de su política comercial y publicitaria. Sin embargo, lo anterior no debe ocultar el riesgo que dicha práctica entraña en todo lo referido a la privacidad e intimidad de los usuarios de servicios de la sociedad de la información, por cuanto resulta obvio que la

[1] En efecto, en la página web del portal citado con anterioridad puede leerse también lo siguiente:

> Cuando utilizas eBay controlas la información que compartes y puedes actualizar tus ajustes en cualquier momento. Esta política describe cómo utilizamos las cookies, colaboramos con los anunciantes y recopilamos información de tus diferentes dispositivos para crear una experiencia consistente y personalizada para ti. Para optimizar tu experiencia, nos gustaría configurar tus ajustes para que coincidan con lo que ves a continuación. Si quieres editar tus preferencias, puedes hacerlo ahora o en cualquier momento en el futuro (eBay, s.f.).

elaboración de estos perfiles predictivos, sobre la base de la observación de determinados patrones de conducta, puede incidir de manera directa en la esfera íntima y personal de aquellos.

De ahí que el uso de *cookies* plantee evidentes problemas de coordinación con toda la normativa referida a la protección de datos de carácter personal, debiendo buscarse un punto de equilibrio que permita el desarrollo y la consolidación de un mercado digital al que es difícil renunciar en la actualidad, pero que garantice, a su vez, el debido respeto a los derechos individuales de las personas que hacen uso de los servicios de la sociedad de la información[2].

Observemos, a continuación, cuál es el marco legal básico en el que se desenvuelve dicho problema en el ordenamiento jurídico español y, por ende, en el europeo.

IV. MARCO LEGAL BÁSICO DE REFERENCIA

La norma básica que regula el uso de las *cookies* en España se halla contenida en el artículo 22.2 de la Ley 34/2002, de 11 de julio de 2002, de Servicios de la Sociedad de la Información y del Comercio Electrónico (en adelante, LSSI), cuyo redactado actual deriva, a su vez, de la adaptación de nuestra legislación a la Directiva 2009/136/CE, de 25 de noviembre, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[3] y el Reglamento 2006/2004/CE sobre la cooperación en materia de protección de los consumidores[4].

Dicho precepto establece lo siguiente:

> 2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
>
> Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.
>
> Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario (Ley 34/2002, 2002, art. 22).

Resulta importante reseñar que la remisión que el precepto realiza a la Ley Orgánica 15/1999 debe entenderse hecha en la actualidad al Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de los derechos digitales (en adelante, LOPDGDD).

De la lectura del artículo 22.2 de la LSSI, se desprende con prontitud que el sistema se articula esencialmente sobre dos conceptos básicos: por un lado, el deber de información y, por otro, el

[2] No en vano el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea (2000) y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) (2012) establecen expresamente que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

[3] Por lo que se refiere a esta específica Directiva, que es la verdaderamente relevante en la regulación de las *cookies*, se procedió a la modificación, entre otros, de su artículo 5.3, cuyo redactado actual es el siguiente:

> Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario (Directiva 2002/58, 2002).

[4] Dicha adaptación tuvo lugar por medio del Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas, en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista.

consentimiento del usuario o destinatario del servicio. Por lo que se refiere al primero de ellos, se trata de una obligación legal de hacer cuyo cumplimiento es de tracto sucesivo, de manera que la información tiene que estar siempre disponible para el usuario, recogiendo en todo momento los posibles cambios o actualizaciones en la misma que se vayan realizando por el titular de la *cookie* (Navas Navarro, 2015, pp. 84-85). Sin embargo, ni la LSSI, ni las directivas comunitarias mencionadas que se ocupan de la cuestión, abordan los aspectos concernientes a la forma en que debe mostrarse dicha información, ni a su contenido propiamente dicho, limitándose el artículo 22.2 de la LSSI a señalar que el consentimiento debe prestarse después de haberse facilitado una "información clara y completa" (Ley 34/2002, 2002).

Con todo, cabe presumir que dicha información, además de ser fácilmente accesible y visible, lo que desde luego impide su disimulo en condiciones generales o declaraciones genéricas de privacidad, debe permitir de modo permanente a un usuario medio comprender, como mínimo, cuál es la función y la finalidad que se persigue con la instalación del archivo correspondiente, puesto que solo por medio de dicha comprensión podrá estarse en condiciones de prestar el antedicho consentimiento (Vidal Portabales, 2013, p. 1091). De tal forma, según palabras del GT29, en lo que se refiere a la publicidad comportamental, "debe informarse claramente al usuario de que la *cookie* permitirá al proveedor de publicidad recoger información sobre sus visitas a otros sitios web, los anuncios que estos muestran, los anuncios en los que ha clicado, el tiempo utilizado, etc." (Dictamen 2/2010, 2010, p. 20).

Del tenor literal del artículo 22.2 de la LSSI, también se deduce que quedan exceptuadas del cumplimiento de las obligaciones recogidas en el precepto, las *cookies* utilizadas para alguna de las siguientes finalidades: (i) permitir únicamente la comunicación entre el equipo del usuario y la red, y (ii) prestar estrictamente un servicio expresamente solicitado por el usuario (Ley 34/2002, 2002). En atención a ello, el GT29, en su Dictamen 4/2012, ha interpretado que son las siguientes: (i) *cookies* de entrada del usuario; (ii) *cookies* de autenticación o identificación de usuario (únicamente de sesión); (iii) *cookies* de seguridad del usuario; (iv) *cookies* de sesión de reproductor multimedia; (v) *cookies* de sesión para equilibrar la carga; (vi) *cookies* de personalización de la interfaz de usuario; y (vii) determinadas *cookies* de complemento (*plug-in*) para intercambiar contenidos sociales (2012).

Sensu contrario, el citado documento nos indica que no están exentos de la obtención de consentimiento los siguientes supuestos: (i) *cookies* de complemento (*plug-in*) de contenidos sociales para el seguimiento, habida cuenta que no pueden considerarse estrictamente necesarias para prestar una funcionalidad solicitada explícitamente por el usuario; (ii) *cookies* utilizadas en la publicidad comportamental; y (iii) *cookies* para análisis propio, que son instrumentos de medición estadística de audiencia de los sitios web (Dictamen 2/2010, 2010). Con respecto a este último caso, el GT29 considera que no es probable que supongan un riesgo para la privacidad, en la medida en que se limiten estrictamente a fines estadísticos propios y que sean utilizadas por sitios web que ya ofrecen información clara sobre estas *cookies* conforme a su política de privacidad, así como garantías adecuadas de privacidad.

En la aplicación e interpretación de este marco legal básico de referencia, ha jugado un papel esencial en nuestro país la Agencia Española de Protección de Datos (en adelante, AEPD), la cual ha venido ofreciendo las pautas y criterios conforme a los que debe ser vigilado el adecuado cumplimiento de las obligaciones y los deberes impuestos a los prestadores de servicios de la sociedad de la información a propósito del respeto de la privacidad de los datos personales. En relación a este último aspecto, constituye un documento de indudable utilidad la Guía sobre el uso de las *cookies* (en adelante, la Guía), publicada en julio de 2020 por la AEPD, por cuanto nos servirá de punto de partida para el análisis de los mecanismos legales de cautela y prevención en lo referido a la función publicitaria de las *cookies*.

V. MECANISMO DE CAUTELA Y PREVENCIÓN

En este apartado, vamos a fijar nuestra atención en las obligaciones que se derivan del artículo 22.2 de la LSSI, así como en la identificación de las personas en las que deben recaer esos deberes, puesto que ambas cuestiones se erigen en los mecanismos básicos de cautela y prevención que el ordenamiento jurídico prevé para tratar de conciliar y hacer compatibles el uso de las *cookies*, y de alguna de sus finalidades, con el necesario respeto a la privacidad de determinados datos personales de los usuarios de un servicio de la sociedad de la información.

A. Obligaciones

Ya hemos visto anteriormente que las obligaciones legales impuestas por la normativa de referencia son esencialmente dos: por un lado, la obligación de transparencia o deber de información y, por otro, la de obtención del consentimiento del usuario o destinatario del servicio en cuestión. Veamos cada una de ellas por separado.

1. Deber de información y de transparencia

El artículo 22.2 de la LSSI dispone que se debe facilitar a los usuarios información clara y completa sobre la utilización de los dispositivos de almacenamiento y recuperación de datos, y, muy particularmente, sobre las finalidades que se persiguen por medio del tratamiento de los mismos. Por consiguiente, la información sobre las *cookies* recabada en el instante de solicitar el consentimiento debe ser suficientemente completa y transparente, con el objeto de que el usuario pueda entender fácilmente las finalidades y el uso que se dará a los datos personales almacenados o susceptibles de recuperación en un momento posterior.

A tales efectos, la Guía de referencia nos indica la información que debe incluirse en la política de *cookies* puesta a disposición de los usuarios de un determinado servicio, de conformidad esencialmente con lo dispuesto en el artículo 13 del RGPD, a saber (Agencia Española de Protección de Datos [AEPD], 2020, pp. 15-17):

a) Definición y función genérica de las *cookies*[5].

b) Información sobre el tipo de *cookies* que se utilizan y su finalidad, aclarando que si no fuera posible para el editor ofrecer una explicación suficiente sobre la finalidad de las *cookies* utilizadas por terceros, o de la forma de eliminarlas, se puede facilitar esta información incluyendo un enlace a la página web de ese tercero.

c) Identificación de quién utiliza las *cookies*, es decir, si los datos recabados serán tratados solo por el prestador de ese servicio o también por terceros a los que dé acceso aquel. Se aclara, en este sentido, que no será preciso que la información concreta sobre esos terceros aparezca directamente visible en la política de *cookies*, siendo suficiente con la utilización de mecanismos como botones que desplieguen esa información o textos emergentes que aparezcan cuando se pasa el puntero del ratón por encima.

d) Información sobre la forma de aceptar, denegar o revocar el consentimiento para el uso de *cookies*, enunciadas por medio de las funcionalidades facilitadas por el prestador del servicio o a través de las plataformas comunes que pudieran existir para esta finalidad.

e) "Si el sistema de gestión o configuración de las *cookies* del editor no permite evitar la utilización de las *cookies* de terceros una vez aceptadas por el usuario, se facilitará información sobre las herramientas proporcionadas por el navegador y los terceros y se deberá advertir que, si el usuario acepta *cookies* de terceros y posteriormente desea eliminarlas, deberá hacerlo desde su propio navegador o el sistema habilitado por los terceros para ello" (p. 16).

f) En su caso, información sobre las eventuales transferencias de datos a terceros países realizadas por el prestador del servicio, especificando que, respecto de las transferencias que, en su caso, realicen terceros, será válida la remisión a la información que faciliten estos.

g) "Cuando la elaboración de perfiles implique la toma de decisiones automatizadas con efectos jurídicos para el usuario o que le afecten significativamente de modo similar, será necesario que se informe sobre la lógica utilizada, así como la importancia y las consecuencias previstas de dicho tratamiento para el usuario en los términos establecidos en el artículo 13.2 f) del RGPD[6]" (p. 17).

h) Periodo de conservación de los datos para los diferentes fines de tratamiento. A este respecto, conviene precisar que el Tribunal de Justicia de la Unión Europea, en su sentencia de 1 de octubre de 2019, en el asunto C-673/17, ha indicado que la información que el proveedor de servicios debe facilitar al usuario de un sitio de internet incluye el tiempo durante el cual las *cookies* estarán

[5] La Guía nos ofrece el siguiente ejemplo:

> ¿Qué son las cookies? Este sitio web utiliza cookies y/o tecnologías similares que almacenan y recuperan información cuando navegas. En general, estas tecnologías pueden servir para finalidades muy diversas, como, por ejemplo, reconocerte como usuario, obtener información sobre tus hábitos de navegación, o personalizar la forma en que se muestra el contenido. Los usos concretos que hacemos de estas tecnologías se describen a continuación (Agencia Española de Protección de Datos [AEPD], 2020, p. 15).

[6] No obstante, en las directrices del GT29 sobre decisiones individuales automatizadas y elaboración de perfiles, adoptadas el 3 de octubre de 2017, y revisadas por última vez y adoptadas el 6 de febrero de 2018, se reconoce que, por ejemplo, la publicidad comportamental no entra generalmente en el ámbito del artículo 22.2 del RGPD, ya que "en muchos casos típicos, la decisión de presentar publicidad dirigida basada en la elaboración de perfiles no tendrá un efecto significativamente similar en las personas" (AEPD, 2020, p. 17).

activas y la posibilidad de que terceros tengan acceso a ellas.

i) Finalmente, por lo que se refiere al resto de información exigida por el artículo 13 del RGPD, que no concierna específicamente a las *cookies*, podrá remitirse a la política general de privacidad.

Por su parte, este deber de información se complementa, a su vez, con el cumplimiento de una serie de requisitos de transparencia, que tienen como objetivo último una adecuada y accesible comprensión por parte del usuario del sentido y significado del almacenamiento de esos datos. En particular, merecen ser destacados los siguientes (AEPD, 2020, pp. 17-18):

a) La información o la comunicación debe ser concisa, transparente e inteligible, teniendo en cuenta, además, el tipo de usuario medio al que se dirige la página web, adecuando el lenguaje y el contenido de los mensajes a su nivel técnico.

b) "Se ha de utilizar un lenguaje claro y sencillo, evitando en todo momento el uso de frases que induzcan a confusión o desvirtúen la claridad del mensaje" (p. 18)[7].

c) La información ha de ser de fácil acceso, de manera que el usuario no debe buscarla, sino que debe resultar evidente para él dónde y cómo puede acceder a ella. En este sentido, internet ya no es algo nuevo o desconocido para los usuarios, y los prestadores de servicios conocen perfectamente los métodos que pueden utilizar para captar su atención, de modo que esa experiencia y conocimiento debería ser aprovechada en este punto.

Por lo demás, resulta conveniente que esa información siga siendo fácilmente accesible una vez obtenido el consentimiento para el uso de las *cookies*, permitiendo en todo momento al usuario gestionar su voluntad con respecto a las mismas. A este respecto, la Guía considera que se cumple dicho requisito cuando el sistema de gestión de las *cookies* (panel de configuración, plataformas de gestión del consentimiento, etc.) esté integrado en la propia política de *cookies* o cuando se incluya en la misma un enlace que lleve directamente al sistema de gestión (AEPD, 2020, p. 19).

De particular importancia en lo referido a este deber de transparencia es el sistema de información por capas, recomendado de manera especial por el GT29, habida cuenta que permite al usuario ir a aquellos aspectos de la declaración o aviso que sean de mayor interés para él, con independencia, claro está, que la totalidad de la información permanezca disponible en un único documento completo al que se puede acceder fácilmente en todo momento. Con ello, se evita la natural fatiga informativa que puede causar al usuario la utilización de un sistema de capa de información única.

De seguirse este sistema de información por capas, la Guía nos indica, en la primera de ellas, que puede identificarse bajo un término de uso común (como, por ejemplo, *cookies*), debería incluirse la siguiente información (AEPD, 2020, pp. 19-20):

a) Identificación del editor responsable del sitio web.

b) Identificación de las finalidades de las *cookies* que van a ser utilizadas.

c) Información sobre si las *cookies* son propias o también de terceros asociados a ese editor, sin que sea necesario identificar a los terceros en esta primera capa.

d) Información genérica sobre el tipo de datos que se van a recopilar y utilizar en caso de que se elaboren perfiles de los usuarios, como sería el caso de la publicidad comportamental.

e) Modo en el que el usuario puede aceptar, configurar y rechazar la utilización de *cookies*, con advertencia, en su caso, de la existencia de acciones que puedan determinar una aceptación tácita o presunta de las mismas;

f) Enlace claramente visible a una segunda capa de información en la que se incluye una información más detallada utilizando, por ejemplo, expresiones tales como 'política de *cookies*, *cookies*, más información, pulsa aquí', etc.

Esta información debe ser facilitada antes del uso de las *cookies*, incluida, en su caso, su instalación, de forma que, en el momento en que se accede a esa primera capa informativa, debe darse ya al usuario la oportunidad de aceptar o rechazar su uso o instalación.

[7] La Guía nos ofrece algunas frases que no deberían ser válidas como, por ejemplo, "usamos *cookies* para personalizar su contenido y crear una mejor experiencia para usted", "para mejorar su navegación", o "podemos utilizar sus datos personales para ofrecer servicios personalizados" (AEPD, 2020, p. 18).

Por su parte, en la segunda capa, que debe encontrarse disponible de forma permanente en el sitio web o en la aplicación, se deberá incluir ya todo el resto de información a la que hemos hecho anteriormente referencia, al detallar el contenido informativo derivado del artículo 13 del RGPD.

Al margen de esta posibilidad de informar por capas, la Guía nos ofrece también otras posibles formas de facilitar la información sobre *cookies*, de entre las que destacan las siguientes (AEPD, 2020, p. 22):

a) El suministro de la información a través de un aviso suficientemente visible.

b) Al darse de alta un servicio, o antes de descargar una aplicación, puede suministrarse esta información junto con la política general de privacidad, o con los términos y condiciones de uso del servicio, siempre que se ofrezca un enlace o acceso directo a la sección referida a *cookies* dentro del propio documento.

c) En estos últimos casos, también será posible suministrar la información y obtener el consentimiento *off-line*, siempre y cuando quede constancia de que los usuarios han sido informados individualmente y han consentido en ello.

2. Obtención del consentimiento

El consentimiento del usuario constituye el eje central sobre el que descansa la normativa a la que nos venimos refiriendo y el mecanismo de cautela más importante para aquel. Sin el mismo, no es posible que el prestador del servicio utilice las *cookies* para según qué tipo de finalidades, de modo que, siempre y en todo caso, precisará obtener ese consentimiento, que deberá ser otorgado de forma libre y, según hemos ido viendo, informado transparentemente.

Por lo que se refiere a quién debe prestar el consentimiento, la dicción literal del artículo 22.2 resulta clara al señalar a los destinatarios de los servicios de la sociedad de la información. En la aclaración de este concepto, conviene precisar que el apartado d) del Anexo de la citada Ley 34/2002 entiende como tales a "la persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información" (2002), es decir, el usuario.

Por su parte, el artículo 6 de la LOPDGDD nos indica que se entiende por consentimiento del afectado "toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen" (Ley Orgánica 3/2018, 2018, art. 6.1), definición que fue tomada del artículo 4.11 del RGPD.

Respecto del consentimiento libre, lo relevante es que nos hallemos ante una elección real por parte del interesado. El GT29 ha manifestado su preocupación por el hecho de que esa libertad de elección pueda verse relativizada en determinadas ocasiones, debido al desequilibrio de poder entre el responsable del tratamiento y el interesado. Precisamente por ello, apuesta por evitar la utilización de solicitudes de consentimiento por defecto, yendo incluso más allá, al entender que el consentimiento no podrá considerarse como libremente otorgado cuando se solicita de tal forma que, si el interesado no lo otorga, podría tener un efecto perjudicial para él (por ejemplo, denegación de un servicio a un cliente por falta de consentimiento) (Dictamen 2/2010, 2010).

En lo que atañe al consentimiento específico, lo que se pretende indicar es que se requiere una manifestación específica para cada finalidad, de manera que cuando se solicite el consentimiento para varias finalidades distintas, será necesario obtener un consentimiento por separado de cada una de ellas. El GT29 pone como ejemplo el de una empresa que solicita el consentimiento a sus clientes para utilizar sus datos para el envío de publicidad por medios electrónicos y, al mismo tiempo, para ceder esos datos a empresas de su grupo. En tales supuestos, los consentimientos deberán obtenerse por separado, por medio de casillas de verificación u otros mecanismos.

Por lo que se refiere al consentimiento informado, dicho requisito implica que el afectado conozca con anterioridad al tratamiento la existencia del mismo y las finalidades que persigue. Ello significa, según el GT29, que la información proporcionada al usuario deberá constar de un lenguaje claro y sencillo, y separada de otros puntos del contrato (por ejemplo, en una cláusula específica), recomendando a los responsables del tratamiento que se revise cuidadosamente el lenguaje utilizado para solicitar el consentimiento, evitando fórmulas excesivamente legalistas de difícil comprensión, sobre todo a la hora de indicar el derecho del interesado a retirar su consentimiento.

Este consentimiento libre, específico e informado puede ser obtenido por medio de fórmulas expresas, como sería el caso de hacer clic en un apartado o botón que indique 'acepto' o 'consiento',

o similares, pero también deducirse de una acción inequívoca realizada por el usuario. Ahora bien, lo que no es admisible es pretender derivar el consentimiento de la mera inactividad del usuario. Un claro ejemplo de ello sería continuar navegando en el sitio web de referencia, que bajo ningún concepto puede ser considerado como tal.

En particular, la Guía (AEPD, 2020, pp. 25-26) nos habla de lo siguientes mecanismos de obtención del consentimiento:

a) Al solicitar el alta en un servicio. Para ello, será necesario que el consentimiento se separe de los términos y condiciones de uso de la página web, de su política de privacidad o de las condiciones generales del servicio.

b) Durante el proceso de configuración del funcionamiento de la página web o de la aplicación, quedando el consentimiento integrado en la elección del usuario y recordando los ajustes elegidos por este.

c) A través de plataformas de gestión del consentimiento, siempre que cumplan los siguientes requisitos y garantías: (i) cumplir los requisitos de transparencia frente a los usuarios; (ii) obtener un consentimiento válido de los usuarios; y (iii) respetar ulteriormente las opciones de consentimiento de los usuarios y permitir su gestión, incluida la revocación.

d) Antes del momento en que se vaya a descargar un servicio o aplicación. En este caso, si las *cookies* no son necesarias para el funcionamiento de ese servicio o aplicación, se debe permitir al usuario dar su consentimiento antes de esa descarga.

e) Resulta relevante destacar, en este último sentido, que si el usuario desea ejercer un derecho que le está legalmente reconocido (por ejemplo, darse de baja de un servicio), y esa aplicación o servicio es el único medio del que dispone para lograr su propósito, no puede condicionarse el acceso a los mismos a la aceptación de las *cookies* no necesarias.

f) A través del formato de información por capas. En estos supuestos, en la primera capa, que contiene la información esencial, debe incluirse la petición del consentimiento para la utilización de las *cookies*, debiendo ser informado, de modo permanente, en la segunda capa sobre ese uso y el modo de configurarlas o rechazarlas.

g) Por medio de la configuración del navegador, por cuanto dicha posibilidad se halla expresamente contemplada en el artículo 22.2 de la LSSI. Para que ello sea válido, la Guía estima necesario que esa configuración permita a los usuarios manifestarse por separado para cada uno de los fines previstos por las *cookies*.

Resulta conveniente advertir que, una vez obtenido el consentimiento de modo válido, no será necesario recabarlo de nuevo cada vez que el usuario visite la página web desde la que se presta el servicio, salvo naturalmente que se cambien los fines de uso de las *cookies*, en cuyo caso será preciso actualizar la política de *cookies* y posibilitar la toma de una nueva decisión al respecto.

En línea con lo anterior, la Guía recomienda como buena práctica que la validez del consentimiento prestado por un usuario no tenga una validez superior a veinticuatro meses, de manera que deba ser actualizado a intervalos periódicos, dejando siempre a salvo la posibilidad de una retirada del mismo en cualquier momento (AEPD, 2020). La revocación debe configurarse de modo fácil, habilitando para ello un acceso simple y sencillo al sistema de gestión o configuración de las *cookies*.

Una cuestión particularmente interesante en esta materia es la referida a los denominados *tracking walls* o muros de seguimiento, que son sistemas que limitan el acceso a un sitio web en tanto el usuario no acepte previamente la instalación de *cookies* de rastreo por terceros. Como se comprenderá, nos hallamos ante una cuestión particularmente importante para los usuarios, por cuanto este tipo de herramientas dificulta o entorpece la libre navegación en la red, condicionándola a la aceptación previa de una opción de privacidad que tolere esta forma de intrusión.

A este respecto, el Supervisor Europeo de Protección de Datos (en adelante, SEPD) ha venido considerando que el acceso a las páginas web no debe condicionarse a que los individuos se vean forzados a consentir que sigan el rastro que deja su huella en la red, lo que equivale, en realidad, a apostar decisivamente por la existencia de un consentimiento libre y genuino, que no puede supeditarse a la previa aceptación de determinadas condiciones. Precisamente por ello, y principalmente sobre la base de que el tratamiento que se solicita, que no es otro que el de poder rastrear el comportamiento del usuario, no es necesario para la prestación del servicio que desea el usuario (navegar por el sitio web en cuestión), el SEPD recomienda la prohibición de

estos muros de seguimiento (Opinión 6/2017, 2017, pp. 21-22)[8].

B. Responsabilidad de las partes en la utilización de *cookies*

Ya hemos indicado anteriormente que la LSSI no define quién es el responsable de cumplir con la obligación de facilitar información sobre las *cookies* y obtener el consentimiento para su uso. Sin embargo, parece razonable entender que, con carácter general, los sujetos obligados son los prestadores de servicios de la sociedad de la información, entendiendo como tal a toda persona física o jurídica que proporciona servicios prestados normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario, así como aquellos servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios (Ley 34/2002, 2002, Anexo).

A tales efectos, la Guía de referencia distingue dos situaciones en función de la finalidad para la que se tratan los datos que se obtienen a través de la utilización de las *cookies*. Si se trata de fines exceptuados de las obligaciones de informar y de obtener el consentimiento, en realidad, no será preciso que el prestador del servicio informe de su utilización, ni que obtenga el consentimiento del que hemos hablado. Tan solo para el caso de que se empleen *cookies* de terceros, deberá cuidar de establecer contractualmente con estos que los datos no serán tratados con ninguna otra finalidad que no sea la de prestar el servicio al usuario.

Mayores dificultades nos planteará el supuesto en el que el prestador del servicio o los terceros utilizan las *cookies* para fines que no están exceptuados de ese deber de informar y de recabar el consentimiento. Si se trata de *cookies* propias, parece evidente que los deberes recaen en el prestador del servicio, que deberá informar y obtener el consentimiento siguiendo las pautas que hemos venido explicando hasta este momento.

En el supuesto en que se utilicen *cookies* de terceros, resulta evidente que esa responsabilidad alcanza ya no solo al prestador del servicio, sino que se extiende también a las otras entidades intervinientes en la gestión de las *cookies*. En este sentido, si se utiliza una plataforma de gestión del consentimiento, en la que los terceros puedan cumplir esos deberes, podemos entender que serán estos quienes respondan individual y directamente de su cumplimiento.

En estos supuestos, el prestador del servicio tan solo deberá asegurarse de que los interesados reciben la información necesaria y que están habilitados los mecanismos que permitan su consentimiento. Sin embargo, cuando no se usa una plataforma de gestión del consentimiento, se le hace más difícil al tercero cumplir con esos requisitos, por cuanto el usuario tiende a manifestar sus inquietudes al prestador del servicio, que es a quien más fácilmente puede identificar.

En este contexto específico de la responsabilidad, conviene recordar la distinción recogida en la normativa general sobre protección de datos entre responsable del tratamiento y encargado del mismo (artículos 28 y siguientes del RGPD). A este respecto, parece razonable entender que los titulares de las *cookies*, en tanto que determinan los fines y los medios del tratamiento, deben ser considerados como responsables de los datos y de la información personal que recogen, mientras que aquellos otros sujetos que se limitan a seguir las instrucciones del responsable tendrán tan solo la condición de encargados del tratamiento.

Desde este punto de vista, cada uno de esos responsables deberá responder del tratamiento concreto que realice, siendo perfectamente posible, de conformidad con lo dispuesto en el RGPD, una situación de corresponsabilidad, que se producirá en aquellas situaciones en las que varios sujetos determinen conjuntamente las finalidades y los medios del tratamiento (Reglamento 2016/679, 2016). En estos supuestos, el nivel de responsabilidad de cada uno de ellos deberá ser determinado tomando en cuenta la implicación que se tenga en ese determinado tratamiento.

En este último sentido, resulta de interés recordar que el artículo 37 de la LSSI dispone expresamente que

> […] cuando las infracciones previstas en el artículo 38.3 i) y 38.4 g) se deban a la instalación de dispositivos de almacenamiento y recuperación de la información como consecuencia de la cesión por parte del prestador del servicio de la sociedad de la información de espacios propios para mostrar publicidad, será responsable de la infracción, además del prestador del servicio de la sociedad de la información, la red publicitaria o agente que gestione directamente con aquel la colocación de anuncios en dichos espacios en caso de no haber adoptado medidas para exigirle el cumplimiento de los deberes de información y la obtención del consentimiento del usuario (Ley 34/2002, 2002).

[8] En sus posteriores Directrices 5/2020, el SEPD parece admitir esta práctica, siempre que se ofrezca una alternativa de acceso al servicio sin necesidad de aceptar el uso de *cookies*.

Por lo demás, en lo que atañe a las sanciones que pueden ser impuestas por el incumplimiento de las obligaciones referenciadas, cabe recordar que el artículo 38.4.g) de la LSSI considera como infracción leve el "utilizar dispositivos de almacenamiento y recuperación de datos cuando no se hubiera facilitado la información u obtenido el consentimiento del destinatario del servicio en los términos exigidos por el artículo 22.2" (Ley 34/2002, 2002), siendo la multa prevista para estos casos de hasta 30 000 euros.

En aplicación precisamente de esta normativa, son ya bastantes las sanciones que ha impuesto la AEPD en esta materia. Sirva a título de ejemplo, la última de ellas a la que hemos tenido acceso, en la que se constata que la página web denunciada utiliza un sistema de información por capas, informando en la primera de ellas de la utilización de *cookies* propias y de terceros, para mejorar los servicios y para mostrar publicidad relacionada con las preferencias de navegación, indicándose que "si continúa navegando, consideran que se acepta su uso", desplegando la misma información en la segunda capa y sin ofrecer la posibilidad al usuario de rechazar todas las cookies (Resolución PS/00208/2020, 2020).

V. CONCLUSIONES

Sin discutir en absoluto el necesario desarrollo y consolidación del mercado de la publicidad *online*, elemento imprescindible para garantizar un acceso libre e igual de todos los ciudadanos a los contenidos digitales ofrecidos en internet, las autoridades deben velar por un cumplimiento adecuado de las disposiciones que aseguran un respeto de la privacidad y de la intimidad personal de los usuarios.

En este contexto, resulta evidente que, más allá de aquellas *cookies* cuya utilización viene amparada por motivos técnicos o de interés público o general, que hallan su acogida en alguna de las excepciones previstas expresamente por la legislación, el uso de este tipo de dispositivos con el objeto de conocer los gustos y las preferencias de los usuarios con fines eminentemente publicitarios (*cookies* de rastreo o de seguimiento) plantea indudables problemas de encaje o acomodación con toda la normativa sobre protección de datos.

Sin poner en tela de juicio las voces que reclaman un cuidado equilibrio entre esta última necesidad y la de asegurar la pervivencia de determinados modelos de servicio digital, que solo pueden sostenerse por medio de una publicidad personalizada y atractiva para los anunciantes, lo cierto es que la situación actual, caracterizada por una presencia constante de molestos avisos en los sitios web, no garantiza, a nuestro entender, la prestación de un consentimiento suficientemente informado y consciente por parte de los usuarios, que acostumbran a recurrir a la fórmula del 'sí a todo' con tal de poder seguir navegando libremente en la red.

En este sentido, resulta de interés destacar, de cara al futuro, la existencia de una Propuesta de Reglamento del Parlamento europeo sobre la privacidad y las comunicaciones electrónicas (*e-Privacy*)[9], que parece apostar por una solución ecléctica, en la que se visualiza, y así se confirma de hecho en algunos de sus considerandos, un claro deseo de retornar, por así decir, al usuario el control o la llave inicial sobre el acceso a sus datos personales, por medio de las opciones de configuración que obligatoriamente le serán facilitadas e informadas en todo programa informático de navegación (2017). De tal forma, el usuario podrá configurar *ab initio*, después de recibir la información correspondiente por parte del proveedor o fabricante del programa informático, cuál de entre las distintas alternativas se ajusta mejor a sus deseos, sin que nada impida que opte por un sistema parecido al que hoy pretenden preservar las asociaciones más representativas del mercado de la publicidad digital.

De hecho, lo razonable es que así se haga si el usuario comprueba los problemas de navegación que pueden surgir cuando se adopta una opción especialmente preservadora de la privacidad personal. Naturalmente, en esta fase o estadio debería también apostarse por normas que impidan el establecimiento de muros de seguimiento que no se hallen debidamente justificados, siendo desde luego completamente inadmisibles aquellos que afecten a sitios web financiados por las autoridades públicas, los relacionados con la salud pública y cualquier otra materia de claro interés general, respecto de los cuales debe garantizarse siempre un libre e igual acceso, con independencia de cuál sea la opción de privacidad escogida por el usuario en su navegador.

La previsión específica de una configuración por defecto, obligatoria para los fabricantes, en la que se establezca una gestión de las *cookies* y de los dispositivos de archivo y almacenamiento lo más

[9] Propuesta de Reglamento del Parlamento europeo y del Consejo, de 10 de enero de 2017, sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE.

restrictiva posible en este campo, nos parece una solución un tanto excesiva, que seguramente, al margen de poner en peligro la existencia misma del mercado publicitario *online*, no se corresponde con la verdadera voluntad de un público suficientemente informado, al menos en lo referido a la necesidad de pago por determinados servicios que hasta ahora se han venido disfrutando de manera gratuita.

De ahí que, en líneas generales, la solución propuesta por el legislador comunitario nos parezca ciertamente razonable, por lo menos en lo referido a realzar las características del consentimiento ya consagradas en el RGPD, de entre las que destaca la de provenir de una clara acción afirmativa del usuario, y no de la simple inacción o de un comportamiento tácito; y en la vocación de asegurar que sea el usuario quien mantenga el control sobre el acceso y el almacenamiento de sus datos personales.

En este último sentido, resulta de interés destacar la sentencia del Tribunal de Justicia de la Unión Europea, de 1 de octubre de 2019, en el asunto C-673/17, en la que se indica expresamente que el consentimiento al que nos hemos venido refiriendo no se presta de manera válida cuando el almacenamiento de información, o el acceso a la información ya almacenada en el equipo terminal del usuario de un sitio de internet a través de *cookies*, se autoriza mediante una casilla marcada por defecto de la que el usuario debe retirar la marca en caso de que no desee prestar su consentimiento.

Parece claro, por consiguiente, que la mera inacción, consistente en dejar esa casilla marcada por defecto, sin ninguna otra acción posterior, no puede ser considerada como consentimiento a la luz de la normativa europea sobre protección de datos, lo que constituye, en todo caso, una cautela absolutamente necesaria para salvaguardar de modo eficaz la privacidad de los usuarios.

REFERENCIAS

Agencia Española de Protección de Datos [AEPD] (2020). *Guía sobre el uso de las cookies.* https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf

eBay (22 de julio de 2020). Cookies, balizas web y tecnología similar ("Aviso de cookies").https://www.ebay.es/help/policies/member-behaviour-policies/ebay-cookie-notice?id=4267

(s.f.). Publicidad y preferencias relacionadas. https://www.ebay.es/gdpr

Navas Navarro, S. (2015). *La personalidad virtual del usuario de internet. Tratamiento de la información personal recogida mediante cookies y tecnología análoga*. Tirant lo Blanch.

Vidal Portabales, J. (2013). Sobre las comunicaciones comerciales en la LSSI y CE: modificaciones introducidas por el RD 13/2012, de 30 de marzo, en materia de cookies. En A. Tobío, A. Fernández & A. Tato (eds.), *Estudios de Derecho Mercantil: libro Homenaje al Profesor José Antonio Gómez Segade* (pp. 1079-1096). Marcial Pons.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Agencia Española de Protección de Datos [AEPD], 26 de octubre de 2020, Resolución de Procedimiento Sancionador (PS/00208/2020) (Esp.).

Carta de los Derechos Fundamentales de la Unión Europea, 18 de diciembre de 2000, 2000 O.J. (C364) 1.

Caso C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände -Verbraucherzentrale Bundesverband e.V. c. Planet49 GmbH, ECLI:EU:C:2019:801 (oct. 1, 2019).

Dictamen 2/2010 sobre publicidad comportamental en línea del Grupo de Trabajo de Protección de Datos del Artículo 29 (GT29) (GT 171), U.N. Doc. 00909/10/ES (22 de junio de 2010) (UE). https://docplayer.es/5355355-Dictamen-2-2010-sobre-publicidad-comportamental-en-linea.html

Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies del Grupo de Trabajo de Protección de Datos del Artículo 29 (GT29) (WP 194), U.N. Doc. 00879/12/ES (WP 194) (7 de junio de 2012) (UE). https://www.apda.ad/sites/default/files/2018-10/wp194_es.pdf

Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal), 2002 O.J. (L 108) 51.

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), 2002 O.J. (L 201) 37.

Directiva 2009/136/CE del Parlamento Europeo y del Consejo de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) 2006/2004 sobre la cooperación en materia de protección de los consumidores, 2009 O.J. (L 337) 11.

Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, Supervisor Europeo de Protección de Datos [SEPD] (4 de mayo de 2020). https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf

Ley 34/2002, Ley de servicios de la sociedad de la información y de comercio electrónico (B.O.E. 2002, 34) (Esp.).

Ley Orgánica 15/1999, Ley de Protección de Datos de Carácter Personal (B.O.E. 1999, 15) (Esp.).

Ley Orgánica 3/2018, Ley de Protección de Datos Personales y garantía de los derechos digitales [LOPDGDD] (B.O.E. 2018, 3) (Esp.).

Opinion 6/2017, EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation) (2017). Supervisor Europeo de Protección de Datos [SEPD] https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas), COM (2017) 10 final (10 ene., 2017).

Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), 2016 O.J. (L 119), 1 (UE).

Versión consolidada del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea (TFUE), 26 de octubre de 2012, 2012 O.J. (C326) 1.

10.18800/themis.202101.008

ATANDO LOS NODOS SUELTOS: *BLOCKCHAIN* PARA LA REDUCCIÓN DE CORRUPCIÓN EN LAS LICITACIONES PÚBLICAS DE PROINVERSIÓN

TYING UP THE LOOSE ENDS: BLOCKCHAIN TO REDUCE CORRUPTION IN PROINVERSIÓN PUBLIC BIDDING

Dana Lorena Masumura Ynami*
Universidad del Pacífico

Valeria Alejandra Acosta Chia**
Universidad del Pacífico

The public-private partnerships in Peru have been created with the intention of establishing a middle ground between privatizations and the absolute control of the State in matters of public interest. The most characteristic example of this are concessions. Despite the benefits that this entails, high levels of corruption are revealed within the concession procedures, which reduces the credibility of the public private associations. Faced with this problem, the alternative of e-procurement arises, which implies the use of technologies to ensure the transparency and efficiency of public tenders. Within this, the blockchain functions as an instrument applicable to concession procedures.

In this article, the authors analyze how corruption appears as a latent problem in concessions, and then go on to answer why blockchain is an alternative to fight against it. Subsequently, they study how it would be possible to apply this in the concession procedures in charge of ProInversión. Finally, they identify the challenges that it would entail and analyze whether the use of the proposed tool is effective.

Keywords: E-procurement; blockchain; Public Private Associations; transparency; ProInversión.

Las asociaciones público-privadas en Perú han sido creadas con la intención de fijar un punto medio entre las privatizaciones y el control absoluto del Estado en asuntos de interés público. El ejemplo más característico de ello son las concesiones. A pesar de los beneficios que ello conlleva, se ponen en manifiesto altos índices de corrupción dentro de los procedimientos de concesiones, lo cual reduce la credibilidad en las asociaciones público-privadas. Frente a esta problemática, surge la alternativa del aprovisionamiento electrónico (e-procurement)*, que implica el uso de tecnologías para procurar la transparencia y eficiencia de licitaciones públicas. Dentro de ello, el blockchain funciona como un instrumento aplicable a los procedimientos de concesiones.*

En el presente artículo, las autoras analizan de qué manera la corrupción se muestra como un problema latente en las concesiones, para luego pasar a responder por qué el blockchain *es una alternativa para luchar contra ello. Posteriormente, estudian de qué manera sería posible aplicar ello en los procedimientos de concesiones a cargo de ProInversión. Finalmente, identifican los retos que conllevaría y analizan si el uso de la herramienta propuesta resulta efectivo.*

Palabras clave: E-procurement; blockchain*; asociaciones público-privadas; transparencia; ProInversión.*

* Estudiante de la Universidad del Pacífico (Lima, Perú). Miembro de la sociedad de honores Alpha Sigma Nu - Capítulo de la Universidad del Pacífico. Contacto: danamasumuray@gmail.com.

** Estudiante de la Universidad del Pacífico (Lima, Perú). Coordinadora legal de 180 Degrees Consulting Universidad del Pacífico. Contacto: valeriaacostachia@gmail.com

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 9 de enero de 2021 y aceptado por el mismo el 7 de abril de 2021.

I. INTRODUCCIÓN

Las asociaciones público-privadas (en adelante, APPs) constituyen el punto medio entre las privatizaciones y el control absoluto del Estado en asuntos de interés público. En términos generales, esta figura se construye a partir de la definición de bienes públicos que tienen como principal característica la no rivalidad y la no exclusión; en otras palabras, dichos bienes pueden ser usados por varias personas simultáneamente sin perjudicarse entre sí y crear sistemas de exclusión resulta muy costoso. En ese sentido, es evidente concluir que un privado no podría encargarse de manera absoluta de bienes públicos, por lo que es necesaria la intervención del Estado. Por otro lado, el sector privado cuenta con un nivel de *expertise* y recursos de los cuales el Estado puede ser beneficiario en la formulación de proyectos que satisfagan una necesidad pública determinada.

De esta manera, las APPs buscan "permitir al sector público y al sector privado beneficiarse de las sinergias creadas con la unión de recursos financieros, conocimientos y experiencia" (O'Neill de la Fuente, 2008, p. 64). Un ejemplo por excelencia de este concepto son las concesiones que, precisamente, fueron la primera forma de introducción de las APPs en el Perú.

No obstante, a pesar de todos los beneficios mencionados, existe un alto grado de corrupción en los procedimientos de concesiones, lo cual conlleva al deterioro y la falta de credibilidad de las APPs. Sobre este aspecto, en líneas generales, el Perú ha demostrado poseer un alto nivel de corrupción según el Índice de Percepción de la Corrupción, realizado de manera anual por la organización Transparencia Internacional. Así, el país ha obtenido una puntuación de 35, ocupando la posición de 101 dentro de un universo de 180 países. Dentro de la última data, la media ha resultado ser de 43, por lo que los resultados no son satisfactorios (Transparencia Internacional, 2020). Por otro lado, en cuanto a las carpetas fiscales que se encuentran en investigación, el 78.79% de los casos están vinculados a infraestructura y corrupción (Ministerio Público, s.f.).

Frente a este problema, una alternativa que hoy en día es muy recomendada por varias entidades internacionales es el aprovisionamiento electrónico (*e-procurement*, por el término en inglés), que sugiere la implementación de tecnologías para coadyuvar no solo en la transparencia, sino también en la eficiencia de las licitaciones públicas. De esta manera, el *blockchain* se encuentra dentro de los instrumentos que podrían emplearse en los procedimientos de concesiones a cargo de ProInversión.

La tecnología *blockchain* se conoce, mayormente, porque ha permitido la creación de las criptomonedas, como Bitcoin o Ethereum. Sin embargo, este instrumento tiene un sinnúmero de aplicaciones, entre ellas, en el ámbito de las licitaciones públicas. Las características propias del *blockchain* (transparente, descentralizado, trazable y sin intermediarios) hacen de este una herramienta ideal para combatir la corrupción.

En las siguientes líneas, se analizará la corrupción como un problema latente en las concesiones y por qué este ámbito en específico ha demostrado ser muy vulnerable. Seguidamente, se explicarán los motivos por los cuales el *blockchain* supone una posibilidad en la lucha contra la corrupción y la implementación del *e-procurement*. Adicionalmente, se expondrá cómo podría implementarse en los procedimientos de concesiones a cargo de ProInversión, los retos que ello supone y se responderá a la disyuntiva sobre si esta tecnología resulta ser suficiente.

II. DEFINICIÓN DEL PROBLEMA: EXISTENCIA DE CORRUPCIÓN EN LAS LICITACIONES PÚBLICAS A CARGO DE PROINVERSIÓN

La organización Transparencia Internacional ha definido la corrupción como "abuse of entrusted power for private gain"[1] (2013, p. 16). Este abuso de poder puede ocurrir en una multiplicidad de ámbitos, incluyendo las licitaciones públicas. De esta manera, se generan varios costos, tales como la mala asignación de recursos públicos, una menor calidad en los servicios públicos, distorsión en la competencia dentro de los procedimientos, entre otros (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2016). Asimismo, "[it] has been estimated that where corruption is systematic it can be expected to account for 20-30% of government procurement, and maybe more"[2] (Schapper, 2007, p. 7).

Ahora bien, el ámbito de las concesiones o de las contrataciones públicas en general consiste en uno de los ámbitos más vulnerables a actos de corrupción. El World Economic Forum (2020, p. 8) men-

[1] Traducción libre: "abuso del poder encomendado para beneficio privado".

[2] Traducción libre: "se ha estimado que cuando la corrupción es sistemática se puede esperar que represente entre el 20 y el 30% de las adquisiciones del Gobierno, y tal vez más".

ciona que existen cinco razones principales por las cuales ocurre esto:

a) Implican grandes cantidades monetarias: cada año, los gobiernos dirigen entre el 10% a 30% del PBI a las contrataciones públicas.

b) Las contrataciones públicas implican una constante interacción entre privados y funcionarios públicos, lo cual incrementa las posibilidades de que ocurra un acto de corrupción, al combinarse intereses públicos y privados.

c) Generalmente, se trata de un proceso muy complejo y burocrático.

d) Existe un nivel bajo de transparencia en este tipo de procedimientos, lo cual muchas veces deja la distribución de grandes cantidades de dinero a la discrecionalidad de los funcionarios públicos a cargo.

e) Incluso en el escenario donde un acto de corrupción es detectado, no es muy frecuente que esto sea reportado o denunciado.

Los instrumentos normativos que regulan las APPs son el Decreto Legislativo 1362 (en adelante, DL 1362) y su reglamento, el Decreto Supremo 240-2018-EF (en adelante, el reglamento). El artículo 30.1 del DL 1362 indica que las APPs constan de las siguientes fases: (i) planeamiento y programación; (ii) formulación; (iii) estructuración; (iv) transacción; y, (v) ejecución contractual. Así, se concluye que las etapas de transacción y ejecución contractual son las más vulnerables a actos de corrupción, debido a que son los momentos en los cuales se incorpora al privado dentro del procedimiento.

Sobre la etapa de transacción, la Organización para la Cooperación y el Desarrollo Económicos (en adelante, OCDE) ha ilustrado algunos actos de corrupción que podrían presentarse en esta fase (2016). Existen casos de falta de competencia entre los postores o incluso colusión entre ellos (ofrecimiento de ofertas equivalentes u ofertas que, agregadas entre sí, pueden cubrir la demanda de la entidad pública). Asimismo, está la probabilidad de conflictos de interés y corrupción en el proceso de evaluación de las ofertas (ha existido un constante contacto con alguno de los postores en distintos procedimientos a lo largo del tiempo o existe el fenómeno de las 'puertas giratorias'). Así como también, una falta de acceso a la documentación.

Con relación a la fase de ejecución contractual, pueden darse escenarios como abusos por parte del ofertante o por parte del Estado, los cuales ocurren por dos motivos: (i) el privado quiere entregar algo incompleto; o, (ii) el Estado quiere exigir un requisito no contratado inicialmente. La facilidad con la que puede modificarse cualquier documento genera incertidumbre respecto de las obligaciones de cada parte; puesto que no se tiene base cierta respecto de cuáles eran las verdaderas cláusulas. Esto último, paralelamente, crea un efecto adverso que se traduce en desincentivos para contratar. Asimismo, este factor desencadena en ineficiencia a lo largo del procedimiento. Por otro lado, hay una supervisión deficiente de las obligaciones financieras o una falta de supervisión de los funcionarios (OCDE, 2016).

Asimismo, se ha demostrado que una práctica recurrente en el Perú son las adendas. Este mecanismo funciona de la siguiente manera: uno de los competidores postula una oferta agresiva para ganar la licitación y, una vez firmado el contrato, tratará de renegociarlo incluyendo adendas para recuperar el monto perdido a raíz de la oferta agresiva (Gálvez Córdova, 2017).

Como puede observarse, existen muchos riesgos dentro de estas dos fases en concreto. En ese sentido, ProInversión ha creado un Nuevo Plan de Integridad y Lucha contra la Corrupción 2019-2021, aprobado por la Resolución de Secretaría General 058-2020. Esta política ha sido creada en línea con instrumentos o acuerdos que tienen efecto a nivel nacional: el Acuerdo Nacional, la Política Nacional de Integridad y Lucha contra la Corrupción, el Plan Nacional de Integridad y Lucha contra la Corrupción (2018-2021) y el Plan Sectorial de Integridad y Lucha contra la Corrupción 2019-2021. Respecto de las políticas nacionales, estas tienen como uno de los aspectos principales la capacidad preventiva del Estado frente a los actos de corrupción, lo cual tiene como una de sus variantes la transparencia.

Respecto del caso particular de ProInversión, se tiene como objetivo específico garantizar la transparencia y el acceso a la información pública de la entidad. Sobre ello, existen también acciones para lograr los objetivos, entre los cuales se encuentra implementar el uso de tecnologías digitales para el incremento de la transparencia y rendición de cuentas, y realizar campañas de capacitación y difusión sobre temas de transparencia y acceso a la información pública a los trabajadores de la entidad. Si bien existen este tipo de políticas, no se observan acciones específicas con las que verdaderamente se logren los objetivos planteados.

En este contexto, el *blockchain* posee características que coadyuvarían a materializar las acciones y por lo tanto a lograr los objetivos planteados en el Nuevo Plan de Integridad y Lucha contra la

Corrupción 2019-2021. Así, "[when] corruption represents a breach of trust, a technology that strengthens trust becomes an attractive solution in public projects"[3] (Aarvik, 2020, p. 10); es decir, la confianza en el código o en la programación de la tecnología podría restaurar la confianza en los procedimientos de concesiones y en los funcionarios públicos.

III. *BLOCKCHAIN*

Blockchain es una tecnología que en los últimos años se ha ido implementando para distintas funciones, de las cuales la más conocida es el Bitcoin. Sin embargo, para poder instaurar dicha tecnología, es necesario conocer cómo funciona.

Blockchain es un *distributed ledger* que almacena bloques unidos e implementados a base de la criptografía. Cada uno de los bloques se concatenan con el siguiente, usando una firma criptográfica o *hash* (American Council for Technology - Industry Advisory Council, 2017). De esta manera, cada bloque contiene una referencia al bloque inmediato anterior, al sello de tiempo y el dato de transacción. Esto permite mayor seguridad y consigue que las adiciones, alteraciones o supresiones no autorizadas sean difíciles –casi imposibles– de realizar u ocultar.

Berryhil, Bourgery y Hanson (2018) definen el *hash* como una función criptográfica que genera un código único a cualquier información que se coloque en *blockchain*, por ejemplo, una imagen. Así, indican que si cualquier parte del contenido introducido se modificara (como un número o signo), el código *hash* cambiaría a uno totalmente diferente y único, por ello es casi imposible que se altere información en el *blockchain* sin que se conozca. De esta manera, ante cualquier modificación en la información, los nodos que se encargan de validar las transacciones de los bloques no aprobarían la transacción, al ser evidente para ellos la alteración que se ha realizado.

Asimismo, cabe indicar que existen diferentes tipos de nodo, entre ellos se encuentran principalmente los siguientes (Rodríguez Garagorri, 2017):

a) Nodos completos: son conectados a la red y verifican el cumplimiento de las normas acordadas en el mecanismo de consenso, corroborando que las transacciones empleadas sean válidas y brindando interfaces para otros nodos.

b) Nodos mineros: son los encargados de generar los nuevos bloques, por lo que necesitan de un alto grado de procesamiento. Funcionan en grupos.

c) Nodos ligeros: no realizan verificaciones de la totalidad de la cadena, sino que confían en que una transacción que se encuentra en un bloque es válida; por lo cual, estos nodos dependen de la verificación de los nodos completos para avalar la seguridad.

En ese sentido, los bloques se agregan al *blockchain* a través de un proceso llamado *mining*. Después de que un nodo inicia una transacción, esta es revisada y validada por los demás, luego se valida un grupo de transacciones y se añaden a un bloque, para que se introduzca el bloque validado al *blockchain* (Berryhil *et al.*, 2018). Al publicar el bloque, el nodo comienza a transmitir el bloque al resto de la red a través de un proceso automatizado por el *software* del *blockchain*. Dicho proceso puede ser programado sobre la base de la frecuencia del proceso y los diferentes parámetros asociados a él que se deseen.

Asimismo, es necesario tomar en cuenta que el *blockchain* se basa en un modelo de consenso. En ese sentido, cada nodo debe obtener permiso para poder publicar un bloque en el *blockchain* según las reglas programadas en este. Así, cuando un nodo publica un bloque, este es compartido a través de todo el sistema, generando una copia de la información o transacción realizada en cada uno de los nodos. De esta manera, la única forma en que se concatena un bloque o una transacción inválida a este sistema es si la mayoría de los nodos están de acuerdo con ello. Esto último es conocido como el "ataque del 51%" (Berryhil *et al*., 2018). El 'ataque del 51%' es una técnica que ocurre cuando el atacante está en posesión del 51% del poder de *hashing*. En ese sentido, este ataque empieza creando una cadena de bloques privados, que se encuentran aislados de la cadena de bloques reales; y, se presenta a la red para que sea considerada como una cadena real. Motivo por el cual, si los atacantes consiguen el 51% del poder de *hashing* o más, podrán tener la cadena más larga, persuadiendo a los nodos a que pertenezcan a la misma. Por lo tanto, mientras uno posea más poder de *hashing*, las probabilidades de comprometer el *blockchain* aumentan (Sayeed & Marco-Gisbert, 2019).

Entre las características principales del *blockchain* se encuentra que es un sistema distribuido y com-

[3] Traducción libre: "cuando la corrupción representa un abuso de confianza, una tecnología que refuerce la confianza se convierte en una solución atractiva en los proyectos públicos".

partido. Por ello, tiene el potencial de reducir y eliminar los costos que producen los intermediarios y contribuir a la integridad de la información y descentralización, al igual que generar confianza en las transacciones, generando un impacto positivo en cómo se dan las operaciones hoy en día.

Por otro lado, también encontramos la inmutabilidad de las transacciones que se almacenan en el *blockchain*. Como se ha mencionado anteriormente, una vez que la transacción se añade es casi imposible modificarla, a menos que se dé el 'ataque del 51%', siendo vital para la confianza en el *blockchain*. Ello a diferencia de otros sistemas de almacenamiento de transacciones en los cuales si se modifica la información en la base de datos, no hay ningún respaldo con el cual esta transacción, operación o información se pueda respaldar. En ese sentido, si es que la seguridad del servidor se ve corrompida, la información se puede modificar o eliminar, sin que sea perceptible a primera vista, lo cual da lugar a que se den casos de fraude.

Igualmente, entre las características del *blockchain* antes mencionadas, aquel permite que se perfeccione la transparencia entre los usuarios al momento de validar las transacciones, teniendo un registro de todas las operaciones que se realizan en el *blockchain*. Esto permite que este sistema tenga el potencial para generar oportunidades para los Gobiernos, reducir costos de operación, transacción, aumentando la transparencia y confianza entre los Gobiernos y los ciudadanos y facilitando las transacciones (Berryhil *et al*., 2018).

El *blockchain* tiene múltiples beneficios, entre los cuales se encuentra aumentar la confianza del público de las transacciones que se realizan a través de la transparencia y validación de la plataforma. Asimismo, es una herramienta que mejora la efectividad de las operaciones, debido a que emplea herramientas que permiten la automatización y reducen el margen de error, como lo son los *smart contracts,* que son contratos en los cuales cada transacción se puede ejecutar automáticamente a través de los términos pactados entre las partes, que han sido redactados en un código de *software*, los cuales se activan ante un determinado evento. Igualmente, en el caso que este quiera ser integrado a operaciones del sector público, este permite reducir la fricción entre las agencias, pues al regirse por la descentralización en las operaciones, reduce las barreras burocráticas, por ejemplo, características de cualquier gobierno.

También, según Yang se debe considerar que el *blockchain* es un sistema "borderless and frictionless" (2019), debido a que normalmente las transacciones comerciales requieren de intermediarios, lo cual agrega distintos costos. En ese sentido, tal sistema permite que se reduzcan dichos costos de transacción, al estar basado en criptografía y confianza, que permite que los individuos realicen transacciones directamente, ahorrando no solo recursos, sino también tiempo, que hoy en día es tan escaso.

Asimismo, considerando que una de las características del *blockchain* es que es un sistema de consenso, se debe describir los diferentes modelos de consenso que existen (Yaga *et al*., 2018):

a) *Proof of work*: en estos supuestos, un usuario publica un bloque cuando ha sido el primero en resolver el 'rompecabezas', y así la muestra de su trabajo es este resultado. Asimismo, cabe precisar que este rompecabezas está diseñado de tal manera que resolverlo es una ardua tarea, pero comprobar que una solución es válida no lo es. Esto a su vez permite a los nodos validar el bloque siguiente propuesto, por lo cual, cualquier bloque que sea propuesto, pero que no cumpla con el rompecabezas, será rechazado, permitiendo a los nodos validar el bloque siguiente propuesto.

b) *Proof of stake*: este modelo se basa en la idea de que cuanto más haya invertido un usuario en el sistema, es mayor la probabilidad que este quiera su éxito y menor la posibilidad que quiera desvirtuarlo. Por ejemplo, en el caso del Bitcoin, la participación puede estar representada por la cantidad de criptomonedas que el usuario ha invertido en el sistema, por distintos medios, como el bloqueo de un tipo de transacción especial en el sistema.

c) *Round Robin*: en este caso, los nodos se turnan para crear bloques, por lo cual, si un nodo no está disponible para publicar un bloque en su turno, los sistemas pueden incluir un tiempo límite para que los nodos disponibles puedan publicar los bloques, con la finalidad de evitar una interrupción en la publicación de bloques. Por lo tanto, este modelo en cierta medida garantiza que ningún nodo cree la mayoría de los bloques.

d) *Proof of authority*: el modelo se basa en la confianza parcial de los nodos que publican a través de su vínculo conocido con identidades del mundo real. En esa medida, los nodos deben tener sus identidades debidamente probadas y verificables dentro de la red (por ejemplo, documentos de identidad

notariados). En ese sentido, se considera que el nodo publicador se está jugando su reputación al publicar los nuevos bloques en el *blockchain,* a través de su vínculo conocido con identidades del ´mundo real´.

e) *Proof of elapse time*: mediante este modelo, cada nodo solicita un tiempo de espera a una fuente de tiempo de *hardware* segura dentro del sistema. Este *hardware* generará un tiempo de espera aleatorio y lo retornará al *software* del nodo. Así, los nodos utilizan este tiempo concedido y se vuelven inactivos durante este periodo. Una vez culminado este tiempo, el nodo ´despierta´ y crea y publica un bloque en la red. De igual manera, este modelo requiere verificar que el nodo esperó el tiempo real y no comenzó antes de tiempo, y que el tiempo de espera fue asignado de manera aleatoria para evitar acciones maliciosas.

Con la finalidad de reducir la potencialidad de corrupción en las licitaciones de ProInversión, es necesario tener en cuenta que el modelo de consenso que se debe seguir es el de *proof of authority*, pues en este se permite que únicamente los usuarios que cuenten con alguna autorización previa, que requiere de identificación, puedan registrar las transacciones en el *blockchain*. En ese sentido, el *blockchain* se convierte en una herramienta que permite la transparencia y la rendición de cuentas, sea de privados o por parte del Estado. Por ejemplo, hacer seguimiento de los pagos a proveedores, recibir productos o servicios, o manejar cronogramas de entrega, se realiza de una manera más ordenada y automatizada. Así, se reducen no solo los costos de transacción, sino también las oportunidades de corrupción, pues, como se ha mencionado anteriormente, la inmutabilidad de la información es una característica vital del *blockchain* que permite que toda modificación o alteración de la información sea perceptible y que ninguna transacción se realice sin la validación de los nodos.

Asimismo, otro beneficio que otorga el *blockchain* al momento de combatir la corrupción es que, mediante este modelo que requiere de permisos para poder registrar transacciones, el *blockchain* se puede programar a que posea determinadas reglas, que garanticen que quien realice la transacción sea un agente que cuente con una autorización auténtica. Por ejemplo, que se requiera validar identidades previo a cualquier operación, ya sea mediante medidas biométricas, códigos, entre otros.

Igualmente, este modelo, de ser usado para actividades del Gobierno, permite que se implementen reglas que sean necesarias para garantizar la transparencia, rendición de cuentas, integridad, entre otros, como lo son políticas públicas anticorrupción, reglamentos y demás normas emitidas. Así, para operaciones del Estado, las autoridades locales y del Gobierno central, de implementarse la tecnología *blockchain*, se volverían menos relevantes en determinados contextos, pasando a un plano secundario, en lugar de procurar realizar cada actividad de manera descentralizada, concentrando sus esfuerzos y recursos en otras áreas, como mejorar la educación o la salud pública.

Por otro lado, se debe tomar en cuenta que el *proof of authority* no solo acelera el proceso de licitaciones, sino que permite que el Gobierno aún tenga una supervisión del sistema para poder detectar el fraude, al conocer y validar las identidades de los intervinientes (Yang, 2019). Sin embargo, no se debe perder de vista que la sola implementación de *blockchain* no eliminará la corrupción de las licitaciones, más bien, esta es una herramienta que coadyuvará a que esta se reduzca. No obstante, se deberá tener cuidado sobre los validadores de transacciones, o incentivos y penalidades para mitigar las conductas maliciosas o la colusión, con la finalidad de preservar la integridad del *blockchain*. Así, se deberá adoptar mecanismos que prevengan que se filtre información sensible, servicios de baja calidad, colusión, entre otros.

Una de las herramientas que se complementan con el *blockchain* son los *smart contracts*. Su beneficio de implementación es que estos son ejecutados precisamente como se han programado, lo cual reduce cualquier tipo de interferencia o fraude, al momento de realizar las transacciones. Por otro lado, estos contratos ofrecen la posibilidad de proporcionar certeza y transparencia en las transacciones que se realicen. De igual manera, en el caso que sea implementado el *blockchain* en el sector público, para cada servicio determinado, se puede desarrollar *smart contracts* que programen los flujos de trabajo y los eventos que gatillarán una determinada acción.

Asimismo, Williams-Elegbe (2019) indica que en contratos tradicionales las partes necesitan tener confianza en que la contraparte actuará sobre la base de los términos y condiciones del contrato que han acordado. Así, muchas veces los contratos cuentan con diversas cláusulas que mitigan el riesgo de incumplimiento contractual, ante el cual se gatillan diversas penalidades. Sin embargo, en el caso de los *smart contracts* no es necesario este elemento de confianza en la contraparte para que esta cumpla con sus obligaciones. Pues, al estar definido por códigos y ejecutados por los mismos de manera automática, se restringe casi en su totalidad la posibilidad de los incumplimientos.

Igualmente, indica que los *smart contracts* se encuentran presentes en una variedad de áreas y que estos, a diferencia de los contratos tradicionales, cuentan con características como las siguientes: (i) la confianza (al ser verificado y autenticado por el *blockchain*, no hay necesidad que se confíe en gran medida en la contraparte); (ii) autonomía (no se necesita de una tercera parte para comprobar la integridad de las transacciones); y (iii) descentralización (al no existir un servidor centralizado y estar distribuidos alrededor del sistema). De esta manera, considera que esto reduce la cantidad de abogados que se necesitan para realizar una transacción; y, al ser ejecutada automáticamente, este no necesita una supervisión excesiva.

IV. CASOS DE ESTUDIO

Con la finalidad de poder entender a cabalidad cómo es que la tecnología *blockchain* se ha implementado en diversas áreas para la contratación de servicios y productos por parte de los gobiernos, presentamos tres casos de estudio.

A. General Services Administration – Estados Unidos[4]

En los últimos años, ha habido esfuerzos por distintos países e instituciones por implementar el *blockchain* en distintas áreas de la economía. Por ejemplo, en Estados Unidos, la General Services Administration (en adelante, GSA) tuvo como propósito implementar esta tecnología para mejorar el tiempo de contratación y modernizar las formas en las cuales hoy en día se contrata. Así, se busca que la implementación del *blockchain* automatice y agilice el proceso de revisión contractual, como por ejemplo las revisiones financieras y el desarrollo de la prenegociación del memorándum para la adjudicación, reduciendo la cantidad de interacción humana que es necesaria para dicha revisión, hasta que se adjudique el contrato. Ello tomando en cuenta que, hacia el año 2017, el GSA otorgaba acceso a más de veinticinco millones de productos y servicios a las autoridades locales, federales y estatales. En ese sentido, utilizar *blockchain* ayudaría a optimizar los procedimientos de contratación; y, proporcionar a las entidades las herramientas necesarias para reducir los ciclos de adquisición, asegurar el cumplimiento y obtener el mejor valor posible para la innovación tecnológica.

Asimismo, para la GSA implementar *blockchain* implica que todos los miembros del sistema puedan tener una mayor visibilidad sobre el proceso de evaluación de las propuestas recibidas, así los oferentes tienen acceso a la información de la situación de su oferta. De igual manera, se ha señalado que el *blockchain* en este caso también permitiría el uso de *smart contracts* y *softwares* que se ejecuten automáticamente. A través de ello, se automatizaría el proceso, que permitan que el personal se centre en tareas más complejas. Así, utilizar esta tecnología, permitiría que las transacciones que se realicen sean supervisadas de una forma más transparente, contribuyendo a que el proveedor pueda seguir un proceso neutral.

Igualmente, se tenía previsto que esta implementación pueda automatizar las revisiones financieras y el cronograma de los procesos. Por ejemplo, se consideró que automáticamente se aprueben las propuestas que excedan las ratios financieras del North American Industry Classification System, y aquellos que sean inferiores podrían ser revisados por un analista financiero. Otro ejemplo era automatizar la creación de un documento para la prenegociación de una propuesta. También, se desea que en la estructura se incluya información contractual como los términos y condiciones, metadata, responsabilidades y la identidad de los proveedores de servicios o productos. En ese sentido, se contempla que incorporar esta tecnología a los procesos de *Fast Lane* de GSA los haría más eficientes, en términos de costos de transacción y tiempo, aumentando el valor para las agencias del Gobierno y reduciendo la carga a los distintos agentes.

B. México[5]

Por otro lado, encontramos el caso de México, en donde, en conjunto con el Coordinador Nacional de Estrategia Digital, el Gobierno de Jalisco, IBM México, la Universidad de Guadalajara y C-Minds, se realizó el proyecto HACKMX. Este proyecto tenía como principales objetivos la creación y desarrollo del *blockchain* y su aplicación práctica. Así, el *proof of concept solution* fue utilizar *blockchain* en las siguientes fases de las licitaciones: (i) la solicitud de un producto determinado, ello considerando que las licitaciones son centralizadas para favorecer la demanda y negociación de condiciones; (ii) dirigir la solicitud a un especialista; (iii) asignar al especialista de la licitación, considerando las reglas del determinado producto o servicio que ha sido solicitado; y (iv) publicar la notificación del contrato. La idea central era implementar *blockchain* en procesos de licitación para crear un proceso confiable, que posea inmutabilidad, transparencia y que sea trazable.

[4] Véase U.S. General Services Administration (2017) y Deloitte (2018).

[5] Véase Deloitte (2018).

Asimismo, del piloto que se implementó para este proyecto, se lograron notar ciertos aspectos relevantes, como (i) la importancia de colaboración intersectorial, sobre todo en la utilización de tecnología que permita una comunicación más fácil, rápida y menos costosa, para reemplazar la necesidad de dividir roles y tareas entre las organizaciones; (ii) promover el entrenamiento para el uso de tecnologías dentro del sector público; (iii) la importancia de crear experimentos para mejorar el valor agregado que se puede esperar del uso de nuevas tecnologías y prevenir riesgos antes que el uso de los sistemas aumente; y, (iv) la necesidad de enfocarse en la experiencia del usuario y evitar digitalizar procesos administrativos que son ineficientes.

La implementación del proyecto se realizó en tres fases:

a) Diseño del sistema: la Secretaría de Planeación, Administración y Finanzas identificó los puntos de interacción del sistema de compras y diseñó un modelo que permite identificar los roles, permisos y las funcionalidades que se integraría en los *smart contracts*. Igualmente, una vez determinados los agentes y activos que participarán en la licitación, se generarán reglas comerciales que determinan qué roles tienen permisos para determinadas acciones y en qué parte del ciclo de vida del activo, permitiendo almacenar la información y las transacciones en el *blockchain*. Esto garantiza que cada nodo de la red mantenga un registro de transacciones actualizado, reduciendo así las oportunidades de fraude, gracias a la inmutabilidad de la red.

b) Interconexión de sistemas: procurando integrar la solución al sistema de contratación del Gobierno de Jalisco. En ese sentido, se generó una *Application Programming Interface* para facilitar la integración entre el sistema de compras, para permitir la comunicación apenas estas se realicen en el sistema de compras al *smart contract*.

c) Almacenar el sistema en la nube: esto abarca la totalidad de los componentes de *blockchain*, incluyendo el *smart contract* y los datos de las transacciones realizadas. Asimismo, este sistema contiene toda la infraestructura y *software* necesarias para operar el *blockchain*.

Para México, este proyecto confirmó la eficacia de *blockchain* como medio para mejorar el proceso de contratación pública y fomentar un gasto más eficiente. A su vez, proporcionó la posibilidad de escalar el proyecto, y, en líneas generales, para el uso de esta tecnología en la administración pública. De esta manera, los aprendizajes de este piloto servirán a este país y en general a los demás, a alentar, informar y fortalecer la implementación de nuevas tecnologías para mejorar la gestión pública en México.

C. Japón[6]

El Ministerio de Asuntos Internos y Comunicaciones evaluó la posibilidad de implementar *blockchain* para sistematizar y almacenar los documentos presentados por las empresas para su calificación y los resultados de los procedimientos de calificación anteriores. Este proyecto incluía una solución de publicación de datos y proporcionando garantías que los mismos no han sido manipulados.

El proceso de calificación y licitación se da de la siguiente manera: (i) oferta de los proveedores para su calificación, para lo cual presentan su aplicación acompañada de la información requerida; (ii) la autoridad evalúa y califica las ofertas, esto se hace basado en la capacidad del proveedor de implementar los contratos; (iii) la autoridad publica la notificación de los proveedores que han sido calificados para que oferten en la licitación; (iv) los proveedores realizan ofertas para la licitación; y (v) la autoridad evalúa las ofertas realizadas, las cuales son observadas sobre la base del precio mínimo y una evaluación técnica de ser necesaria.

Una vez que se implemente el *blockchain*, el proceso de calificación y licitación sería el siguiente: (i) la empresa presentará su aplicación de calificación con la documentación necesaria; y, (ii) la autoridad califica y revisa la documentación y aplicación para lo cual concede o deniega la calificación, almacenando la data en el *blockchain*. En caso desee la empresa aplicar a una calificación de otra autoridad, se seguirían los siguientes pasos: (i) la empresa postula a su calificación; (ii) la autoridad revisa en el *blockchain* la documentación y calificación previa de la empresa; (iii) el *blockchain* indica la información almacenada en la solución de información publicada; y (iv) la autoridad utiliza la data en el *blockchain* para su calificación actual.

Asimismo, cabe precisar que la utilidad de *blockchain* para la solución de información publicada es que esta permite tener evidencia de que la información fue publicada en un momento determi-

[6] Véase Deloitte (2018).

nado y que no ha sido alterada o manipulada. Por otro lado, luego de que se realizó el piloto se identificó que la potencialidad de *blockchain*, al menos para algunos casos, sería muy alta para implementarse en el sector público. A su vez, se consideró que *blockchain* no sería necesariamente la mejor herramienta para almacenar una vasta cantidad de información, lo cual también se relacionaría con la inmutabilidad que esta posee.

V. IMPLEMENTACIÓN DE LA TECNOLOGÍA *BLOCKCHAIN* EN LAS LICITACIONES PÚBLICAS A CARGO DE PROINVERSIÓN

Normalmente existen determinados principios que dictan las políticas anticorrupción (OCDE, 2016). En ese sentido, se expondrá sus aplicaciones respecto del *blockchain*:

a) Integridad: debe garantizarse la integridad, valores y moralidad de los funcionarios. Implementar *blockchain* contribuiría a que los involucrados en los procedimientos de licitaciones públicas estén expuestos al escrutinio público y, de esta manera, dirigir su buen comportamiento.

b) Transparencia: debido a que las transacciones realizadas a través del *blockchain* son totalmente públicas, los miembros de la red podrán verificarlas en cualquier momento.

c) Participación de actores interesados: la transparencia de *blockchain* facilita el control de actores interesados, así como también el escrutinio público de la ciudadanía en general.

d) Accesibilidad: la implementación de *blockchain* y *smart contracts* contribuiría a garantizar igualdad entre competidores.

e) *E-procurement*: la aplicación de tecnologías como el *blockchain*, en conjunto con los *smart contracts*, contribuyen no solo a la lucha contra la corrupción en el ámbito materia de análisis, sino también a hacer del procedimiento más eficiente y automatizado.

f) Supervisión y control: la inmutabilidad y trazabilidad de la información ingresada en el *blockchain* permite realizar un seguimiento de los actos y documentación presentada en el procedimiento de licitación pública.

Ahora bien, la implementación de la tecnología *blockchain* debe incluirse a través de las etapas más vulnerables a actos de corrupción, es decir, las fases de Transacción y Ejecución Contractual, lo cual debe hacerse en conjunto a la programación de *smart contracts*.

El mecanismo de consenso elegido será *proof of authority*, puesto que permitiría a la entidad pública tener control del procedimiento a su cargo. Este mecanismo no solo otorga el beneficio de mantener el control, sino que también permite procesar más transacciones en un menor tiempo comparativamente a otros métodos de consenso, así como también consume menos energía. Esto ocurre por la menor cantidad de nodos que participan en la formación de los bloques (Aarvik, 2020). Los nodos podrían consistir en los actores que resalta el artículo 41 del DL 1362, y son los siguientes: el Organismo Promotor de la Inversión Privada (en adelante, OPIP), la entidad pública titular del proyecto, el organismo regulador, el Ministerio de Economía y Finanzas, y la Contraloría General de la República.

En cuanto al procedimiento en conjunto con *blockchain* y *smart contracts*, ocurriría de la siguiente forma, considerando lo establecido por el DL 1362 y su reglamento:

a) El OPIP lanzará al mercado el proyecto de licitación como un *smart contract* a través del *blockchain*. De esta forma, se estipularán los criterios de evaluación y la documentación que debe ser presentada para constatar la calidad de los postores, así como también la versión inicial del contrato de APP.

b) Existirá un plazo de comentarios, consultas y recomendaciones que los postores podrán realizar. El plazo aplicable habrá sido programado en el s*mart contract* del paso a). De ser pertinente, el OPIP incorporará las recomendaciones. Asimismo, de encontrarse cambios de último minuto, la programación del s*mart contract* arrojará una alerta, por la posibilidad de algún cambio inesperado o no acordado.

c) Las opiniones emitidas por parte de las entidades mencionadas en el artículo 41 del DL 1362 respecto del proyecto de contrato, habiendo incluido los comentarios de los postores de ser pertinente, deberán ingresarse como transacciones dentro del *blockchain*.

d) Se publicará la versión final del contrato y las bases. Los nodos del *proof of authority* evaluarán si es que la versión final efectivamente sigue la línea de las recomendaciones de los postores y, más importante, de las opiniones favorables de las entidades involucradas. De lo contrario, la programación del *smart contract* arrojará una alerta. En

caso se apruebe la transacción, consistente en la versión final del contrato, este será un *smart contract* que dictará los plazos en el procedimiento.

e) Empezará el plazo de presentación de propuestas (artículo 56 del reglamento). Con la finalidad de evitar la colusión entre los ofertantes, cada uno podrá ingresar sus ofertas encriptadas dentro del plazo programado en el *smart contract* y a través de usuarios anónimos u ocultos que solo estarán disponibles durante este plazo.

f) Según el tiempo programado en el *smart contract*, se cerrará el plazo de presentación de propuestas y ninguna otra será aceptada por el sistema.

g) El *blockchain* verificará las ofertas con los requisitos estipulados en las bases a través de los mecanismos de consenso, es este caso, *proof of authority*. El *smart contract* descartará las que no cumplan con los criterios y filtrará las que sí lo hacen.

h) Se otorgarán puntajes, ya sea de manera automática o manual a cada oferta, de lo cual saldrá el ganador del procedimiento. En este paso, el sistema sumará los puntajes y recomendará a un ganador; si es que la entidad decide diferir de la decisión, deberá estipular un motivo. Los puntajes, evaluaciones y decisión del ganador serán publicados para el escrutinio público.

i) Se deberá programar un período en el *smart contract* en caso se interponga un recurso de impugnación contra la adjudicación de la buena pro.

j) Una vez que exista un ganador definitivo, podrán programarse las fechas de cumplimiento de las prestaciones y las consiguientes fechas de pago en el *smart contract*.

Si bien se ha expuesto sobre la implementación del *blockchain* en este tipo de procedimientos, cabe cuestionarse: ¿es suficiente esta tecnología para resolver el problema de corrupción? La respuesta debe ser negativa, pues las nuevas tecnologías consisten en medios para un fin; para que aquellas puedan ser verdaderamente aprovechadas, deben estar acompañadas de políticas paralelas que contribuyan a la lucha contra la corrupción.

Se ha establecido que las características particulares del *blockchain* pueden contribuir a reducir las oportunidades de corrupción que existen en los procedimientos de concesiones y, por lo tanto, reafirmar los beneficios que este tipo de procedimientos puede otorgar. Sin embargo, la sola implementación de la tecnología no es suficiente para resolver de manera automática los altos índices de corrupción, lo cual no quiere decir que su implementación no sea necesaria o beneficiosa. Al contrario, con la finalidad de explotar las características del *blockchain* al máximo y garantizar su correcto funcionamiento, deben implementarse políticas paralelas. La transición e implementación de nuevas tecnologías no constituye tarea fácil, por lo que deben establecerse medidas que las complementen. En ese sentido, el World Economic Forum (2020) recomienda algunas, como las siguientes:

a) Establecer licitaciones competitivas como el proceso de contratación por defecto: puede verse reflejado en facilitar el acceso a más participantes a través de hacer de los procedimientos menos burocráticos y fomentar la participación de las medianas y pequeñas empresas , si bien no en proyectos a nivel nacional, sí en niveles regionales. Asimismo, limitar el número de contrataciones directas.

b) Estandarización de los avisos, las licitaciones, las ofertas y los contratos: de esta forma, los posibles competidores sabrán qué esperar del procedimiento, tendrán incentivos y mayor preparación para involucrarse. Asimismo, la estandarización reduce las posibilidades de discreción y, por lo tanto, este tipo de políticas ataca el problema de las contrataciones dirigidas.

c) Facilitar el escrutinio ciudadano o actores interesados: debido a que el objetivo de usar el mecanismo de consenso *proof of authority* es que la entidad mantenga control del procedimiento, el proceso de monitoreo debe ser cerrado. En esta modalidad, se invita a terceras partes especialistas, que se mantendrán anónimas, a participar del procedimiento y observar si existe alguna alerta o comportamiento irregular. Debe garantizarse a los participantes la libertad de expresión, así como también a los postores en el procedimiento de que existen condiciones equitativas para los competidores.

VI. PRINCIPALES RETOS DE LA IMPLEMENTACIÓN

Si bien el *blockchain* es una herramienta altamente versátil que es de gran ayuda en distintos sectores, es necesario reconocer que cuenta con retos

de implementación, entre los cuales podemos encontrar los siguientes (Berryhil *et al*., 2018):

a) La inmutabilidad es uno de los rasgos principales de *blockchain*; sin embargo, esta funcionalidad del sistema también cuenta con un aspecto negativo. A diferencia de otras plataformas o bases de datos que se utilizan en el sector público, es casi imposible eliminar información de *blockchain*. Por lo cual, en caso sea necesario que se remueva información constantemente, el *blockchain* no será la alternativa más viable. No obstante lo anterior, este reto de implementación no cuenta con mayor asidero para la aplicación de *blockchain* en licitaciones públicas de ProInversión, pues precisamente se quiere evitar que la información sea cambiada constantemente, previniendo que aparezcan fenómenos similares a las famosas adendas.

b) Asimismo, el *blockchain* no es el sistema de almacenamiento idóneo para registrar una vasta cantidad de información, tomando en cuenta que lo que se registra en esta plataforma es una lista de transacciones y operaciones para que estas sean ejecutadas posteriormente, por ejemplo, a través de *smart contracts*. Sin embargo, en caso sea necesario realizarlo, se puede almacenar en un servidor fuera de *blockchain* y conectarlo a una transacción validada.

c) Igualmente, un reto a considerar es al momento de diseñar y programar la estructura del *blockchain*, las reglas a elegirse, niveles de toma de decisiones, cómo se integrarán las decisiones en la plataforma, los desarrolladores de códigos, personas que asumirán roles esenciales, entre otros.

d) También, uno de los retos principales que afronta *blockchain* es el poco conocimiento que tiene la ciudadanía en general en cómo funciona, sus beneficios, sus características y las múltiples utilidades que posee, entre otros. En vista de que es una tecnología compleja, es necesario que las autoridades conozcan a profundidad cómo es que sus beneficios pueden reducir los costos de transacción, o que posean asesores que posibiliten su comprensión.

e) De igual manera, se considera que los costos de corto plazo para una tecnología que es 'relativamente' nueva, pueden ser un limitante para que esta sea implementada a cabalidad. En ese sentido, al momento de considerar integrar esta tecnología a algún sector, sobre todo al público, se debe realizar un análisis costo-beneficio, con la finalidad que ayude a discernir si es válida la inversión que esta implica.

VII. CONCLUSIÓN

En síntesis, se ha demostrado que las licitaciones públicas suponen uno de los ámbitos más vulnerables a la corrupción. De esta manera, respecto de las cinco fases correspondientes a las APPs, dos significan los mayores riesgos: Transacción y Ejecución Contractual, pues incorporan al privado. Si bien existen medidas implementadas para reducir la corrupción en este ámbito, no ha sido posible materializarlas en acciones concreta, por lo que la alternativa de *blockchain* surge como una vía desde el punto de vista del *e-procurement*.

Es así como la inmutabilidad de las operaciones, descentralización, transparencia y la política de consenso del *blockchain* se posicionan como una alternativa viable para reducir la corrupción en las licitaciones públicas. Ello debido a que, al utilizarse el modelo de *proof of authority*, se otorga menor discrecionalidad a los actores, sin impedir que sean las entidades correspondientes aquellas que supervisen y dirijan el proceso. De esta manera, se limita la posibilidad de fraude, pues la única alternativa que esto se dé es a través del 'ataque del 51%'. En ese sentido, resulta vital que se analice la estructura que adoptará el *blockchain*, sus reglas, validadores, programación, entre otros.

Asimismo, ha podido observarse que las características propias del *blockchain* permiten cumplir con los principios que generalmente se emplean para la preparación de políticas anticorrupción. Sin embargo, si bien se ha expuesto que la implementación de dicha tecnología es factible, la sola puesta en marcha no es suficiente ni supone una solución automática al problema de la corrupción. Por este motivo, es necesario acompañar al *blockchain* de políticas paralelas que garanticen los procedimientos competitivos; la estandarización de los requisitos, términos de referencia, avisos o contratos y la participación de los actores interesados, como las organizaciones del sector privado, los consumidores finales, medios de comunicación, entre otros.

Finalmente, de implementarse el *blockchain* en las licitaciones públicas de ProInversión, se deberá tomar en cuenta los retos de poner en práctica esta herramienta, principalmente el escaso conocimiento que se tiene en el sector público o privado sobre esta tecnología. Es fundamental que los agentes intervinientes entiendan cuáles son las funcionalidades que otorga esta plataforma, sus beneficios, y también sus riesgos. También, se

deberá tomar en cuenta que es necesario realizar un análisis costo-beneficio de implementación, hallando las reglas y programación necesarias para poder optimizar el potencial que esta herramienta puede otorgar para reducir la corrupción y agilizar las licitaciones públicas de ProInversión.

REFERENCIAS

Aarvik, P. (2020). Blockchain as an anticorruption tool: Case examples and introduction to the technology. *U4 Anti-Corruption Resource Centre*, 2020, (7), 1-33.

American Council for Technology - Industry Advisory Council (2017). *Enabling Blockchain innovation in the U.S. Federal Government*. https://www.actiac.org/system/files/ACT-IAC%20ENABLING%20BLOCKCHAIN%20INNOVATION_3.pdf

Berryhill, J., Bourgery, T., & Hanson, A. (2018). Blockchains Unchained: Blockchain Technology and its Use in the Public Sector. *OECD Working Papers on Public Governance,* (28). https://doi.org/10.1787/3c32c429-en.

Data Foundation (2019). *Bringing Blockchain Into Government, a path forward for creating effective federal Blockchain initiatives*.

Deloitte (2018). *Blockchain in Public Sector: Transforming government services through exponential technologies.* https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-ps-blockchain-noexp.pdf

Gálvez Córdova, V. (20 de enero de 2017). Así se infiltra la corrupción en las concesiones de APP. *El Comercio*. https://elcomercio.pe/economia/peru/infiltra-corrupcion-concesiones-app-232651-noticia/?ref=ecr

Ministerio Público (s.f.). Carpetas Fiscales. https://www.mpfn.gob.pe/equipo_especial/carpetas_fiscales/

O'Neill de la Fuente, C. (2008). De las priv%&$# iones a las asociaciones público privadas. *Ius et Veritas*, (37), 60-85.

Organización para la Cooperación y el Desarrollo Económicos [OCDE] (2016). *Preventing Corruption in Public Procurement.* https://www.oecd.org/gov/ethics/Corruption-Public-Procurement-Brochure.pdf

Public-Private Analytic Exchange Program (2018). *Blockchain and Suitability for Government Applications*. https://www.dhs.gov/sites default/files/publications/2018_AEP_Blockchain_and_Suitability_for_Government_Applications.pdf

Rodríguez Garagorri, M. (2017). *Análisis de tecnologías Bitcoin y Blockchain* [Trabajo de Fin de Máster, Universitat Oberta de Catalunya]. Archivo de la Universitat Oberta de Catalunya. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72606/6/mrgaragorriTFM-1217memoria.pdf

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing *Blockchain* Consensus and Security Mechanisms against the 51% Attack. *Applied sciences*, *9*(9), 1788. https://doi.org/10.3390/app9091788

Schapper, P. R. (2007). *Corruption and Technology in Public Procurement*.

Transparencia Internacional (2013). *Integrity Pacts in Public Procurement: An Implementation Guide.* https://images.transparencycdn.org/images/2013_IntegrityPactGuide_EN.pdf

(2020). Índice de Percepción de la Corrupción 2019. https://images.transparencycdn.org/images/2019_CPI_Report_ES.pdf

U.S. General Services Administration. (2017). *GSA's Making it Easier to do Business with the Government.* https://www.gsa.gov/cdnstatic/making_it_easier_october16_final.pdf

Williams-Elegbe, S. (2019). Public procurement, corruption and Blockchain technology in South Africa: A preliminary legal inquiry. En G. Quinot & S. Williams-Elegbe (eds.), *Public Procurement Regulation in Africa: Development in Uncertain Times.* LexisNexis.

World Economic Forum (2020). *Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption.* http://www3.weforum.org/docs/WEF_Blockchain_Government_Transparency_Report.pdf

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview. *National Institute of Standards and Technology (NIST) Internal Report- 8202* (pp. 1-59). https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf

Yang, C. (2019). Is there a role for Blockchain for enhancing public procurement integrity? *2019 OECD Global Anticorruption & Integrity Forum*.

https://www.oecd.org/corruption/integrity-forum/academic-papers/Chan-Yang-blockchain-public-procurement-integrity.pdf

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Decreto Legislativo 1362, Decreto Legislativo que regula la promoción de la inversión privada mediante asociaciones público privadas y proyectos en activos, Diario Oficial *El Peruano*, 23 de julio de 2018 (Perú).

Decreto Supremo 240-2018-EF, Reglamento del Decreto Legislativo Nº 1362, Decreto Legislativo que regula la promoción de la inversión privada mediante asociaciones público privadas y proyectos en activos, Diario Oficial *El Peruano*, 30 de octubre de 2018 (Perú).

Resolución de Secretaría General 058-2020 de la Agencia de Promoción de la Inversión Privada, Plan de integridad y lucha contra la corrupción 2019-2021 de ProInversión modificado, del 21 de julio de 2020 (Perú).

RODRIGO,
ELIAS
& MEDRANO
ABOGADOS

10.18800/themis.202101.009

LA RED DORSAL Y LOS 'COSTOS JURÍDICOS' DE MANTENER UN PROYECTO QUE YA NO ES VIABLE

THE DORSAL NETWORK AND THE 'LEGAL COSTS' OF MAINTAINING A PROJECT THAT IS NO LONGER VIABLE

María del Rosario Quiroga*
Rodrigo, Elías & Medrano

Luis Fernando Roca**
Exmiembro del Consejo Directivo de THĒMIS
Rodrigo, Elías & Medrano

It is not difficult to identify the monetary costs derived from the execution of a major infrastructure project. That is why, when these projects fail to produce the expected results, they are labeled as 'white elephants': due to their high costs and low benefits. However, cost analysis tends to ignore the serious impact that a project can have on the legal system, especially when it involves a legal framework that is not fully coherent with other law principles and may enable authorities to perform arbitrary actions.

The authors propose this to be the case of Peru's National Dorsal Fiber Optic Network. More than five years after its implementation, the project cannot meet the market's needs and has led to the issuance of contradictory and arbitrary decisions. This situation has affected some constitutional principles, such as legal predictability, a cost that must be considered when implementing future projects.

Keywords: Broadband; infrastructure; legal certainty; rule of law.

Es fácil identificar el costo en dinero que implica para el Estado ejecutar un gran proyecto de infraestructura. Por eso, cuando estos proyectos no traen los beneficios esperados, se les califica de 'elefantes blancos', porque implican un alto costo sin brindar mayores beneficios. Sin embargo, este análisis de suele obviar la grave afectación en el ordenamiento jurídico que puede causar un gran proyecto de infraestructura, especialmente si ha implicado la emisión de un marco normativo que no es plenamente coherente con otros principios jurídicos y ha derivado en un actuar de las autoridades que podría ser calificado como arbitrario.

Para los autores, este último sería el caso de la Red Dorsal Nacional de Fibra Óptica. A más de cinco años de su licitación, dicho proyecto no solo ha demostrado que no responde a las necesidades del mercado, sino que también ha dado lugar a decisiones contradictorias y arbitrarias. Esto ha vulnerado diversos principios constitucionales, como la seguridad jurídica, cuyo impacto también debe considerarse al evaluar el impacto de futuros proyectos.

Palabras clave: Banda ancha; infraestructura; seguridad jurídica; Estado de derecho.

* Abogada. Consejera del Despacho Regulatorio del Estudio Rodrigo, Elías & Medrano Abogados (Lima, Perú). Contacto: rquiroga@estudiorodrigo.com.

** Abogado. Asociado del Despacho Regulatorio del Estudio Rodrigo, Elías & Medrano Abogados (Lima, Perú). Contacto: lroca@estudiorodrigo.com.

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 30 de enero de 2021, y aceptado por el mismo el 10 de agosto de 2021.

I. INTRODUCCIÓN

En los últimos meses, el Congreso peruano ha acaparado titulares por la emisión de una serie de medidas que contravienen principios económicos y jurídicos básicos de nuestra economía social de mercado[1]. Este tipo de medidas, tan comunes en nuestra región, parecen impulsadas por el afán populista de algunos congresistas. Sin embargo, incluso proyectos de largo plazo, beneficiosos para el país y debidamente planificados, pueden incurrir en vicios similares cuando sus resultados no son los previstos y, a pesar de ello, las autoridades insisten en seguir impulsándolos, aunque eso signifique dejar de lado los principios de nuestra Constitución y las bases del Estado de derecho.

Este último parece ser el caso de la Red Dorsal Nacional de Fibra Óptica (en adelante, RDNFO), proyecto que tuvo el loable objetivo de promover el desarrollo igualitario del país, conectando Lima y todas las capitales de provincia del Perú a través de una red de fibra óptica de más de 13,000 kilómetros.

La implementación de la RDNFO requirió la formulación de un complejo marco regulatorio y una inversión de más de US$300 millones[2], cuyo riesgo es compartido por el concesionario y el Estado peruano, bajo un modelo cofinanciado.

Lamentablemente, una serie de circunstancias no previstas al elaborar el proyecto determinaron su fracaso en los términos que explicaremos más adelante. Esto no solo ha implicado un costo económico para todos los peruanos, quienes seguimos financiando el proyecto, pues lo más grave es que, con el objeto de mantener la RDNFO –cuya concesión, hoy en día, el Estado ha resuelto mediante Resolución Ministerial 689-2021-MTC/01 (2021), por motivos de interés público– se han forzado instituciones jurídicas con decisiones de cuestionable sustento, que debilitan la seguridad jurídica en nuestro país.

En el presente artículo nos proponemos analizar una cuestión que suele ser ignorada por los informes económicos, pues es difícil de medir: el impacto de tales decisiones en nuestro sistema jurídico e instituciones, es decir, el 'costo jurídico' de la RDNFO. Para ello, primero repasaremos las principales características del marco normativo aplicable a la RDNFO, incluyendo las disposiciones que se han ido incorporando a este; luego, describiremos el costo económico que ha generado, según ha sido identificado por diversas instituciones que han evaluado el proyecto; y, finalmente, analizaremos las decisiones administrativas que se han tomado bajo el marco legal de la RDFNO, con énfasis en las múltiples distorsiones que toda esta actuación ha generado.

II. EL DESPLIEGUE DE REDES DE BANDA ANCHA EN EL PERÚ

La Unión Internacional de Telecomunicaciones (en adelante, UIT) define a la 'banda ancha', de modo general, como el conjunto de tecnologías que ofrece capacidad de conexión a internet de forma veloz, sin limitarse a una velocidad determinada ni a un servicio específico[3]. Entre las tecnologías que puedan aplicarse a la prestación de servicios de banda ancha se encuentran las redes de área local inalámbrica (WLAN), los módems de cable, las líneas de abonado digital (ADSL) y los cables de fibra óptica, que usan láseres para transmitir impulsos de luz a lo largo de fibras muy finas de silicona. Como la luz usa frecuencias más altas que las señales eléctricas o radioeléctricas, los cables de fibra óptica pueden transportar muchos más datos que otros medios de comunicación[4].

La legislación peruana, en línea con la UIT, tampoco ha limitado el significado de 'banda ancha' a una velocidad o tecnología[5]. De hecho, dicho término se encuentra definido en el artículo 4 de la Ley 29904 de la siguiente manera:

> La conectividad de transmisión de datos principalmente a Internet, en forma permanente y de alta velocidad, que le permite al usuario estar siempre en línea, a velocidades apropiadas para la obtención y emisión interactiva de información multimedia, y para el acceso y utilización adecuada de diversos servicios y aplicaciones de voz, datos y contenidos audiovisuales (2012).

---

1 Nos referimos a la Ley 31018, que suspende el cobro de peajes durante el estado de emergencia por el brote de COVID-19 (declarada inconstitucional por el Tribunal Constitucional mediante sentencia recaída en el Expediente 00006-2020-PI/TC, 2020) y la Ley 31083, que establece la devolución de los aportes administrados por la Oficina de Normalización Previsional (cuya constitucionalidad se encuentra en debate en el Tribunal Constitucional).

2 Ver Agencia de Promoción de la Inversión Privada [ProInversión] (s.f).

3 Ver Unión Internacional de Telecomunicaciones (s.f.).

4 Ver Unión Internacional de Telecomunicaciones (s.f.).

5 Sin perjuicio de que el Ministerio se encuentra facultado a fijar la velocidad mínima para el acceso a internet de banda ancha.

La velocidad y capacidad de transmisión de los servicios de banda ancha en general, y de las redes de fibra óptica en especial, produce una serie de ventajas frente a otras tecnologías. Particularmente, la banda ancha favorece la prestación de servicios de telecomunicaciones en convergencia, permitiendo que una sola red sirva para la prestación de múltiples aplicaciones –voz, video y datos– con el acceso a internet como componente central (Comisión Multisectorial Temporal, 2011, p. 17). Esto ha generado que la banda ancha forme parte de los planes de desarrollo económico de los Estados, ya que puede producir un impacto positivo en su productividad (Pacheco, 2012, p. 16).

El Perú no ha sido ajeno a esta tendencia y, mediante Decreto Supremo 034-2010-MTC (2010), aprobó como Política Nacional la implementación de una red dorsal de fibra óptica para facilitar a la población el acceso a internet de banda ancha. En la misma línea y como medida para facilitar el acceso a internet y promover la competencia en la provisión de servicios de banda ancha, el Plan Nacional para el Desarrollo de la Banda Ancha en el Perú recomendó la creación de una red dorsal nacional de fibra óptica que pueda soportar altos niveles de tráfico (Comisión Multisectorial Temporal, 2011, p. 165).

Considerando las recomendaciones planteadas en el Plan Nacional para el Desarrollo de la Banda Ancha en el Perú, el 20 de julio del 2012 se promulgó la Ley 29904, Ley de Promoción de la Banda Ancha y construcción de la Red Dorsal Nacional de Fibra Óptica (en adelante, Ley de Banda Ancha).

Es importante tener en cuenta que, a la fecha de publicación de la Ley de Banda Ancha, se habían desplegado solo alrededor de 8,900 kilómetros de fibra óptica en el Perú, limitados principalmente a la costa del país. Además, el número de conexiones de banda ancha por cada 100 habitantes (teledensidad) era bajo (4.39%), pero venía creciendo sostenidamente. Los motivos de esta baja penetración fueron identificados en el Plan Nacional para el Desarrollo de la Banda Ancha en el Perú, que destacó la necesidad de incentivar la inversión en el despliegue de redes y generar sinergias con prestadores de otros servicios (hidrocarburos, electricidad, carreteras) para facilitar dicho despliegue, entre varias otras medidas (Pacheco, 2012, pp. 19-20).

Considerando dicho objetivo, la Ley de Banda Ancha y su Reglamento[6], vigentes hasta el día de hoy, establecieron el marco normativo general aplicable al despliegue de redes de banda ancha, en el cual se dispuso, entre otros, lo siguiente:

a) Se declaró de necesidad pública y de interés nacional la construcción de la RDNFO, la cual conectaría las capitales de provincia del país. También, se dispuso la implementación de redes regionales, que conectarían las capitales de distrito (Ley 29904, 2012, arts. 3 & 7).

b) Se estableció que el Estado será el titular propietario de la RDNFO (Ley 29904, 2012, art. 8).

c) Se facultó al Ministerio de Transportes y Comunicaciones (en adelante, el Ministerio) a establecer las condiciones técnicas, económicas y legales para el diseño y la construcción de la RDNFO, pudiendo entregarla en concesión (Ley 29904, 2012, arts. 7 & 8).

d) Se definió al operador de la RDNFO como un "operador neutro"; esto es, que proporciona servicios portadores a otros operadores y no tiene usuarios finales (Ley 29904, 2012, art. 9.2).

e) Se estableció que las tarifas de los servicios prestados mediante la operación de la RDNFO sean, en la medida de lo posible, iguales a nivel nacional (Ley 29904, 2012, art. 9.3).

f) Se reservó un porcentaje de la capacidad de la RDNFO para la implementación de una red nacional de banda ancha estatal (REDNACE), que se utilizaría para el "desarrollo de la sociedad de la información y el conocimiento" (Ley 29904, 2012, arts. 17 & 18).

g) Se dispuso el acceso y uso obligatorio de los proveedores de servicios de banda ancha a la infraestructura de servicios públicos de energía eléctrica e hidrocarburos. En caso de falta de acuerdo en los términos y condiciones de dicho acceso, se faculta al Organismo Supervisor de Inversión Privada en Telecomunicaciones (en adelante, Osiptel) a emitir un mandato de compartición (Ley 29904, 2012, art. 13; Decreto Supremo 014-2013-MTC, 2013, art. 25).

h) Se estableció una metodología para determinar la contraprestación por el acceso y uso de la infraestructura de los concesionarios de servicios públicos de energía eléctrica e

[6] Aprobado mediante Decreto Supremo 014-2013-MTC (2013).

hidrocarburos (Decreto Supremo 014-2013-MTC, 2013, art. 25, Anexo 1).

Definido el marco normativo, en mayo de 2013, la Agencia de Promoción de la Inversión Privada (en adelante, ProInversión) convocó al Concurso de Proyectos Integrales para la entrega en concesión de la RDNFO, del cual resultó adjudicataria Azteca Comunicaciones S.A.C. (en adelante, Azteca). El 17 de junio de 2014, la empresa y el Ministerio suscribieron el Contrato de Concesión para la construcción y operación de la RDNFO (Resolución Ministerial 343-2014-MTC/03, 2014), que dispuso, entre otras, las siguientes condiciones:

(i) Estableció el cobro de una tarifa única a nivel nacional por la prestación de servicios portadores, prohibiéndose a Azteca efectuar descuentos de cualquier tipo a dicha tarifa (cláusula 40 del Contrato de Concesión).

(ii) Se acordó el cofinanciamiento estatal de la RDFNO. Así, en caso los ingresos de Azteca por la operación de la RDNFO no cubran el monto de la Retribución por Inversión (RPI) o de la Retribución por Operación y Mantenimiento (RPMO) ofertados por la concesionaria, el Estado estaría obligado a asumir la diferencia (cláusula 30 del Contrato de Concesión).

Como puede verse, la implementación de la RDNFO no fue sencilla; todo lo contrario, requirió de la emisión de un amplio y detallado marco legal y contractual, que tuvo por objeto otorgar el soporte normativo para un proyecto de conectividad viable y competitivo que facilite el acceso a internet de banda ancha a todos los rincones del Perú. Ese objetivo, sin embargo, no se ha logrado.

Desde que empezó a operar en el 2016, la RDNFO ha tenido más problemas que logros. Ello ha resultado en que este proyecto resulte económicamente inviable, motivo por el cual, a la fecha, el Ministerio ha terminado el Contrato de Concesión de Azteca por razones de interés público[7]. Esto no ha impedido, sin embargo, que, durante la ejecución del Contrato, se hayan ejecutado una serie de actos bastante cuestionables que, como describiremos a continuación, no solo tienen un impacto económico negativo, sino que afectan la seguridad jurídica y otras instituciones en las que se funda el Estado de derecho.

III. LA RED DORSAL: ¿UN ELEFANTE BLANCO?

En la actualidad, se afirma que la RDNFO es un 'elefante blanco'[8], es decir, un proyecto costoso de mantener y que no aporta mayores beneficios[9]. No se trata, además, de una impresión ligera; el mismo Ministerio y otras entidades, como el Banco Mundial, señalan que la RDNFO no ha cumplido las expectativas que se generaron cuando fue ideada, debido a su alto costo y a que se encuentra infrautilizada (Dirección General de Políticas y Regulación en Comunicaciones, 2019, p. 18).

El primer problema fueron las proyecciones realizadas por el Ministerio, las cuales no se cumplieron debido a una respuesta del mercado que no fue anticipada por el Estado. En efecto, la oferta privada supo atender la demanda por servicios de banda ancha de manera más rápida y eficaz que la RDNFO, dejando a este costoso proyecto con pocos clientes y muy pocos ingresos. Repasemos la historia.

En el 2011, existían pocas iniciativas de banda ancha en el Perú, por lo que se consideró necesario impulsar la oferta de estos servicios para hacer frente a una esperada demanda por el uso de nuevas aplicaciones basadas en internet. En ese momento no se sabía cómo se comportaría la oferta, por lo que no era posible prever si toda la demanda esperada sería atendida (Bando Mundial, 2018, p. 18). Es entonces que se optó por impulsar el desarrollo de la RDNFO.

Los pronósticos del año 2011, respecto al crecimiento de la demanda por servicios de banda ancha, sí se cumplieron. De hecho, según estadísticas publicadas por Osiptel, el tráfico de internet móvil ha mostrado un crecimiento exponencial en los últimos años, multiplicándose veintisiete veces entre inicios de 2014 y fines de 2017. El consumo de *megabytes* promedio por usuario también se ha multiplicado catorce veces en dicho periodo, lo que da muestra de la exponencial evolución de la demanda por contenidos digitales en el Perú (Banco Mundial, 2018, p. 15).

Más aún, el comportamiento de los usuarios en este periodo ha llevado a incrementar la velocidad

7 Ver Resolución Ministerial 689-2021-MTC/01 (2021).

8 Así se han expresado múltiples artículos periodísticos que tratan el tema. Ver Lucas (2018) y DN Consultores (2018a). Las notas de prensa que resaltan el fracaso del modelo han sido muchas.

9 Véase la definición de la expresión 'elefante blanco' consignada por la Real Academia Española de la Lengua: https://dle.rae.es/elefante.

de sus conexiones de internet mediante el uso de tecnologías más avanzadas. La tecnología 3G pasó de ser usada por menos del 10% de los usuarios en 2010 a representar el 44% de las conexiones en el 2018, mientras que la tecnología 4G pasó a representar el 24% de las conexiones, acercándose al nivel de la rezagada tecnología 2G (Banco Mundial, 2018, p. 16).

Sin embargo, por el otro lado, la oferta para la prestación de servicios portadores de banda ancha excedió largamente lo previsto. Entre 2013 y 2020, se pasó de aproximadamente trece mil (13,000) kilómetros a más de cincuenta y ocho mil (58,000) kilómetros de fibra óptica tendida (Dirección de Gestión de Inversiones en Comunicaciones, 2021a, p. 22). Esto se explica principalmente por el crecimiento de la fibra óptica interurbana. Se incorporaron nuevos operadores que pasaron a ser competidores directos de la RDNFO (Banco Mundial, 2018, p. 18).

Los nuevos competidores de la RDFNO, además, son hoy en día quienes se esperaba que fueran clientes de esta: los operadores que brindan servicios de telecomunicaciones a usuarios finales. De hecho, actualmente hay por lo menos tres operadores verticalmente integrados que cuentan con cobertura de fibra óptica a nivel nacional: Telefónica del Perú, América Móvil y Viettel. Estos son los competidores que también lideran el mercado nacional de acceso a internet fijo, lo que debilita en gran medida la demanda potencial por el uso de la RDFNO (Dirección General de Políticas y Regulación en Comunicaciones, 2019, pp. 19-20).

Esta situación competitiva no tiene visos de cambiar. Por el contrario, se espera que los operadores minoristas continúen fortaleciendo su red de banda ancha propia, para así asegurar la autonomía de sus costos ante la creciente demanda del servicio. Así, la tercerización del servicio portador que ofrecería la RDNFO deviene en un recurso marginal, viable únicamente en lugares remotos o para operadores que no cuentan con red propia (Banco Mundial, 2018, p. 18).

Resulta claro, pues, que la oferta de banda ancha hoy es mucho mayor que la proyectada cuando se decidió implementar la RDNFO y puede perfectamente atender la demanda de uso de internet. Por eso, a septiembre de 2020, la RDNFO tenía una capacidad de 17.5 gigabits por segundo (Gbps) arrendada a sus clientes; esto es catorce veces menos de lo estimado originalmente para fines de ese año (More & Argandoña, 2020, p. 16). De hecho, desde 2017, el promedio de utilización de la RDNFO ha sido del 3.27% de la capacidad de la red (Dirección de Gestión de Inversiones en Comunicaciones, 2021a, p. 27). Esta subutilización es la que ha llevado a calificar la RDNFO de 'elefante blanco', y la que nos lleva a cuestionar si era realmente necesario que el Estado asuma el riesgo y cofinancie el despliegue de estas redes a nivel nacional.

Ahora bien, los problemas de la RDNFO no solo responden a una evolución del mercado de banda ancha distinto del previsto al momento de formular el proyecto. Estos también han derivado del marco regulatorio y contractual bajo el cual se ha desarrollado la red que, como explicaremos a continuación, en muchos casos puede constituir una barrera para que esta se adapte a la realidad económica que ha dictado el mercado para poder competir.

Una primera barrera sería la falta de incentivos que tiene Azteca, como operador de la RDNFO, para dinamizar y hacer crecer la operación. El cofinanciamiento estatal asegura los ingresos de la empresa, liberándola de la necesidad de mantener o incrementar su margen de resultados (Banco Mundial, 2018, p. 19) tratando de captar más clientes (Dirección de Gestión de Inversiones en Comunicaciones, 2021a, p. 26). Esto habría dado lugar a que el Estado haya tenido que realizar pagos por retribuciones contractuales a favor de Azteca, por más de US$290 millones entre junio de 2015 y junio de 2021, monto que excede en US$191 millones el cofinanciamiento originalmente proyectado para dicho periodo (Dirección de Gestión de Inversiones en Comunicaciones, 2021b, p. 91). La RDNFO está lejos, pues, de ser autosostenible, al punto que hoy en día sus ingresos cubren únicamente el 7.7% de sus costos (Dirección de Gestión de Inversiones en Comunicaciones, 2021b, p. 90).

La RDNFO, además, se encontraría en desventaja frente a sus competidores en el mercado de servicios de banda ancha, porque está impedida de prestar servicios a usuarios finales, lo que limita el tamaño de su mercado. Además, cuenta con una tarifa fija muy por encima del promedio del mercado (Dirección de Gestión de Inversiones en Comunicaciones, 2021b, p. 89) que le impide responder con ofertas o descuentos para captar clientes.

Finalmente, se ha señalado que la demora en implementar las redes regionales complementarias a la RDFNO, que la conectarían a las capitales distritales, también ha afectado la demanda por su uso. A la fecha, y con ayuda de ProInversión, se ha licitado la construcción de redes de fibra óptica para una gran cantidad de regiones; sin embargo, resulta discutible que esto vaya a revertir la baja demanda por el uso de la RDNFO, pues muchas capitales distritales ya se encuentran servidas por otros operadores y las que no lo están tienen muy

baja demanda (Dirección General de Políticas y Regulación en Comunicaciones, 2019, p. 25).

El impacto de estas distorsiones y barreras en la operatividad y viabilidad de la RDNFO no ha sido menor. Azteca ha declarado públicamente sus problemas económicos y ha negociado con el Ministerio posibles adendas, pidiendo finalmente la caducidad de su Contrato de Concesión[10], lo que le permitiría abandonar el proyecto y trasladar su operación y responsabilidad al Estado peruano.

El Estado, por su parte, ha respondido a la situación modificando diversas disposiciones del Reglamento de la Ley de Banda Ancha para flexibilizar algunas de las barreras legales que restringían su operación. Así, mediante Decreto Supremo 002-2020-MTC, del 24 de enero de 2020, se excluyó a las redes regionales de la RDNFO (evitando, así, que se le apliquen sus restricciones) y se permitió expresamente al operador de la RDNFO prestar ciertos servicios complementarios.

Al no obtener resultados con las medidas planteadas, y como ya fue adelantado, el Ministerio incluso ha terminado unilateralmente el Contrato de Concesión suscrito con Azteca, con el objeto de proteger el interés público subyacente al desarrollo de la RDNFO, pues "la finalidad para la cual se realizó el Contrato de Concesión de la RDNFO no se viene cumpliendo" (Dirección de Gestión de Inversiones en Comunicaciones, 2021a, p. 34); sus objetivos son "inalcanzables" (Dirección de Gestión de Inversiones en Comunicaciones, 2021a, p. 35) y su situación actual "imposibilita la satisfacción del bien público" (Dirección de Gestión de Inversiones en Comunicaciones, 2021b, p. 56). Además, el mismo Ministerio ha determinado que la terminación del contrato es lo menos perjudicial para la caja del Estado, pues le permitiría ahorrar más de US$600 millones (Dirección de Gestión de Inversiones en Comunicaciones, 2021a, p. 56).

A pesar de las idas y venidas del Estado en lo que respecta a la operación de la RDNFO, y a pesar de que, con la terminación contractual, esta pasará a ser operada por un tercero distinto de Azteca, lo cierto es que su estructura básica se mantiene. Esta estructura legal y contractual impide que el operador de la RDNFO compita en el mercado de usuarios finales por los servicios de banda ancha, limitando sus oportunidades de generar ingresos. Además, al haber sido la RDNFO un proyecto cofinanciado por el Estado, sus pérdidas implican un desembolso de dinero estatal, lo que representa un costo económico asumido finalmente por todos los peruanos.

Sin perjuicio de lo anterior, creemos que los costos económicos y competitivos generados por la RDNFO, que hacen de esta un elefante blanco que cuesta mucho y que aporta poco, no constituyen el único problema que dicho proyecto ha causado a nuestro país. Creemos que el impacto que ha tenido el proyecto sobre la seguridad jurídica y predictibilidad del actuar estatal, a pesar de ser difíciles de cuantificar, son tan importantes como los costos económicos mencionados. Este impacto no ha sido analizado en los estudios citados; por ello, consideramos de suma importancia el análisis que expondremos en la siguiente sección.

IV. EL VERDADERO IMPACTO DE LA RED DORSAL

Para identificar el impacto generado por la implementación de la red dorsal en términos de daño a la confianza en las instituciones legales, particularmente en el sector telecomunicaciones, resulta importante analizar cómo se viene aplicando el marco normativo que regula el despliegue de la banda ancha.

Como describiremos a continuación, desde su concepción, el referido marco legal incluyó una serie de disposiciones cuestionables, por ser contrarias a los principios que regulan la libre competencia y la autonomía privada, permitiendo intervenciones innecesarias en el mercado de telecomunicaciones. Peor aún, tales intervenciones implicaron luego una aplicación distorsionada del marco legal, con el objeto de sostener la operación de un proyecto inviable, lo que ha derivado en la vulneración de otros principios jurídicos elementales para el Estado de derecho.

A. La compartición obligatoria de infraestructura en la Ley de Banda Ancha

El marco general aplicable a la prestación de servicios de telecomunicaciones es claro al señalar que tales servicios deben prestarse en condiciones de competencia. Así lo dispone el artículo 6 de la Ley de Telecomunicaciones[11]:

> El Estado fomenta la libre competencia en la prestación de los servicios de telecomunicacio-

[10] El Contrato se puede encontrar en el siguiente enlace: https://cdn.www.gob.pe/uploads/document/file/461868/001_Proyecto_de_Adenda_No._3.pdf.

[11] Cuyo Texto Único Ordenado fue aprobado mediante Decreto Supremo 013-93-TCC.

> nes, regula el mercado de forma que se asegure su normal desenvolvimiento, se controle los efectos de situaciones de monopolio, se evite prácticas y acuerdos restrictivos derivados de la posición dominante de una empresa o empresas en el mercado (Decreto Supremo 013-93-TCC, 1993) .

Esta disposición es concordante con los principios de libre competencia reconocidos en el artículo 61 de la Constitución[12] y es a la luz de estos que se deben evaluar las disposiciones de la Ley de Banda Ancha, norma que, como veremos a continuación, contiene serias incoherencias con dicho marco.

Un ejemplo es la estipulación contenida en el Contrato de Concesión de Azteca, que la obliga a cobrar una tarifa única y le impide competir en el mercado ofreciendo descuentos atractivos (Banco Mundial, 2018, p. 20). Igualmente, la Ley de Banda Ancha es contraria al principio de convergencia (recogido en el artículo 1 de la Ley de Telecomunicaciones)[13], pues prohíbe a Azteca prestar otros servicios de telecomunicaciones (además del portador) sobre la misma red, lo cual también limita la posibilidad de Azteca de competir ofreciendo una variedad de paquetes de servicios y de generar ahorros con el uso de una misma plataforma para todos ellos.

Ahora bien, sin perjuicio de la relevancia de los ejemplos señalados, consideramos que la mayor incoherencia contenida en la Ley de Banda Ancha se encuentra en la disposición que establece que el acceso de los proveedores de banda ancha a la infraestructura de servicios públicos (infraestructura eléctrica y de hidrocarburos) es obligatoria. Incluso el Reglamento de la norma llega más lejos, cuando faculta a Osiptel a emitir mandatos de acceso en caso el proveedor de banda ancha y el titular de la infraestructura no lleguen a un acuerdo para el uso de esta.

Si bien la posibilidad de que Osiptel dicte mandatos de acceso no es nueva, ya que se encontraba regulada desde el 2004 en la Ley 28295, que regula el acceso y uso compartido de infraestructura de uso público para prestar servicios de telecomunicaciones; dicha norma limitaba la emisión de mandatos a supuestos bastante específicos: (i) cuando las autoridades administrativas restringen la construcción o instalación de infraestructura, o (ii) cuando Osiptel establezca que no existen condiciones de competencia para el acceso a determinada infraestructura en algún mercado, luego de realizar el análisis respectivo[14].

Sin embargo, la Ley de Banda Ancha extendió esta obligación de brindar acceso a la infraestructura de uso público, a cualquier supuesto y siempre que lo pidiera un proveedor de banda ancha, salvo que se configure alguna de las causales expresas de negativa establecidas en la norma y referidas a imposibilidades técnicas[15]. En nuestra opinión, a pesar de la buena intención de favorecer el despliegue de banda ancha y aprovechar la infraestructura instalada, esta disposición podría colisionar con los principios de la libre competencia (desincentivando el desarrollo de infraestructura propia o de otros medios de transmisión) por contravenir la doctrina de las facilidades o instalaciones esenciales.

Esta doctrina se aplica cuando una empresa requiere acceder a un recurso propiedad de un tercero, sin el cual no puede competir en el mercado. Verificada esta situación, la doctrina reconoce el derecho de la empresa afectada a acceder a la instalación **esencial** para poder competir (Kresalja & Quintana, 2005, p. 60).

---

[12] Artículo 61 de la Constitución Política del Perú: "El Estado facilita y vigila la libre competencia. Combate toda práctica que la limite y el abuso de posiciones dominantes o monopólicas. Ninguna ley ni concertación puede autorizar ni establecer monopolios […]" (1993).

[13] Artículo 1 de la Ley de Telecomunicaciones:

> El Estado promueve la convergencia de redes y servicios, facilitando la interoperabilidad de diferentes plataformas de red, así como la prestación de diversos servicios y aplicaciones sobre una misma plataforma tecnológica, reconociendo a la convergencia como un elemento fundamental para el desarrollo de la Sociedad de la Información y la integración de las diferentes regiones del país (Decreto Supremo 013-93-TCC, 1993).

[14] Artículo 5 de la Ley 28295:

> Se podrá disponer el uso compartido obligatorio de infraestructura de uso público en caso de presentarse restricción a la construcción y/o instalación de dicha infraestructura de uso público declarada por la autoridad administrativa competente, por cualquiera de las siguientes razones: (a) Medio ambiente; (b) Salud pública; (c) Seguridad; (d) Ordenamiento territorial. Sin perjuicio de estos supuestos, el Organismo Supervisor de la Inversión Privada en Telecomunicaciones - OSIPTEL podrá imponer el acceso compartido de infraestructura en aplicación de lo dispuesto por el Decreto Legislativo Nº 701, sus normas complementarias o por las normas vinculadas a la interconexión de servicios de telecomunicaciones (2004).

[15] Así lo señala la Exposición de Motivos del Reglamento de la Ley de Banda Ancha (Ley 29904, 2012). El artículo 13 de la Ley, por su parte, señala que el "acceso y uso podrá ser denegado cuando existan limitaciones técnicas que pongan en riesgo la continuidad en la prestación de los servicios" (Ley 29904, 2012), norma replicada en el artículo 26 del Reglamento (Decreto Supremo 014-2013-MTC, 2013).

En este contexto, es necesario entender lo que significa la condición de **esencial** que debe cumplir un bien para que le resulte aplicable la doctrina de las facilidades esenciales. Un bien esencial debe ser **irremplazable** para ingresar a un mercado (Kresalja y Quintana, 2005, p. 60) y debe cumplir, cuando menos, con las siguientes características: (i) el bien no debe ser duplicable; (ii) debe tener un exceso de capacidad que puede ser compartido sin generar problemas; y (iii) debe conferir a su propietario el control sobre el mercado de provisión de dicha infraestructura, asemejándose a un monopolio natural (Diez Canseco, 2012, p. 68)[16].

La necesidad de que la infraestructura a la que se accede sea **esencial** se extrae claramente de la Ley 28295 (2004). De hecho, según dicha norma, el acceso obligatorio se limita a infraestructura **necesaria** para prestar servicios de telecomunicaciones, que **no puede ser replicada** (por existir limitaciones legales) y que **sí puede ser compartida por su titular** (de lo contrario, se permite el rechazo, según regula el artículo 20 del Reglamento de la Ley 28295[17]).

Similares disposiciones contienen el Decreto Legislativo 1019, que establece la obligación del acceso a la infraestructura solo para los Proveedores Importantes de Servicios Públicos de Telecomunicaciones (2008), esto es, aquellos que tienen posición de dominio en el mercado o controlan facilidades esenciales.

A diferencia de las normas citadas, la Ley de Banda Ancha, al hacer obligatorio todo acceso a infraestructura eléctrica y de hidrocarburos para el despliegue de redes de banda ancha –salvo por excepciones muy puntuales–, se apartó de la doctrina de las facilidades esenciales, generando una inconsistencia en el marco normativo del sector telecomunicaciones. Pero lo más grave es que esto ha hecho posible el uso abusivo de la figura del mandato de acceso por parte de aquellos operadores que prestan servicios de banda ancha y, sobre todo, por parte de Azteca, operador de la RDNFO.

En efecto, entre los años 2011 y 2017, Osiptel registró[18] la negociación y suscripción de más de treinta (30) contratos de compartición bajo la Ley de Banda Ancha, la gran mayoría de los cuales (21) fue suscrita en el año 2017, cuando la RDNFO empezó a funcionar. En el mismo periodo, según registra Osiptel[19], solo se emitieron diez mandatos. Y es que estos contratos, cuyos términos fueron pactados **libremente** dentro del marco normativo, beneficiaban a ambas partes. No era necesario obligar a las empresas eléctricas a dar acceso a su infraestructura, porque les convenía percibir ingresos de los operadores de telecomunicaciones, a los que también les convenía ahorrar el costo de desplegar nueva infraestructura.

Lamentablemente, para el periodo agregado 2018-2020, la situación cambiaría radicalmente. Para ese entonces, Osiptel tiene registrado en su portal web cuarenta y cuatro mandatos en aplicación de la Ley de Banda Ancha[20]; y casi la mitad de estos han sido emitidos a favor de Azteca[21]. El mismo Osiptel reconoce que, desde 2017, la cantidad de mandatos es mayor a la cantidad de contratos,

---

16 No existe un reconocimiento legislativo expreso de la doctrina de las facilidades esenciales en nuestro país. Sin embargo, el Decreto Legislativo 1034, que aprueba la Ley de Represión de Conductas Anticompetitivas otorga un sustento a la aplicación de la doctrina cuando, en su artículo 10, califica como un abuso de posición de dominio el "negarse injustificadamente a satisfacer demandas de compra o adquisición, o a aceptar ofertas de venta o prestación, de bienes o servicios" (2008). El Reglamento de la Ley 28295 hace referencia a esta disposición normativa cuando, en su artículo 11, señala que, para determinar la obligatoriedad del acceso a infraestructura de uso público, Osiptel debe aplicar "el análisis de mercado relevante, posición de dominio y negativa injustificada de trato" (Decreto Supremo 009-2005-MTC, 2005).

17 Aprobado mediante Decreto Supremo 009-2005-MTC. La norma señala los siguientes supuestos de negativa injustificada de acceso:

1. Cuando existan limitaciones físicas, tecnológicas, técnicas, ambientales o de seguridad en la infraestructura de uso público, para admitir y soportar razonablemente su uso, con el fin de brindar los servicios solicitados.
2. Cuando existan niveles de congestión real o potencial derivados de limitaciones de espacio o tiempo.
3. Cuando existan otros beneficiarios utilizando la infraestructura de uso público y no sea posible incorporar beneficiarios adicionales.
4. Cuando el solicitante haya incumplido anteriores contratos de compartición o mandatos de compartición suscritos con el mismo titular de la infraestructura de uso público o con terceros titulares de infraestructura de uso público.
5. Por aplicación de la excepción dispuesta en el artículo 12 de la Ley.
6. Si el solicitante no otorga los seguros y garantías que el titular de la infraestructura de uso público le hubiere exigido (Decreto Supremo 009-2005-MTC, 2005, art. 20).

18 Ver Osiptel (s.f. a).

19 Ver Osiptel (s.f. b).

20 Ver Osiptel (s.f. b).

21 Ver Osiptel (s.f. b).

siendo la mayoría de tales mandatos[22] requeridos en aplicación de la Ley de Banda Ancha (Informe 00043-2020-DPRC/202, 2020, pp. 16-17).

Como puede verse, el marco legal y contractual que regula la operación de la RDNFO es, en varios puntos, incoherente con los principios que rigen la libre iniciativa, la competencia y el desarrollo de las telecomunicaciones. En particular, la disposición sobre la obligatoriedad del acceso a la infraestructura ha permitido un ejercicio excesivo del derecho a obtener mandatos de compartición por parte de los operadores de telecomunicaciones. La posibilidad de que Osiptel emita mandatos en cualquier supuesto también ha derivado en una serie de intervenciones excesivas, como se describirá a continuación.

B. La repentina reducción, a la tercera parte, de la contraprestación por el acceso a la infraestructura y las contradictorias decisiones de las autoridades

En el contexto antes descrito, Azteca se dirigió a las empresas eléctricas, con las que había suscrito contratos de acceso en el 2015, para solicitarles reducir a la tercera parte la contraprestación mensual que habían acordado en sus respectivos contratos. Según puede apreciarse en distintos expedientes que terminaron en Osiptel[23], Azteca presentó estas solicitudes en el segundo semestre del 2017 y luego argumentó que se habría 'equivocado' al pactar la contraprestación en el 2015, puesto que se basó en una incorrecta interpretación normativa[24] y que, por lo tanto, ahora esta debía dividirse entre tres (3).

Naturalmente, las empresas eléctricas rechazaron el pedido de Azteca, por lo que esta recurrió a Osiptel para que emitiera mandatos en los que estableciera una nueva contraprestación. Es así como, solo en el año 2018, Osiptel dictó veintiún mandatos[25] que no tenían por objeto brindar a Azteca el acceso a la infraestructura eléctrica (Azteca ya había desplegado sus redes sobre dicha infraestructura), sino que simplemente modificaban los acuerdos que habían suscrito libremente las partes y reducían la contraprestación acordada a la tercera parte[26].

Como puede deducirse fácilmente, el motivo que dio lugar a tantos mandatos de acceso desde el 2018 ha sido, básicamente, el valor de la contraprestación. De hecho, las controversias referidas a dicho valor corresponden al 56% de las solicitudes de mandato durante el periodo 2017-2020, llegando al 100% en el año 2020 (Informe 00043-2020-DPRC/202, 2020, p. 17).

Lo que ocurrió fue que Azteca negoció, desde el 2015, diversos contratos con las empresas eléctricas, en los que pactó una contraprestación acorde con el tope máximo establecido en el Anexo 1 del Reglamento de la Ley de Banda Ancha, según lo declaró en los mismos contratos. Más aún, según los actuados en varios expedientes, fue la propia Azteca quien instruyó a las empresas eléctricas sobre la fórmula legal aplicable para calcular la contraprestación. Sin embargo, dos (2) años después de haber venido utilizando las redes eléctricas, Azteca decidió desconocer la fórmula pactada, alegando que se habría equivocado en la interpretación del referido Anexo 1 del Reglamento y que la contraprestación debía ser dividida entre tres (3), para que se ajuste a lo realmente establecido en el marco legal[27].

---

22 El 86% para el periodo 2016-2020, analizado por Osiptel en su Informe 00043-2020-DPRC/2020 (2020).

23 Ver, por ejemplo, los mandatos emitidos con Resolución 045-2018-CD/OSIPTEL; 046-2018-CD/OSIPTEL; y, 062-2018-CD/OSIPTEL, entre varios otros publicados en la web de Osiptel (Osiptel, s.f. b). La aplicación de una 'interpretación equivocada' en la fijación de la contraprestación al suscribir los contratos de compartición dio lugar a reclamos presentados ante los órganos de solución de controversias de Osiptel, que han ordenado la devolución de los montos pagados 'en exceso'. Así, por ejemplo, las Resoluciones del Tribunal de Solución de Controversias de Osiptel 004-2020-TSC/OSIPTEL; 006-2020-TSC/OSIPTEL; 017-2020-TSC/OSIPTEL; y, 026-2020-YTSC/OSIPTEL, entre otras.

24 Azteca ha afirmado que los informes técnicos que sustentaron la emisión de la Resolución Viceministerial 768-2017-MTC/03, habría permitido conocer el auténtico valor de una de las variables (Na) de dicha metodología. Por eso, los precios originalmente pactados con las empresas eléctricas responderían a una incorrecta aplicación de la norma (no a una modificación de esta). Los detalles sobre esta discusión se explican líneas abajo.

25 Ver Osiptel (s.f. b).

26 Ese fue el caso de todos los mandatos emitidos por Osiptel a favor de Azteca y publicados en la web de Osiptel (s.f. b).

27 A modo de ejemplo de lo alegado por Azteca respecto a su 'equivocación' al fijar la contraprestación contractual, nos remitimos al Expediente 00103-2020-0-1817-SP-CO-01, seguido por Azteca contra Transmisora Eléctrica del Sur S.A.C. en el Poder Judicial, y en el cual se discute la validez del laudo emitido en un proceso arbitral seguido por las empresas mencionadas sobre el monto dela contraprestación por el acceso a infraestructura eléctrica. La sentencia que pone fin a dicho expediente (Expediente 00103-2020-0-1817-SP-CO-01, 2020) contiene amplias secciones del laudo arbitral impugnado, en el cual el Tribunal Arbitral resume muy claramente, y del siguiente modo, la postura de Azteca:

> AZTECA, durante el proceso, ha manifestado principalmente que debido a un 'error' la variable 'Na' recibió en el contrato el valor de uno (1) -número de arrendatarios- cuando el valor correcto que debió asignarse desde la firma del contrato era tres (3) (2020, p. 110).

Veamos lo que dispone este marco legal, es decir, el Anexo 1 del Reglamento. Según este anexo, el costo adicional en que incurran las empresas eléctricas por compartir su infraestructura debía ser dividido entre 'Na', que es definido como "número de arrendatarios" (Decreto Supremo 014-2013-MTC, 2013); esto es, el número de empresas que tienen un contrato de arrendamiento con la empresa eléctrica. Así, en el supuesto que solo hubiera una arrendataria (es decir, una sola operadora de telecomunicaciones que estuviera usando la infraestructura eléctrica), entonces 'Na' debía ser igual a uno (1) y la arrendataria única debía asumir todo el costo adicional de mantenimiento en que incurran las empresas eléctricas por compartir su infraestructura.

A pesar de la definición de 'Na' contenida en la fórmula, Azteca planteó que la variable 'Na' no representaba el número de arrendatarios, sino el número **posible** de cables que **eventualmente** podrían arrendar la infraestructura eléctrica; y, como dicha infraestructura generalmente puede soportar hasta tres (3) cables desde un punto de vista técnico, entonces, 'Na' debía ser siempre tres (3)[28]. El sustento de la posición de Azteca fue un informe técnico emitido como sustento para la aprobación de la Resolución Viceministerial 768-2017-MTC/03, en el que se explicaba que la infraestructura eléctrica usualmente podía soportar tres (3) cables de fibra óptica, siguiendo los criterios de peso. Es importante señalar que no hubo una modificación del marco normativo y menos aún del valor del 'Na' que sustentara la nueva posición de Azteca; únicamente se sustentó en un informe del Ministerio que tampoco aludía al valor de 'Na', sino que analizaba el peso de los cables y la capacidad de la infraestructura eléctrica para soportarlos[29].

Siguiendo el novedoso razonamiento de Azteca, el costo adicional en que incurran las empresas eléctricas por compartir su infraestructura tendría que dividirse siempre entre tres (3). Es decir que 'Na' ya no sería una variable que deben completar las partes en función al 'número de arrendatarios' existentes, sino que pasaría a ser un número fijo: tres (3). De esta forma, se reduce a la tercera parte la contraprestación que debía pagar Azteca, simulando que existen otros dos (2) arrendatarios; y, mientras estos no aparezcan, quien tiene que asumir el costo de los arrendatarios inexistente son las empresas eléctricas.

Es importante tomar en cuenta que la insólita pretensión de Azteca fue planteada en la misma época en la que se dieron a conocer públicamente las dificultades económicas que enfrenta la RDNFO[30]; y también las negociaciones que venía sosteniendo Azteca con el Estado peruano para modificar el respectivo Contrato de Concesión (incluyendo su posible caducidad)[31].

También es importante mencionar que uno de los costos operativos más altos que conlleva la RDNFO es el costo de soporte sobre la infraestructura. Esto se identificó desde la etapa del diseño y estructuración de la RDNFO por ProInversión[32]. Por lo tanto, resulta evidente que una reducción, a la tercera parte, de los pagos mensuales que deben realizarse a favor de las empresas eléctricas, reduce significativamente los costos operativos de la RDNFO y podría considerarse determinante para su viabilidad económica.

Es en este contexto que Azteca recurre a Osiptel, quien ampara su posición dictando decenas de mandatos en los que modifica los contratos existentes (supuesto que ni siquiera está previsto o

---

Esta misma hipótesis del 'error' es descartada por dicho Tribunal Arbitral en el mismo laudo citado en la mencionada sentencia:

> […] el Tribunal Arbitral estima que corresponde señalar que cuando las partes suscribieron el Contrato y fijaron el monto de la contraprestación lo hicieron en cumplimiento de la normativa aplicable […] no existió inducción a error, dolo, violencia o vicios de la voluntad de las partes (Expediente 00103-2020-0-1817-SP-CO-01, 2020, p. 116).

28 Azteca y Osiptel llegan a esta conclusión a partir los informes emitidos por el Ministerio en el marco de diversas propuestas normativas vinculadas al Reglamento de la Ley de Banda Ancha, los cuales señalan que técnicamente es posible que la infraestructura eléctrica soporte hasta tres (3) cables. Según Azteca y Osiptel, esto demostraría que el auténtico valor de 'Na' es tres (3), por lo que cada operador de telecomunicaciones solo debe asumir la tercera parte del costo generado por la compartición. Para mayor información sobre el razonamiento de Osiptel, es posible revisar los informes que sustentan las resoluciones citadas en pies de página anteriores.

29 Nos referimos al Informe 292-2017-MTC/26 (2017) que, a criterio de Azteca, 'aclaró' que el valor de la variable 'Na' siempre fue igual a tres (3). Esto a pesar de que la Resolución Viceministerial 768-2017-MTC/03 (2017) no hace referencia alguna al valor de 'Na', y a que dicho informe únicamente contiene una explicación estrictamente técnica que detalla que las infraestructuras eléctricas pueden soportar hasta tres (3) cables de fibra óptica.

30 Las declaraciones vinculadas a las pérdidas económicas de Azteca han sido recogidas en diversos medios de comunicación en los últimos años. Ver, DN Consultores (2018b), América Sistemas (2019) y Larroca (2020).

31 El Ministerio ha presentado una contrapropuesta, pero las partes aún no llegan a un acuerdo.

32 Así lo señala el informe elaborado por Apoyo Consultoría y Kordo S.A. denominado Metodología y Resultados de la demanda del Proyecto Cobertura Universal, incorporado a la sala de datos virtual del proyecto.

permitido por la norma habilitante[33]) o en los que dispone el acceso a nueva infraestructura. En efecto, solo durante el año 2020, el Consejo Directivo de Osiptel ha emitido diez (10) mandatos de compartición de infraestructura[34][35], en los que interpreta el Anexo 1 del Reglamento de la Ley de Banda Ancha de tal modo que reduce a la tercera parte el valor de la contraprestación que debe pagarse a las empresas eléctricas.

Como ya adelantamos, según Azteca y el Consejo Directivo de Osiptel, los costos totales generados por la compartición de infraestructura no deben ser asumidos por los arrendatarios que la utilizan, sino que debe considerarse a los posibles arrendatarios; y, hasta que los mencionados arrendatarios existan, el titular de la infraestructura eléctrica debe asumir el costo por ellos. Es decir que las empresas eléctricas están obligadas legalmente a asumir el costo de reforzar su infraestructura y mantenerla para albergar a varios arrendatarios; y luego deben asumir el riesgo comercial (costo) de que se presenten arrendatarios para usarla.

Los órganos de solución de controversias de Osiptel[36] también han adoptado esta posición. Tanto es así que el último año el Tribunal de Solución de Controversias de Osiptel emitió la Resolución 00026-2020-TSC/OSIPTEL, que aprobó como precedente administrativo de observancia obligatoria la interpretación mencionada, que reduce a la tercera parte la contraprestación por compartir infraestructura (2020).

Pero el cambio de posición que permite reducir a la tercera parte la contraprestación que correspondía pagar a las operadoras de telecomunicaciones se hace más evidente en las opiniones emitidas por el Ministerio, que en el 2013 aprobó el Reglamento de Banda Ancha que regula la mencionada contraprestación.

Las opiniones emitidas por el Ministerio los años siguientes a la aprobación del Reglamento coinciden en que el costo adicional en que incurran las empresas eléctricas por compartir su infraestructura debía ser dividido entre un 'Na' que refleje el número real de arrendatarios que usan dicha infraestructura (no entre los posibles arrendatarios). Como puede comprobarse en los documentos elaborados en el marco de propuestas normativas para modificar el Reglamento de Banda Ancha[37], el Ministerio es claro al señalar que "el costo por el mantenimiento por los cables de FO [fibra óptica] se incrementa de forma marginal ante la existencia de más de un cable", por lo que el costo (en que incurren las empresas eléctricas) "se mantiene" a pesar de la llegada de nuevos arrendatarios (Dirección General de Regulación

[33] El artículo 25 del Reglamento de la Ley de Banda Ancha dispone lo siguiente:

> 25.1 Efectuado el requerimiento para el acceso y uso de infraestructura, el concesionario de energía eléctrica o hidrocarburos respectivo, tiene la obligación de enviar al solicitante el requerimiento de la información necesaria para dar trámite oportuno a la solicitud, dentro del plazo de cinco (5) días hábiles desde la recepción de la solicitud.
>
> 25.2 Presentada la solicitud del Operador de Telecomunicaciones, los concesionarios tendrán un plazo máximo de treinta (30) días hábiles para la negociación y suscripción del contrato de acceso y uso de infraestructura, el cual deberá ser remitido al OSIPTEL en un plazo máximo de cinco (05) días hábiles, contados desde la firma del contrato, para efectos de supervisión.
>
> 25.3 En el caso de falta de acuerdo en el plazo de treinta (30) días hábiles señalado en el numeral precedente, el Operador de Telecomunicaciones podrá solicitar al OSIPTEL la emisión de un mandato de compartición (Decreto Supremo 014-2013-MTC, 2013).

La norma dispone la emisión de mandatos solo cuando no se haya suscrito un contrato; sin embargo, Osiptel ha emitido mandatos modificando cláusulas de contratos ya suscritos.

[34] Nos referimos a las Resoluciones 203-2020-CD/OSIPTEL; 195-2020-CD/OSIPTEL; 157-2020-CD/OSIPTEL; 155-2020-CD/OSIPTEL; 108-2020-CD/OSIPTEL; 086-2020-CD/OSIPTEL; 079-2020-CD/OSIPTEL; 078-2020-CD/OSIPTEL; 076-2020-CD/OSIPTEL; y, 035-2020-CD/OSIPTEL.

[35] Búsqueda realizada en la web de Osiptel el día 25 de enero de 2021.

[36] Cuya función consiste en resolver controversias suscitadas entre operadores de telecomunicaciones o entre estos últimos y tercero, siempre que afecten o puedan afectar al mercado de servicios públicos de telecomunicaciones.

[37] Así, en el marco de la emisión de la Resolución Viceministerial 133-2017-MTC/03 (propuesta de norma para modificar el Reglamento de la Ley de Banda Ancha), Osiptel remitió un comentario señalando que el 'Na' debería ser equivalente al número máximo de arrendatarios a los que es factible dar acceso a la infraestructura; es decir, igual a tres (3) (Informe 292-2017, 2017, p. 8). Este planteamiento fue rechazado por el Ministerio, señalando lo siguiente:

> El costo por el mantenimiento por los cables de FO se incrementa de forma marginal ante la existencia de más de un cable, es decir, las actividades de mantenimiento por un cable deberían ser las mismas que por dos o tres, por tanto, el costo se mantiene. Sin embargo, este pago debería ser compensado en su totalidad desde el primer arrendatario, y posteriormente debería ser retribuido ante la presencia de más de un arrendatario, hecho que se plasma a través de un Na dinámico (Dirección General de Regulación y Asuntos Internacionales de Comunicaciones, 2017, p. 12).

En el mismo sentido ya se había expresado en el Informe 021-2015-MTC, del 29 de enero de 2015, en el que, al comentar otra propuesta de modificación, el Ministerio reconoce el valor dinámico de la variable 'Na' y le asigna un valor igual a uno (1) cuando calcula la contraprestación para solo un arrendatario (p. 9).

y Asuntos Internacionales de Comunicaciones, 2017, p. 12). Así, concluye: "por tanto el costo […] debería ser compensado en su totalidad desde el primer arrendatario, y posteriormente debería ser retribuido ante la presencia de más de un arrendatario, hecho que se plasma a través de un Na dinámico" (Dirección General de Regulación y Asuntos Internacionales de Comunicaciones, 2017, p. 12).

La misma posición se ha reflejado en oficios y comunicaciones posteriores del Ministerio, en las cuales señala lo siguiente: "El valor de "Na" corresponde al número efectivo de arrendatarios […] por ejemplo, si una determinada torre atiende a un único arrendatario, se deberá considerar 'Na = 1'" (Oficio 579-2017-MTC/26, 2017, p. 1).

El Ministerio incluso ha aprobado contratos en los que se consigna una fórmula en la que 'Na' es igual a uno (1), porque solo hay un arrendatario en la infraestructura eléctrica. En efecto, el Programa Nacional de Telecomunicaciones (en adelante, Pronatel), que forma parte del Ministerio, debe aprobar los contratos de compartición que se firmen en el marco de las licitaciones de banda ancha que lleva a cabo ProInversión[38]; y es en ese contexto que aprobó varios contratos donde se expresaba que 'Na' era igual a uno (1) y que el operador de telecomunicaciones pagaría el íntegro del costo adicional en que incurría la empresa eléctrica por compartir su infraestructura[39], hasta que apareciera otro arrendatario.

Cabe mencionar que los contratos de compartición aprobados por Pronatel también fueron remitidos a Osiptel, al igual que todos los contratos que suscribió Azteca y en los que consignó un 'Na' igual a uno (1) (por ser Azteca el único arrendatario). Osiptel nunca cuestionó tales contratos. Sin embargo, años después, determina que son ilegales y dicta mandatos para modificarlos.

El repentino cambio en la posición de las autoridades respecto al valor de la contraprestación máxima regulada en el Reglamento de la Ley de Banda Ancha responde, a nuestro parecer, a una interpretación equivocada de la normativa[40]. Sin embargo, tan grave como este cambio de parecer son las acciones que ha realizado Osiptel para desconocer la vía arbitral pactada y para evitar los cuestionamientos de sus decisiones en sede judicial, afectando así la tutela jurisdiccional efectiva.

C. La afectación al debido proceso y el derecho a la tutela jurisdiccional efectiva

Osiptel viene sosteniendo que los mandatos de compartición que emite son actos de carácter reglamentario y no actos administrativos, por lo que no existiría una vía judicial para cuestionarlos[41].

---

38 Desde 2014, PRONATEL ha encargado a ProInversión la licitación de la implementación de diversos proyectos de Instalación de Banda Ancha para la Conectividad Integral y Desarrollo social para varias regiones (Lambayeque, Tumbes, Piura, Cajamarca, Cusco, Huancavelica, Ayacucho, Apurímac, Lima, Arequipa, Ica, Huánuco, La Libertad, entre otros). Los concursos han dado lugar a la suscripción de Contratos de Financiamiento entre PRONATEL y los adjudicatarios, por los cuales estos últimos se obligan a, entre otros, a sujetar a la aprobación de PRONATEL los contratos de compartición que suscriban.

39 Nos referimos a los contratos suscritos por Gilat Networks Perú S.A. con: (i) Electrodunas S.A.A., de fecha 13 de mayo de 2016; y (ii) Empresa de Generación Eléctrica Machupicchu S.A., del 27 de junio de 2016, publicados en la página web de Osiptel.

40 Además de no existir sustento para cambiar la 'interpretación' que siempre se dio a la norma, los motivos por los cuales consideramos que no es correcta la posición de Azteca y Osiptel sobre el valor de 'Na' son variados. Desde un punto de vista legal, la norma define el valor 'Na' como 'número de arrendatarios'; es decir, aquellos que han suscrito un contrato de arrendamiento con una concesionaria eléctrica (un arrendatario es únicamente quien ha obtenido el derecho de usar temporalmente un bien por cierta renta convenida, conforme al artículo 1666 del Código Civil de 1984 que define el "arrendamiento" como el acto mediante el cual "el arrendador se obliga a ceder temporalmente al arrendatario el uso de un bien por cierta renta convenida"). No tiene sustento legal, pues, interpretar que la norma se refiere a aquellos que "potencialmente" pueden sostenerse de la infraestructura eléctrica.

La posición de Azteca también es contraria a principios económicos y lógicos elementales. Como se explicó, la fórmula busca repartir entre 'Na' el costo incremental de operación y mantenimiento en el cual debe incurrir el concesionario eléctrico como consecuencia de compartir su infraestructura. Así, la variable 'Na' sirve para que la empresa eléctrica pueda repartir este el costo adicional en el que incurre (representado por 'OMs x f'), entre el número de arrendatarios ('Na') que se encuentren soportados en su infraestructura, lo cual es consistente con la definición expresa de 'Na' contenida en la normativa. Por eso, la variable 'Na' debe ser igual al número real de arrendatarios, y no tiene sentido que equivalga siempre a tres (3) aun cuando haya menos de tres arrendatarios.

Estos argumentos han sido analizados en diversos casos arbitrales cuyos tribunales han emitido laudos contrarios a la interpretación esgrimida por Azteca (y Osiptel). Tales laudos incluso han obtenido confirmación judicial (por ejemplo, la Primera Sala Civil de la Corte Superior de Justicia de Lima confirmó la validez de un laudo emitido contra Azteca a favor de Transmisora Eléctrica del Sur S.A.C. Ver expediente 00103-2020-0-1817-SP-CO-01).

41 Si bien los actos reglamentarios teóricamente pueden cuestionarse mediante una acción popular, lo cierto es que un requisito para que dicha acción proceda es que se trate de actos normativos de carácter general.

Esta posición no solo se ha expresado en diversas resoluciones emitidas por el Consejo Directivo de Osiptel[42], sino en diversas excepciones de incompetencia planteadas por el regulador ante el Poder Judicial.

Sobre este punto, cabe mencionar que los mandatos de interconexión no cumplen con las características que exige la doctrina para que un acto sea normativo. En efecto, los mandatos no son actos impersonales (pues regulan una relación que solo involucra a dos partes); tampoco son normas cuya aplicación trasciende un caso en concreto, pues sus efectos se limitan a una relación de compartición en particular; y, no se incorporan al ordenamiento, pues supuestamente se limitan a aplicar normas preexistentes a un caso particular (Morelli & Roca, 2020, pp. 117-118).

La posición de Osiptel, que impide la presentación de acciones contencioso-administrativas contra sus mandatos, limita el derecho al debido proceso reconocido en el artículo 139 de la Constitución[43]. Este derecho, aplicable a los procedimientos administrativos como el de emisión de mandato[44], garantiza a toda persona que cualquier acto que incida en la esfera subjetiva de sus derechos debe estar precedido de un procedimiento donde aquella pueda ejercer de manera plena los derechos que componen el derecho al debido proceso, incluyendo la posibilidad de impugnar las decisiones de la administración, bien mediante los mecanismos administrativos o, llegado el caso, a través de la vía judicial[45].

Lo anterior resulta más claro de la lectura del artículo 148 de la Constitución, que dispone que "las resoluciones administrativas que causan estado son susceptibles de impugnación mediante la acción contencioso-administrativa" (Constitución Política del Perú [Const.], 1993); derecho constitucional que no es posible ejercer si Osiptel se opone al cuestionamiento judicial de sus resoluciones de mandato.

En adición a lo anterior, Osiptel pretende sustraer de la jurisdicción arbitral las materias derivadas del cumplimiento del Reglamento de la Ley de Banda Ancha. Esta pretensión se ha visto reflejada en diversas decisiones en las que, tanto el Consejo Directivo como el Tribunal de Solución de Controversias de Osiptel, han optado por desconocer laudos arbitrales que se pronuncian sobre la existencia o no de deudas (ya devengadas) que se habrían generado entre el 2015 y el 2018 como consecuencia de la alegada 'interpretación equivocada' (por parte de Azteca) en la aplicación de la fórmula del Anexo 1 del Reglamento de Banda Ancha.

Asimismo, esta posición ha sido recogida en la reciente publicación para comentarios del Proyecto de norma que establece la Oferta Básica de Compartición (en adelante, proyecto de OBC) aplicable a la infraestructura eléctrica usada para el despliegue de redes de telecomunicaciones (Resolución del Consejo Directivo de Osiptel 00199-2020-CD/OSIPTEL, 2020).

Sin perjuicio de las varias afectaciones a los derechos de los titulares de infraestructura que es posible identificar en el referido proyecto[46], este pretende prohibir el pacto de cláusulas arbitrales que versen sobre el "cumplimiento de las disposiciones normativas para la compartición de Infraestructura previstas en las Leyes 28295, 29904, sus reglamentos y normas relacionadas" (Resolución del Consejo Directivo de Osiptel 00199-2020-CD/OSIPTEL, 2020, art. 8).

Al respecto, es importante considerar que, en principio, Osiptel solo tiene competencia para resolver controversias entre empresas operadoras de servicios de telecomunicaciones. Sin embargo, mediante norma con rango de ley[47], se ha exten-

[42] Por ejemplo, el Informe 00103-GPRC/2020, que da sustento a la Resolución 140-2020-CD/OSIPTEL, señala que el procedimiento para la emisión de un mandato "no es un procedimiento administrativo, sino una norma de carácter particular con efectos generales" (2020).

[43] Cuyo numeral 3 señala que "ninguna persona puede ser desviada de la jurisdicción predeterminada por la ley, ni sometida a procedimiento distinto de los previamente establecidos, ni juzgada por órganos jurisdiccionales de excepción ni por comisiones especiales creadas al efecto, cualquiera sea su denominación" (Constitución Política del Perú, 1993, art. 139).

[44] Sobre el derecho al debido proceso, el Tribunal Constitucional ha señalado que es un derecho cuyo ámbito de irradiación no abarca exclusivamente el campo judicial, sino que se proyecta, con las exigencias de su respeto y protección, sobre todo órgano, público o privado, que ejerza funciones formal o materialmente jurisdiccionales (Expediente 07289-2005-AA/TC, 2006, fundamento 4).

[45] Ver sentencia del Tribunal Constitucional recaída en el expediente 03741-2004-AA/TC (2005).

[46] Que pretende obligar a todos los titulares de infraestructura a suscribir una OBC siempre que una empresa de telecomunicaciones les requiera acceso, ignorando nuevamente la doctrina de las facilidades esenciales.

[47] Nos referimos al artículo 36 de la Ley 27336, que señala lo siguiente: "Son competentes para resolver controversias: (a) En primera instancia: el Cuerpo Colegiado; (b) En segunda instancia: el Tribunal Administrativo, de acuerdo con la legislación aplicable" (2000).

dido excepcionalmente esta competencia para que también pueda resolver controversias que, entre tales empresas y terceros no prestadores de servicios de telecomunicaciones, únicamente cuando aquellas controversias "se plantee[n] como consecuencia de acciones u omisiones que afecten o puedan afectar el mercado de los servicios públicos de telecomunicaciones" (Ley 27336, 2000, art. 36).

En ese sentido, y en tanto no todos los incumplimientos de disposiciones normativas afectan o pueden afectar al mercado de servicios públicos de telecomunicaciones, la inclusión de la disposición de 'no arbitrabilidad' en el proyecto de OBC podría dar lugar a una ilegal exclusión del arbitraje. De hecho, esto ya ocurrió cuando Azteca ha requerido que le devuelvan supuestos pagos en exceso entre el 2015 y 2018 por haberse 'equivocado' al pactar una contraprestación que, según alega, debía dividirse entre tres (3). Esta deuda no afecta el actual pago de la contraprestación (regulado en un mandato), sino que es una obligación patrimonial ya devengada, por lo que no afecta al mercado de servicios públicos de telecomunicaciones; sin embargo, Osiptel ha considerado que es de su competencia (exclusiva) resolver sobre dichas deudas, por lo que desconoce los laudos arbitrales sobre la materia[48].

En nuestra opinión, la decisión de Osiptel de desconocer la jurisdicción arbitral pactada por las partes y de excluir la futura posibilidad de pactarla, también resulta contraria a la Constitución, vulnerando el derecho a la tutela jurisdiccional efectiva[49].

Como puede verse, ciertas incoherencias en el diseño de la RDNFO han sido la puerta de entrada para que se emita una serie de actos y proyectos normativos que han impedido la revisión judicial de las decisiones de Osiptel, desconociendo diversos derechos en el camino. Esto, como describiremos a continuación, ha dañado también la predictibilidad y la confianza en las decisiones de las autoridades, lo cual deriva en un menoscabo de la seguridad jurídica de nuestro sistema.

D. La actuación descrita de las autoridades afecta la seguridad jurídica y el Estado de derecho

Como ya hemos adelantado, un concepto importante para identificar el impacto jurídico de la implementación y mantenimiento de la RDNFO y el marco regulatorio vinculado es el de la **seguridad jurídica**, principio derivado directamente de nuestra Constitución y reconocido en los siguientes términos por el Tribunal Constitucional:

> El principio de la seguridad jurídica forma parte consubstancial del Estado Constitucional de Derecho**. La predictibilidad de las conductas (en especial, las de los poderes públicos) frente a los supuestos previamente determinados por el Derecho, es la garantía que informa a todo el ordenamiento jurídico y que consolida la interdicción de la arbitrariedad.** Tal como estableciera el Tribunal Constitucional español, la seguridad jurídica supone "la expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en aplicación del Derecho" (STCE 36/1991, FJ 5). […].
>
> Así pues, como se ha dicho, **la seguridad jurídica es un principio que transita todo el ordenamiento**, incluyendo, desde luego, a la Norma Fundamental que lo preside. **Su reconocimiento es implícito en nuestra Constitución**, aunque se concretiza con meridiana claridad a través de distintas disposiciones constitucionales […] (Expediente 0016-2002-AI/TC, 2003, fundamentos 4 & 5) [el énfasis es nuestro].

En línea con lo señalado por el Tribunal Constitucional, el principio de seguridad jurídica consiste en "la predictibilidad de las conductas de los poderes públicos frente a los supuestos previamente determinados por el Derecho" (Morón, 2017, p. 125). La doctrina le reconoce, a su vez, una doble proyección del principio de seguridad jurídica (Ugartemendia, 2006, p. 22):

(i) Una dimensión objetiva, que exige a los poderes públicos a que se atengan al cumplimiento del derecho, y de las normas y principios del ordenamiento jurídico; y,

---

Además de las controversias señaladas en el Decreto Supremo 013-93-TCC, Texto Único Ordenado de la Ley de Telecomunicaciones, y en la Ley 26285, Ley que dispone la desmonopolización progresiva de los servicios públicos de telecomunicaciones, Osiptel es competente para conocer de toda controversia que se plantee como consecuencia de acciones u omisiones que afecten o puedan afectar el mercado de los servicios públicos de telecomunicaciones, aunque solo una de las partes tenga la condición de empresa operadora de tales servicios.

48 Al respecto, ver el precedente administrativo de observancia obligatoria mencionado en el literal anterior, que fue aprobado mediante Resolución 00026-2020-TSC/OSIPTEL (2020).

49 El numeral 2 del artículo 139 de la Constitución señala que "ninguna autoridad puede avocarse a causas pendientes ante el órgano jurisdiccional ni interferir en el ejercicio de sus funciones" (1993). Este derecho no se cumpliría si Osiptel se avoca al conocimiento de controversias que han sido sometidas a las partes al fuero arbitral, que tiene carácter jurisdiccional.

(ii) Una dimensión subjetiva que consiste, fundamentalmente, en la posibilidad de los destinatarios de las normas jurídicas de conocer el derecho (Pérez, 2000, p. 29). Pero esto no se limita en el mero conocimiento; más bien, se concreta en el respeto por los poderes públicos de la "expectativa razonablemente fundada del ciudadano en cuál ha de ser la actuación del poder en aplicación del Derecho" (Ugartemendia, 2006, p. 22).

Así, el principio de seguridad jurídica debe funcionar como criterio de obligatorio cumplimiento que las autoridades deben aplicar siempre que **creen y apliquen normas**, considerando que tales normas deben necesariamente ejecutarse en beneficio de sus destinatarios (Ugartemendia, 2006, p. 23); brindándoles seguridad. La exigencia de certeza frente a cambios imprevisibles en el marco regulatorio también ha sido reconocida por el Tribunal Constitucional[50].

El principio de seguridad jurídica tiene diversas manifestaciones en nuestro ordenamiento. Una de ellas, vinculada a la dimensión subjetiva del principio, se resume en el **principio de protección de la confianza legítima**, que consiste en la protección de la "confianza en el actuar normativo que el poder público haya podido generar" (Ugartemendia, 2006, p. 27). Es decir que el derecho cautela no solo la expectativa de que la Administración actúe conforme a lo establecido en la ley, sino que también emita leyes que guarden coherencia con el marco normativo ya existente, proscribiendo cambios que no sean razonablemente previsibles[51].

En nuestro ordenamiento jurídico el reconocimiento legal expreso del principio de seguridad jurídica (además de su referencia implícita en nuestra Constitución) se encuentra recogido en el Título Preliminar de la Ley del Procedimiento Administrativo General:

> Principio de predictibilidad o de confianza legítima: La autoridad administrativa brinda a los administrados o sus representantes información veraz, completa y confiable sobre cada procedimiento a su cargo, de modo tal que, **en todo momento, el administrado pueda tener una comprensión cierta sobre los requisitos, trámites, duración estimada y resultados posibles que se podrían obtener.**
>
> Las actuaciones de la autoridad administrativa son **congruentes con las expectativas legítimas de los administrados razonablemente generadas por la práctica y los antecedentes administrativos**, salvo que por las razones que se expliciten, por escrito, decida apartarse de ellos.
>
> **La autoridad administrativa se somete al ordenamiento jurídico vigente y no puede actuar arbitrariamente**. En tal sentido, la autoridad administrativa no puede variar irrazonable e inmotivadamente la interpretación de las normas aplicables (Decreto Supremo 004-2019-JUS, 2019, Título Preliminar, art. IV, inciso 1.15) [el énfasis es nuestro].

Así, el principio de confianza legítima implica que la actuación de la administración pública debe ajustarse a los cánones de las políticas públicas establecidas, generando el derecho de los administrados a confiar en la estabilidad de una situación jurídica. Este sería el reflejo directo del principio de seguridad jurídica en el derecho administrativo (Morón, 2017, p. 128).

En nuestra opinión, resulta claro que las inconsistencias normativas de la Ley de Banda Ancha y del Contrato de Concesión de la RDFNO con las normas y principios generales que regulan la libre competencia y el sector telecomunicaciones, han afectado la seguridad jurídica en su dimensión objetiva; esto es, han afectado la expectativa legítima de los administrados de que las normas emitidas por las autoridades serán coherentes con el marco normativo precedente.

Consideramos que la vulneración es más clara aun cuando nos referimos al actuar de las autoridades, el cual es inconsistente con pronunciamientos previos y contrario a diversas normas constitucionales; además de que vulnera el principio de subsidiariedad que debe regir la actuación del Estado,

[50] En la sentencia recaída en el Expediente 009-2001-AI/TC:

> A juicio del Tribunal, es lícito que el legislador pueda modificar el sistema normativo. Sin embargo, debe protegerse también la confianza de los ciudadanos frente al cambio brusco, irrazonable o arbitrario de la legislación. Ciertamente, no se garantiza un régimen de derechos adquiridos –con excepción, naturalmente, de los previstos en la Constitución- sino fundamentalmente, el derecho a que no se cambie las reglas de juego abruptamente. En consecuencia, **cuando cambia la legislación, y de por medio se encuentra comprometido el ejercicio de determinados derechos fundamentales, todo cambio sólo podrá ser válido si es que, además, se encuentra conforme con el principio de seguridad jurídica** (2002, fundamento 18) [el énfasis es nuestro].

[51] Es necesario considerar que la obligación de la Administración de ejercer su facultad normativa de forma coherente con el marco jurídico existente no es absoluta, pues ello llevaría a 'petrificar' el derecho e impedir su evolución. Sin embargo, tales innovaciones deben estar debidamente motivadas y ser proporcionales a sus fines.

porque interviene de manera excesiva e innecesaria en el ámbito de las relaciones privadas. Esta actuación contradictoria afecta la seguridad jurídica en su dimensión subjetiva; es decir, en la expectativa de los administrados de que las decisiones o aplicación de las normas efectuadas por las autoridades será conforme a derecho.

En este punto, conviene recordar lo señalado por el Tribunal Constitucional, en el sentido que la seguridad jurídica resulta **consustancial al Estado constitucional de derecho**; es decir, con aquel modelo de Estado sujeto al derecho y que reconoce la fuerza vinculante y normativa de la Constitución (García Cobián, 2013, p. 445). En el Estado constitucional de derecho, los derechos reconocidos en la ley y en la Constitución, incluyendo la seguridad jurídica, se cumplen y se encuentran vigentes.

Y es que la afectación a la seguridad jurídica puede representar un verdadero **costo**. El respeto a los derechos constitucionales en el Estado de derecho otorga a las personas el dominio sobre las variables que influyen en sus actividades económicas, incentivando la inversión y el tráfico económicos; hay pues, una conexión directa entre Estado de derecho y desarrollo económico (Borea, 1999, p. 592). La relación entre institucionalidad estatal, derivada de la seguridad jurídica, y creación de riqueza sería, pues, directamente proporcional (Kresalja & Ochoa, 2016, p. 20), por lo que las medidas estatales que afectan la seguridad jurídica tienen un impacto económico directo, asumido como costo por la sociedad en su conjunto.

En línea con lo anterior, consideramos que la afectación a la seguridad jurídica derivada de la RDFNO ha resultado, como acabamos de explicar, en un costo social que podría cuantificarse y debe tenerse en cuenta al evaluar el impacto del proyecto, más allá del costo económico directo que haya podido generar.

V. A MODO DE CONCLUSIÓN

A lo largo del presente artículo hemos aludido al impacto económico que ha ocasionado al país la decisión de mantener la RDNFO, debido a que es un proyecto muy costoso que no está aportando los beneficios previstos. Sin embargo, el principal objeto del artículo ha sido destacar que el grave impacto que la implementación de la RDNFO ha ocasionado por las decisiones de ciertas autoridades, que no solo insisten en mantener este proyecto, cofinanciándolo con los recursos que aportamos los peruanos, sino que han reducido artificialmente sus costos trasladándolos a otras empresas. De esta manera, han distorsionado el marco legal del sector y han vulnerado la confianza legítima y la seguridad jurídica, además de otros derechos fundamentales para el Estado de derecho, como la tutela jurisdiccional efectiva.

Este impacto, que podría considerarse como un 'costo jurídico' y el consiguiente 'costo social' no ha sido analizado por la gran cantidad de estudios económicos dedicados a evaluar el impacto de la RDNFO. Sin embargo, consideramos que sí deberá tomarse en cuenta al evaluar la implementación de futuros proyectos de infraestructura; y también, por supuesto, al considerar las distintas alternativas con que cuenta el Estado sobre el futuro de la RDFNO, las que incluyen la completa modificación del modelo o incluso la desinversión del proyecto (Banco Mundial, 2019, p. 122). Más allá de las buenas intenciones, necesitamos proyectos sustentables y coherentes con nuestro entorno, que nos dejen un saldo positivo en términos económicos y de respeto a los derechos ciudadanos.

REFERENCIAS

Agencia de Promoción de la Inversión Privada [ProInversión] (s.f.). Red Dorsal Nacional de Fibra Óptica. http://www.proinversion.gob.pe/MODULOS/LAN/landing.aspx?are=0&pfl=1&lan=13&tit=red-dorsal-de-fibra-%C3%B3ptica.

América Sistemas (22 de mayo de 2019). Millonarias pérdidas en la Red Dorsal. *América Sistemas*. https://www.americasistemas.com.pe/millonarias-perdidas-en-la-red-dorsal/

Banco Mundial (2018). *Acuerdo de Cooperación Técnica: Reformas para la Expansión de Servicios de Infraestructura de Banda Ancha a Zonas Remotas y Rurales*. https://portal.mtc.gob.pe/comunicaciones/regulacion_internacional/regulacion/proy%20normativos/2019/Informe_DiagnosticoBancoMundial.pdf

(2019). *Informe 2 – Escenarios y Modelos de Negocios de la RDFNO y redes de Transporte Regionales*. https://cdn.www.gob.pe/uploads/document/file/493980/Informe_2_Banda_Ancha_Banco_Mundial.pdf

Borea, A. (1999). *Derecho y Estado de Derecho* (tomo II). Editorial Gráfica Monterrico.

Comisión Multisectorial Temporal creada mediante Resolución Suprema 063-2010-PCM (2011). *Plan Nacional para el Desarrollo de la Banda Ancha en el Perú*. https://www.Osiptel.gob.pe/media/io0g0vti/plan-nacional-desarrollo-banda-ancha-peru.pdf

DN Consultores (2018a, 8 de enero). Red Dorsal, ¿aún un elefante blanco? *DN Consultores*. http://dnconsultores.com/diarios/impreso/reddorsalaunun-elefanteblanco/

(2018b, 18 de abril). Azteca dejaría el país: ¿qué pasará con la Red Dorsal de Fibra Óptica?. *DN Consultores.* http://dnconsultores.com/diarios/revistas/web-revistas/azteca-dejaria-el-pais-que-pasara-con-la-red-dorsal-de-fibra-optica/

Diez Canseco, L. (2012). Teoría del cuello de botella: Las facilidades esenciales. *THĒMIS-Revista De Derecho*, (61), 65-93.

Dirección de Gestión de Inversiones en Comunicaciones del Ministerio de Transportes y Comunicaciones (2019). *Informe 0946-2019-MTC/26, que sustenta el Proyecto de Decreto Supremo que modifica el Reglamento de la Ley N 29904, aprobado por Decreto Supremo 014-2013-MTC.*

(2021a). *Informe 008-2021-MTC/27.01, que sustenta la caducidad del Contrato de Concesión de la RDNFO.*

(2021b). *Informe 350-2021-MTC/27.01, que sustenta la caducidad del Contrato de Concesión de la RDNFO.*

Dirección General de Políticas y Regulación en Comunicaciones (2019). *Oficio 11902-2019-MTC/26*.

Dirección General de Regulación y Asuntos Internacionales de Comunicaciones (2017). *Matriz de comentarios al Proyecto de Resolución Viceministerial que modifica los valores de las variables "m" y "f" de la "Metodología para la Determinación de las Contraprestaciones por el Acceso y Uso de la Infraestructura de los Concesionarios de Servicios Públicos de Energía Eléctrica e Hidrocarburos", establecida en el Anexo 1 del Reglamento de la Ley N° 29904, "Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica" (Resolución Viceministeral N°133-2017-MTC/01.03, publicada en el Diario Oficial El Peruano el 18 de febrero de 2017)*. Ministerio de Transportes y Comunicaciones.

García Cobián, E. (2013). Control Gubernamental del Gasto Público en el Estado Constitucional: Reflexiones a propósito de la aprobación de las facultades sancionadoras de la Contraloría General en materia de responsabilidad administrativa funcional. *Derecho PUCP*, (71), 443-475. https://doi.org/10.18800/derechopucp.201302.016.

Kresalja, B., & Ochoa, C. (2016). *Derecho Constitucional Económico*. Fondo Editorial de la Pontificia Universidad Católica del Perú.

Kresalja, B., & Quintana, E. (2005). La doctrina de las facilidades esenciales y su recepción en el Perú. *Ius et Veritas*, (31), 59-89.

Larocca, N. (2020). TV Azteca multiplicó por siete sus pérdidas al primer trimestre. *TeleSemana*. https://www.telesemana.com/blog/2020/05/27/tv-azteca-multiplico-por-siete-sus-perdidas-al-primer-trimestre/

Lucas, N. (31 de enero de 2018). La Red Dorsal de Perú debe ser un modelo a evitar en México. *El Economista*. https://www.eleconomista.com.mx/empresas/La-Red-Dorsal-de-Peru-debe-ser-un-modelo-a-evitar-en-Mexico-20180131-0066.html

More, J., & Argandoña, D. (2020). *Las redes de transporte de fibra óptica, microondas y satelital, y su rol para promover la expansión de la cobertura de los servicios públicos de telecomunicaciones: Reporte y mapas de cobertura*. https://repositorio.Osiptel.gob.pe/bitstream/handle/20.500.12630/745/49%20DT%20Reporte%20y%20Mapas%20de%20cobertura%20Redes%20de%20Tx%20Fibra%20_%20MW%20y%20Satelital.pdf?sequence=1&isAllowed=y

Morelli, A., & Roca, L. (2020). La naturaleza jurídica de los mandatos de interconexión de redes de telecomunicaciones y el cambio de posición de OSIPTEL. *Forseti Revista de Derecho*, *8*(11), 108-125.

Morón, J. (2017). *Comentarios a la Ley del Procedimiento Administrativo General* (tomo I). Gaceta Jurídica.

Organismo Supervisor de Inversión Privada en Telecomunicaciones [Osiptel] (s.f. a). Contratos remitidos para supervisión en el marco de la Ley de Banda Ancha N° 29904 y su Reglamento. https://www.osiptel.gob.pe/portal-de-operadoras/contratos/compartici-on-de-infraestructura/contratos-remitidos-para-supervisi%C3%B3n-en-el-marco-de-la-ley-de-banda-ancha-n-29904-y-su-reglamento/

(s.f. b). Mandatos. https://www.osiptel.gob.pe/portal-de-operadoras/mandatos/?anio=2017&subcat=Compartici%C3%B3n+de+infraestructura&input=.

Pacheco, L. (2012). Hacia un mayor desarrollo de la banda ancha en el Perú. *Revista de Derecho Administrativo*, *2*(12), 13-32.

Pérez, A. (2000). La seguridad juídica: una garantía del derecho y la justicia. *Boletín de la Facultad de Derecho de la UNED*, (15), 25-38.

Ugartemendia, J. (2006). El concepto y alcance de la seguridad jurídica en el Derecho constitucional español y en el Derecho comunitario europeo: un estudio comparado. *Cuadernos de Derecho Público*, (28), 17-54.

Unión Internacional de Telecomunicaciones [UIT] (2003). Nacimiento de la banda ancha, preguntas formuladas con frecuencia. https://www.itu.int/osg/spu/publications/birthofbroadband/faq-es.html.

Zegarra, D. (2018). *Introducción al Derecho de las Telecomunicaciones*. Fondo Editorial Pontificia Universidad Católica del Perú.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Código Civil [CC], Diario Oficial *El Peruano*, 25 de julio de 1984 (Perú).

Constitución Política del Perú [Const.] (1993).

Decreto Legislativo 1019, Decreto Legislativo que aprueba la Ley de Acceso a la Infraestructura de los Proveedores Importantes de Servicios Públicos de Telecomunicaciones, Diario Oficial *El Peruano*, 10 de junio de 2008 (Perú).

Decreto Legislativo 1034, Decreto Legislativo que aprueba la Ley de Represión de Conductas Anticompetitivas, Diario Oficial *El Peruano,* 25 de junio de 2008 (Perú).

Decreto Supremo 013-93-TCC, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley de Telecomunicaciones, Diario Oficial *El Peruano*, 6 de mayo de 1993 (Perú).

Decreto Supremo 009-2005-MTC, Decreto Supremo que aprueba el Reglamento de la Ley 28295, que regula el acceso y uso compartido de infraestructura de uso público para la prestación de servicios públicos de telecomunicaciones, Diario Oficial *El Peruano*, 21 de marzo de 2005 (Perú).

Decreto Supremo 034-2010-MTC, Decreto Supremo que establece como política nacional la implementación de una red dorsal de fibra óptica para facilitar a la población el acceso a internet de banda ancha y promover la competencia en la prestación de este servicio, Diario Oficial *El Peruano,* 24 de julio de 2010 (Perú).

Decreto Supremo 014-2013-MTC, Reglamento de la Ley 29904, Ley de Promoción de la Banda Ancha y construcción de la Red Dorsal Nacional de Fibra Óptica, Diario Oficial *El Peruano,* 4 de noviembre de 2013 (Perú).

Decreto Supremo 004-2019-JUS, Texto Único Ordenado de la Ley del Procedimiento Administrativo General, Diario Oficial *El Peruano,* 25 de enero de 2019 (Perú).

Dirección General de Regulación y Asuntos Internacionales de Comunicaciones del Ministerio de Transportes y Comunicaciones, Informe 021-2015-MTC-26, 29 de enero de 2015 (Perú).

Dirección General de Regulación y Asuntos Internacionales de Comunicaciones del Ministerio de Transportes y Comunicaciones, Informe 292-2017-MTC/26, 4 de agosto de 2017 (Perú).

Dirección General de Regulación y Asuntos Internacionales de Comunicaciones del Ministerio de Transportes y Comunicaciones, 8 de septiembre de 2017, Oficio 579-2017-MTC/26 (Perú)

Gerencia de Políticas Regulatorias y Competencia de Osiptel, Informe 00043-2020-DPRC/2020, que sustenta el Proyecto de Norma que aprueba el Proyecto de Norma que aprueba la Oferta Básica de Compartición (OBC) y Otras Disposiciones aplicables a la Infraestructura Eléctrica para el despliegue de redes de telecomunicaciones, 28 de mayo de 2020 (Perú).

Gerencia de Políticas Regulatorias y Competencia de Osiptel, Informe 00103-GPRC/2020, Expediente 00002-2019-CD-GPRC/MC, 1 de octubre de 2020 (Perú).

Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en Servicios Públicos, Diario Oficial *El Peruano,* 29 de julio de 2000 (Perú).

Ley 28295, Ley que regula el acceso y uso compartido de infraestructura de uso público para la prestación de servicios públicos de telecomunicaciones, Diario Oficial *El Peruano,* 21 de julio de 2004 (Perú).

Ley 29904, Ley de Promoción de la Banda Ancha y construcción de la Red Dorsal Nacional de Fi-

bra Óptica, Diario Oficial *El Peruano,* 20 de julio de 2012 (Perú).

Primera Sala Civil Subespecialidad Comercial de la Corte Superior de Justicia de Lima, 17 de noviembre de 2020, Resolución 11, Expediente 00103-2020-0-1817-SP-CO-01 (Perú).

Proyecto de Adenda, Adenda N.3 al contrato de concesión del proyecto "Red Dorsal Nacional de Fibra Óptica: cobertura universal norte, cobertura universal sur y cobertura universal centro". https://cdn.www.gob.pe/uploads/document/file/461868/001_Proyecto_de_Adenda_No._3.pdf

Resolución del Consejo Directivo de Osiptel 00199-2020-CD/OSIPTEL que aprueba la publicación para comentarios del "Proyecto de norma que establece la Oferta Básica de Compartición y otras disposiciones aplicables a la Infraestructura Eléctrica utilizada para el despliegue de redes de telecomunicaciones", Diario Oficial *El Peruano*, 23 de diciembre de 2020 (Perú).

Resolución Ministerial 343-2014-MTC/03, Otorgan a la empresa AZTECA COMUNICACIONES PERÚ S.A.C. concesión única para la prestación de servicios públicos de telecomunicaciones en todo el territorio nacional, Diario Oficial *El Peruano*, 10 de junio de 2014 (Perú).

Resolución Ministerial 689-2021-MTC/01, que Declara la resolución del Contrato de Concesión para el Diseño, Financiamiento, Despliegue, Operación y Mantenimiento del Proyecto "Red Dorsal Nacional de Fibra Óptica: Cobertura Universal Norte, Cobertura Universal Sur y Cobertura Universal Centro", Diario Oficial *El Peruano*, 13 de julio de 2021 (Perú).

Resolución Viceministerial 133-2017-MTC/03 que publica el proyecto de modificación los valores de las variables "m" y "f" de la "Metodología para la Determinación de las Contraprestaciones por el Acceso y Uso de la Infraestructura de los Concesionarios de Servicios Públicos de Energía Eléctrica e Hidrocarburos", establecida en el Anexo 1 del Reglamento de la Ley N° 29904, "Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica". Diario Oficial *El Peruano*, 9 de febrero de 2017 (Perú).

Resolución Viceministerial 768-2017-MTC/03 que modifica los valores de las variables "m" y "f" de la "Metodología para la Determinación de las Contraprestaciones por el Acceso y Uso de la Infraestructura de los Concesionarios de Servicios Públicos de Energía Eléctrica e Hidrocarburos", establecida en el Anexo 1 del Reglamento de la Ley N° 29904, "Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica", aprobado mediante Decreto Supremo 014-2013-MTC. Diario Oficial *El Peruano*, 7 de agosto de 2017 (Perú).

Tribunal Constitucional [T.C.], 29 de enero de 2002, sentencia recaída en el Expediente 009-2001-AI/TC (Perú).

Tribunal Constitucional [T.C.], 30 de abril de 2003, sentencia recaída en el Expediente 0016-2002-AI/TC (Perú).

Tribunal Constitucional [T.C.], 24 de noviembre de 2005, sentencia recaída en el Expediente 03741-2004-AA/TC (Perú).

Tribunal Constitucional [T.C.], 3 de mayo de 2006, sentencia recaída en el Expediente 07289-2005-AA/TC (Perú).

Tribunal de Resolución de Controversias de Osiptel, 4 de diciembre de 2020, Resolución 00026-2020-TSC/OSIPTEL, Expediente 008-2018-CCO-ST/CI (Perú).

10.18800/themis.202101.010

LA COLABORACIÓN DE LAS PLATAFORMAS DIGITALES EN LA APLICACIÓN Y EN LA RECAUDACIÓN DE LOS TRIBUTOS

THE COLLABORATION OF DIGITAL PLATFORMS IN THE APPLICATION AND COLLECTION OF TAXES

Carmen Ruíz Hidalgo*
Universidad de Vigo
Mónica Siota Álvarez**
Universidad de Vigo

The use of digital platforms for the provision of services and sale of goods has increased in recent years, thereby transforming the performance of markets. These transactions have called into question some of the pillars on which taxation has been based, due to the tax obligations generated. At the same time, new opportunities are created to help both tax administrations and taxpayers in the application of the tax system, also facilitating its subsequent control.

Since digital platforms are destined to become important collaborating agents of the tax administration, throughout this article, the authors identify the way in which they affect the application and collection of taxes. First, they address the issue of tax enforcement, reviewing the tasks and obligations of these platforms in this regard. Then, they cover the issue of tax collection and the way in which the platforms collaborate with it.

Keywords: Digital platforms; tax administration; collection; information exchange; assistance and collaboration.

El uso de plataformas digitales para la prestación de servicios y venta de bienes se ha intensificado en los últimos años, transformando el funcionamiento de los mercados. Estas transacciones han puesto en cuestionamiento algunos pilares sobre los que se ha venido asentando la fiscalidad, debido a las obligaciones tributarias generadas. Al mismo tiempo, se crean nuevas oportunidades para ayudar tanto a las administraciones tributarias como a los contribuyentes en la aplicación del sistema tributario, facilitando también su consiguiente control.

Tomando en consideración que las plataformas digitales están llamadas a configurarse como importantes agentes colaboradores de la administración tributaria, a lo largo del presente artículo, las autoras identifican la forma en que inciden en la aplicación y recaudación de tributos. Primero, toman el tema de la aplicación de tributos, repasando las tareas y obligaciones propias de estas plataformas con relación a ello. Luego, abarcan el tema de la recaudación de los mismos y la forma en que las plataformas colaboran con aquello.

Palabras clave: Plataformas digitales; administración tributaria; recaudación; intercambio de información; asistencia y colaboración.

* Profesora Titular de Derecho Financiero y Tributario de la Universidad de Vigo (Pontevedra, España). Contacto: cruiz@uvigo.es

** Profesora Contratada Doctora de Derecho financiero y tributario de la Universidad de Vigo (Pontevedra, España). Contacto: msiota@uvigo.es

Trabajo realizado al amparo del proyecto de investigación desarrollado en la Universidad de Vigo "PID2019-107450GB-C31", sobre "Retos y oportunidades de la administración tributaria", financiado por el Ministerio de Economía y Competitividad de España.

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 12 de enero de 2021, y aceptado por el mismo el 24 de abril de 2021.

I. INTRODUCCIÓN

En el marco de la economía digital han surgido, en los últimos años, nuevos modelos de producción y consumo en los que, a través de plataformas digitales, se transfieren bienes o se prestan servicios, normalmente a cambio de una contraprestación monetaria. La utilización de dichas plataformas es, precisamente, uno de los elementos diferenciadores, novedosos, o disruptivos, de esta nueva economía; ya que la plataforma digital, accesible normalmente a través de un *software* de aplicación móvil (*app*), o a través de una página web, establece una conexión directa entre oferta y demanda, facilita la transacción y el pago, permite la valoración del servicio por los clientes, etc.

No existe, en todo caso, un único modelo o tipo de plataforma digital (Siota Álvarez, 2020, pp. 45-ss.). Así, hay plataformas que actúan en el proceso de provisión de bienes o de prestación de servicios como meras intermediarias digitales, poniendo en contacto a los prestadores/proveedores con los usuarios, como, por ejemplo, Airbnb, BlaBlaCar, Ebay, Wallapop, etc. Otras, en cambio, proporcionan el propio producto o servicio principal, o prestan servicios auxiliares o complementarios a los principales, por ejemplo, Uber, Glovo, Booking, etc. A su vez, las mencionadas plataformas pueden actuar con o sin ánimo de lucro, siendo múltiples los mecanismos de obtención de ingresos en el primer caso: cobro de una comisión o de una tarifa a los usuarios de la plataforma por el mero acceso a la misma, por las labores de intermediación realizadas, o por las entregas de bienes o prestaciones del servicio llevadas a cabo; o bien pueden obtener ingresos, de forma indirecta, a través de la gestión de los datos de los usuarios o bien mediante la venta de espacios de publicidad visibles desde la página web o aplicación.

Desde una perspectiva tributaria, los nuevos modelos de negocio que surgen al amparo de la economía digital –en general– y de la economía colaborativa –en particular–, así como la utilización de las mencionadas plataformas digitales, generan retos y oportunidades tanto para las Administraciones como para los usuarios de las mismas.

Así, uno de los principales desafíos a los que se enfrentan las administraciones tributarias está relacionado con la masificación de transacciones con relevancia fiscal que, en principio, provocarían dificultades de fiscalización y control (Montesinos Oltra, 2016, p. 47). Mientras que los usuarios de este tipo de plataformas digitales tendrían que afrontar problemas vinculados al cumplimiento de las obligaciones fiscales cuando obtienen rentas a través de ellas (Antón Antón, 2019, p. 210).

En contrapartida, debe reconocerse que los nuevos modelos de negocio que se llevan a cabo a través de plataformas digitales presentan ciertas ventajas desde una óptica tributaria. Por una parte, este tipo de transacciones, al aprovecharse de las herramientas tecnológicas que ofrece internet, dejan rastro y proporcionan información sobre las operaciones realizadas (Sánchez Huete, 2017b, p. 122); lo que, unido a las posibilidades que brinda el tratamiento masivo de datos, ofrecen a las administraciones tributarias sistemas de control tributario, hasta el momento, desconocidos e inconcebibles (Rozas Valdés, 2017, p. 143). Además, la función mediadora que desempeñan, en ocasiones, las plataformas digitales en el momento del pago generan grandes oportunidades para un cumplimiento más ágil en la recaudación de las posibles obligaciones tributarias surgidas y para llevar a cabo una fiscalización más efectiva de las mismas por parte de la administración tributaria (Montesinos Oltra, 2016, p. 48).

Por su parte, los usuarios de las plataformas digitales también pueden verse auxiliados o asistidos por dichas plataformas en el cumplimiento de sus obligaciones tributarias, simplificando así el proceso de declaración fiscal, en particular cuando los usuarios no son empresarios o profesionales.

Queda justificado, por tanto, que la colaboración y asistencia de las plataformas digitales puede resultar esencial no solo para facilitar y simplificar la correcta aplicación del sistema tributario, sino también para el correspondiente control del mismo. Asimismo, pueden desempeñar un importante papel colaborando con la Administración en tareas de recaudación tributaria.

II. LA COLABORACIÓN DE LAS PLATAFORMAS DIGITALES EN LA APLICACIÓN DE LOS TRIBUTOS

A. Asistencia y colaboración de las plataformas digitales

Son múltiples y variados los problemas tributarios que generan los nuevos modelos de negocio que han surgido con la economía digital. Ello se debe, fundamentalmente, a que hay que tratar de reconducir las nuevas transacciones a los conceptos y elementos tributarios ya existentes; aunque en muchas ocasiones dicha adecuación no sea posible, obligando al legislador a ofrecer soluciones específicas. En este sentido, se ha reconocido abiertamente que "desde una perspectiva fiscal, la economía colaborativa ha puesto en cuestionamiento algunos pilares y estructuras básicas sobre las que se ha venido asentando nuestra fiscalidad" (Ruiz Garijo, 2018, p. 183).

Sin embargo, y al mismo tiempo, también se ha señalado que los Estados no solo deberían de preocuparse por establecer nuevos tributos –o, en su caso, adaptar los vigentes–, sino que también deberían informar y asistir a los diferentes obligados tributarios que surgen a propósito de esta nueva realidad (Navarro Egea, 2017, p. 525). Así, se han identificado hasta tres tipos de acciones específicas que se han implementado en los Estados miembros para simplificar los costes de cumplimiento de las obligaciones tributarias en el caso de la economía colaborativa[1]: (i) campañas de orientación e información para aclarar las normas aplicables; (ii) introducción de un régimen específico/simplificado para los ingresos generados en el ámbito de la economía colaborativa hasta un umbral; y (iii) la participación voluntaria de las plataformas, ya sea para intercambiar datos fiscales con los contribuyentes y/o la administración pública o para actuar directamente como agentes retenedores de la administración tributaria (Antón Antón, 2019, p. 199).

Por tanto, se impone la necesidad, enmarcada en el genérico deber de proporcionar información y asistencia a los obligados tributarios –que, en el ordenamiento español, reconoce el artículo 85 de la Ley General Tributaria (en adelante, LGT)[2]–, de que las administraciones tributarias ofrezcan información clara sobre las obligaciones tributarias que son exigibles a los distintos agentes implicados, por ejemplo, a través de campañas informativas, o mediante la elaboración de guías específicas, en función del modelo de negocio de que se trate; existiendo distintas iniciativas, al respecto, en el derecho comparado (Antón Antón, 2017, pp. 570-571).

Pero esa misma tarea, junto a otras que faciliten la correcta aplicación de los tributos como proporcionar información con trascendencia tributaria, también puede ser desarrollada por las propias plataformas digitales que realizan una labor de intermediación en prestaciones de servicios o en la venta de bienes. Las especiales circunstancias en que estas desarrollan su actividad (utilizando tecnologías informáticas que permiten un tratamiento masivo de datos y registran las distintas transacciones que se realizan a través de ellas), las hacen especialmente propicias para prestar ayuda y colaboración a los usuarios de las mencionadas plataformas en el cumplimiento de sus obligaciones tributarias. Y ello, al margen de que sería deseable la utilización de ciertas herramientas, por parte de las administraciones tributarias, que simplificasen los costes de cumplimiento tributarios que generan estas tareas también para las propias plataformas: creando ventanillas únicas, desarrollando mecanismos de intercambio de información en línea, etc.

En este sentido, se ha subrayado que las plataformas digitales no deberían desentenderse de las obligaciones tributarias de las partes a las que ponen en contacto (Vega García, 2017, p. 600). De hecho, algunas de ellas, conscientes de la importancia de la fiscalidad, tienen un servicio de asesoría fiscal para sus usuarios.

De todas formas, la colaboración de las plataformas digitales, con el objetivo de facilitar y simplificar la correcta aplicación de los tributos, puede llevarse a cabo tanto con los usuarios de las propias plataformas como con las administraciones tributarias. Así, por ejemplo, y respecto de la posible colaboración de las plataformas proporcionando información con relevancia tributaria, cabrían varias posibilidades: que las plataformas enviasen los datos pertinentes a las autoridades tributarias para que estas comunicasen, en su caso, las obligaciones fiscales a los usuarios de las plataformas; que las plataformas comunicasen directamente los datos a sus usuarios, e informasen a las autoridades tributarias; que las plataformas informasen exclusivamente a los usuarios, etc. (Antón Antón, 2017, p. 572).

Las plataformas digitales, en particular las de intermediación, han sido reconocidas como "sujetos idóneos de colaboración con la Hacienda Pública" (Pastor del Pino, 2019, p. 230), de acuerdo con lo previsto en el artículo 92 de la LGT (Ley 58/2003, 2003). Si bien, se han identificado distintos niveles o ámbitos de colaboración (Pastor del Pino, 2019, p. 231), conforme a ese mismo precepto normativo[3].

1 Al respecto, véase también Pastor del Pino (2019, p. 230).

2 Por su parte, el artículo 34.1. a) de la LGT reconoce el derecho del obligado tributario a "ser informado y asistido por la administración tributaria sobre el ejercicio de sus derechos y el cumplimiento de sus obligaciones tributarias" (Ley 58/2003, 2003).

3 El artículo 92.3 de la LGT dispone que la colaboración social puede referirse, entre otros, a los siguientes aspectos:

(a) realización de estudios o informes relacionados con la elaboración y aplicación de disposiciones generales; (b) campañas de información y difusión; (c) simplificación del cumplimiento de las obligaciones tributarias; (d) asistencia en la realización de autoliquidaciones, declaraciones y comunicaciones y en su correcta cumplimentación; (e) presentación y remisión a la administración tributaria de autoliquidaciones, declaraciones, comunicaciones o cualquier otro documento con trascendencia tributaria, previa autorización de los obligados tributarios; (f) subsanación de defectos, previa autori-

Así, y en primer lugar, las plataformas digitales podrían realizar tareas de simple suministro de información a la población, en general, o a los usuarios o clientes de la propia plataforma, en particular, sobre las obligaciones tributarias derivadas de las prestaciones de servicios o de las entregas de bienes que realizan, conforme a las normativas tributarias vigentes. En este sentido, algunos Estados obligan a las plataformas a informar a sus usuarios sobre sus obligaciones tributarias, incluyendo informes periódicos sobre las transacciones realizadas (Bilbao Estrada, 2018, p. 242).

Un segundo nivel de colaboración se concretaría en labores más directas de asesoramiento y ayuda informal, asistiendo a los usuarios de las plataformas en la cumplimentación de autoliquidaciones, liquidaciones o comunicaciones tributarias; proporcionándoles, por ejemplo, un listado de las transacciones realizadas en su plataforma con inclusión de las contraprestaciones abonadas. También se podrían articular herramientas de simplificación en el cumplimiento de las obligaciones tributarias.

Al respecto, la Comisión Europea en su documento La agenda europea de la economía colaborativa pone, como ejemplo de buena cooperación con plataformas de uso compartido de vehículos, que estas puedan simplificar el proceso de declaración fiscal de los conductores. Para ello, describe lo que sucede en Estonia: las transacciones entre el conductor y el cliente son registradas por la plataforma colaborativa, que después envía solo los datos pertinentes a efectos fiscales a las autoridades que, a continuación, prerellenarán los formularios fiscales del contribuyente. La idea principal es ayudar a los contribuyentes a cumplir sus obligaciones fiscales eficazmente y con el mínimo esfuerzo (Comisión Europea, 2016, p. 15).

En tercer lugar, las plataformas también podrían implicarse más en la correcta aplicación de los tributos llevando a cabo auténticas actuaciones de asistencia o ayuda formal realizando directamente la presentación de las correspondientes autoliquidaciones, liquidaciones o comunicaciones, o desarrollando otras tareas de intermediación entre la administración tributaria y los obligados tributarios, resultado necesario en estos casos el consentimiento expreso de los obligados.

A la hora de hacer efectiva esta labor de asistencia y colaboración por parte de las plataformas digitales, algunos países han preferido emplear la vía de la voluntariedad en lugar de la obligatoriedad, tratando de llegar a acuerdos de cooperación con estas. Aunque la relación cooperativa entre entidades y administraciones tributarias plantea dudas sobre su eficacia, se ha reconocido que la extensión y aplicación de tales planteamientos puede facilitar las tareas de asistencia y colaboración de las plataformas, sin que su ubicación territorial constituya un límite (Sánchez Huete, 2017a, p. 5). Además, siempre se podrían articular algunas medidas para promover la cooperación de plataformas no residentes, como, por ejemplo, la creación de una mención o calificación administrativa que refuerce la reputación de la plataforma colaboradora.

Urge, en todo caso, articular vías para lograr asistencia y colaboración, voluntaria o imperativa, por parte las plataformas digitales respecto de las obligaciones tributarias de sus usuarios. Solo así se podrá avanzar en la simplificación y en el control de la aplicación de los tributos, garantizando la efectividad del deber de contribuir.

En este sentido, el Comité Económico y Social Europeo de la Unión Europea

> espera que las normativas europeas y nacionales contemplen mecanismos para fomentar la cooperación entre los operadores de la economía colaborativa y las autoridades tributarias. Gracias a una utilización amplia de datos fiables y rastreables, esta cooperación podría promover la simplificación y la transparencia fiscal, lo que podría llegar a permitir que, a efectos de estas actividades, las plataformas digitales se convirtieran en 'sustitutos del contribuyente' en colaboración con las autoridades tributarias (Dictamen 2018/C 081/09, 2018, apartado 5.12).

B. Obligaciones de suministro de información con trascendencia tributaria

Aunque las tareas de suministro de información también pueden incardinarse entre las labores de asistencia y colaboración que pueden prestar las plataformas digitales, ya sea a la administración tributaria, ya sea a los usuarios de las plataformas, ya sea a ambos; hemos consideramos oportuno analizar de forma específica las obligaciones de suministro de información con trascendencia tributaria, por la gran relevancia que adquieren en este ámbito.

zación de los obligados tributarios; (g) información del estado de tramitación de las devoluciones y reembolsos, previa autorización de los obligados tributarios; o, (h) solicitud y obtención de certificados tributarios, previa autorización de los obligados tributarios (Ley 58/2003, 2003).

La economía digital, al igual que ocurriera en su día con el comercio electrónico, genera una masificación de actos, hechos o negocios con posible relevancia tributaria que, en principio, provocarían dificultades de control para la administración tributaria (Montesinos Oltra, 2016, p. 47). Pero las ventajas tecnológicas que presentan las plataformas digitales, junto con la función mediadora que desempeñan –en ocasiones, en el momento del pago– ofrecen grandes oportunidades para llevar a cabo una fiscalización más efectiva de las obligaciones tributarias que se generan en su seno (en particular las de los usuarios de dichas plataformas). Además, y frente a épocas pasadas, las administraciones tributarias están evolucionando hacia un crecimiento exponencial en la captación, el análisis y el tratamiento de datos con trascendencia tributaria y, por tanto, en las posibilidades de detección de las rentas derivadas de la economía digital gracias a la irrupción y combinación de distintas tecnologías como, por ejemplo, *software* araña, *big data*, *machine learning*, Internet de las cosas, etc. (Bilbao Estrada, 2018, p. 260). En definitiva, la combinación de información requerida a las plataformas digitales, junto a la que pueda ser obtenida por la Administración a través de nuevas tecnologías, permitirá estrechar el cerco de los usuarios de plataformas digitales que incumplen con sus obligaciones tributarias.

Tradicionalmente, las administraciones tributarias nacionales han obtenido información con trascendencia tributaria relevante, fundamentalmente, mediante el establecimiento de específicos deberes de información tributaria; pero también y, en su caso, a través de requerimientos individualizados de información. Por otra parte, los deberes de proporcionar información pueden establecerse sobre datos propios de los obligados tributarios o sobre datos referenciados, esto es, sobre datos de terceras personas con las que los obligados a proporcionar información se relacionan económicamente.

En nuestra opinión, el establecimiento de específicos deberes de información tributaria, tanto de carácter nacional como supranacional, en virtud de los cuales las plataformas digitales se viesen obligadas a proporcionar información tributaria relevante sobre las actividades económicas desarrolladas por los usuarios de las mismas –sobre todo cuando los usuarios son particulares– tendría un impacto muy positivo en la correcta aplicación de los tributos; y, en última instancia, en el incremento de los ingresos públicos estatales.

Al respecto, la Organización para la Cooperación y el Desarrollo Económicos (en adelante, OCDE), ha señalado que

> dada la disponibilidad y posibilidad de acceso a 'datos masivos' o macrodatos, es necesario intensificar la cooperación internacional entre administraciones tributarias, principalmente en lo concerniente a la información sobre los usuarios de plataformas en línea en su condición de parte integrante de iniciativas como la economía colaborativa y la economía por encargo, con el fin de garantizar el pago de los impuestos devengados por los ingresos percibidos (2018, p. 2).

En todo caso, consideramos que resultaría precipitado instaurar dichos deberes de información si todavía no se ha clarificado la fiscalidad de alguno de los nuevos modelos de negocio que han surgido al amparo de las plataformas digitales.

1. El necesario establecimiento de obligaciones de suministro información de carácter supranacional

En los últimos años, y debido fundamentalmente a la globalización, las administraciones tributarias han ido contando, progresivamente, con nuevos e importantes instrumentos normativos que persiguen garantizar el intercambio y el suministro de información tributaria entre ellas. De ahí que se afirme que uno de los mayores avances de la fiscalidad internacional es el establecimiento de un nuevo estándar de intercambio efectivo de información tributaria entre Estados.

Buen parte de las rentas que se obtienen a través o por plataformas digitales tienen un componente transfronterizo. Con frecuencia los proveedores de bienes/prestadores de servicios que actúan por medio de una plataforma digital pueden operar, gracias a esta, en varios países al mismo tiempo. También es habitual que las plataformas estén situadas en un determinado territorio y los usuarios de las mismas estén radicados en países distintos. Por tanto, si una Administración quisiera obtener información con trascendencia tributaria sobre los usuarios de una plataforma cuando esta es no es residente en el país, o incluso sobre los propios ingresos que esta obtiene en los distintos países donde opera, resulta imprescindible la asistencia mutua entre las distintas administraciones tributarias para conseguir dicha información. Para ello sería necesario recurrir, en principio, a normas de carácter supranacional; aunque no se ha descartado explorar modelos de acuerdo voluntario de colaboración en materia de suministro de información por parte de las plataformas (Antón Antón, 2017, pp. 574-575).

Es claro que se podría apelar, tal y como ha señalado Falcón y Tella (2014, p. 15), a la red de ins-

trumentos internacionales con cláusula de intercambio de información entre administraciones tributarias, previa petición, entre los que destaca la cláusula del artículo 26 del Modelo de Convenio de Doble Imposición de la OCDE (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2010). También se podría recurrir al Convenio sobre Asistencia Administrativa Mutua en Materia Fiscal (OCDE & Consejo de Europa, 2011)[4]. Pero, junto a las limitaciones generales que algunas de estas normas prevén con relación al propio mecanismo de intercambio de información fiscal entre Estados, habría que añadir las dificultades específicas que presenta la obtención de información tributaria relevante en el ámbito de la economía digital. Consideramos, por tanto, que estos instrumentos normativos presentarían problemas para lograr un adecuado intercambio de información tributaria con relación a las plataformas digitales.

Desde la perspectiva de la Unión Europea (en adelante, UE), hay normas específicas que regulan el intercambio de información entre los Estados miembros, tanto en materia de impuestos indirectos como directos. Entre las primeras, habría que mencionar el Reglamento 904/2010 de 7 de octubre de 2010 del Consejo de la Unión Europea, relativo a la cooperación administrativa y la lucha contra el fraude en el ámbito del Impuesto sobre el Valor Añadido (en adelante, IVA). Por lo que respecta a las segundas, el instrumento ordinario de obtención de información entre administraciones tributarias es la Directiva 2011/16/UE, del Consejo de la Unión Europea, de 15 de febrero de 2011, relativa a la cooperación administrativa en el ámbito de la fiscalidad.

Esta última norma, la Directiva 2011/16/UE, también presentaría importantes restricciones a la hora de lograr un apropiado intercambio de información en el ámbito de la economía de plataforma. Concretamente, se ha afirmado que solo el mecanismo de intercambio previa solicitud de los Estados sería potencialmente idóneo para conseguirlo (Pastor del Pino, 2019, p. 219). Sin embargo, creemos que las importantes limitaciones a las que se ve sometido este mecanismo de intercambio de información condicionarían seriamente su eficacia. Así, por ejemplo, no podría solicitarse información de forma genérica sobre los usuarios de las plataformas. Por otra parte, y en virtud del principio de subsidiariedad, por el que solo se puede recabar información de otro Estado miembro, tras agotar las fuentes habituales de información interna en el propio Estado, será difícil identificar dichas fuentes, sobre todo, cuando a nivel interno no se han previsto, con carácter general, específicas obligaciones de suministro periódico de información con relación a las plataformas digitales.

No obstante, se está abordando una importante modificación normativa de esta Directiva, que podría subsanar la mayor parte de dificultades que existen actualmente para lograr un efectivo intercambio de información en el ámbito de las plataformas digitales. Nos referimos a la Propuesta de Directiva del Consejo por la que se modifica la Directiva 2011/16/UE relativa a la cooperación administrativa en el ámbito de la fiscalidad (en adelante, la Propuesta de Directiva), la cual actualmente se está debatiendo en el Consejo de la Unión Europea. La Exposición de Motivos de la Propuesta de Directiva justifica la necesidad de la modificación normativa del siguiente modo:

> [E]n la UE es necesario ampliar la cooperación administrativa a ámbitos nuevos, con el fin de abordar los desafíos que plantea la digitalización de la economía y ayudar a las administraciones tributarias a recaudar los impuestos de una forma mejor y más eficiente y a adaptarse al ritmo de los nuevos acontecimientos. Las características de la economía de las plataformas digitales complican en gran medida la trazabilidad y la detección de los hechos imponibles por parte de las administraciones tributarias. El problema se agrava especialmente cuando estas operaciones se realizan a través de operadores de plataformas digitales establecidos en otra jurisdicción. El hecho de que los vendedores no comuniquen las rentas obtenidas a cambio de la prestación de servicios o la venta de bienes a través de plataformas digitales conlleva un déficit en los ingresos fiscales de los Estados miembros. También otorga una ventaja a esos vendedores en comparación con los que no operan en plataformas digitales. De no abordarse este vacío legislativo, será imposible garantizar la consecución del objetivo de la equidad tributaria (2020).

En caso de que, finalmente, se aprobase esta Propuesta de Directiva con la que, una vez más, se

[4] El Convenio sobre Asistencia Administrativa Mutua en Asuntos Fiscales (*Convention on Mutual Administrative Assistance in Tax Matters*) fue desarrollado conjuntamente por la Organización para la Cooperación y el Desarrollo Económicos (en adelante, OCDE) y el Consejo de Europa en 1988 y enmendada por protocolo en 2010, firmada por 113 jurisdicciones y de la que España es signataria desde el 12 de noviembre de 2009, encontrándose en vigor en nuestro país desde 2013. Para mayor información, véase un listado de los países signatarios del Convenio y de las fechas de entrada en vigor de la misma para tales jurisdicciones en la página web de la OCDE: http://www.oecd.org/tax/exchange-of-tax-information/Status_of_convention.pdf.

trataría de ampliar el ámbito de aplicación de la Directiva 2011/16/UE, se darían grandes pasos a la hora de lograr que las administraciones tributarias de la UE obtuviesen información tributaria sobre las transacciones que se realizan a través de plataformas digitales.

En concreto, la Propuesta de Directiva prevé que tanto los operadores de plataformas digitales de la UE –residentes fiscales en la UE o que operan en la UE a través de un establecimiento permanente– como los operadores no residentes –pero que intermedian en la venta de bienes o en el arrendamiento de inmuebles que se encuentran situados en la UE– tienen la obligación de recopilar una serie de información con relevancia tributaria y comunicarla, de forma automática, a las autoridades competentes de los Estados miembros en los que residan los usuarios registrados en dichas plataformas sobre una serie de transacciones que estos realicen. Las actividades sobre las que se establece esta obligación de suministro de información realizadas con la intermediación de las plataformas son: (i) el arrendamiento de bienes inmuebles; (ii) la prestación de servicios personales; (iii) la venta de bienes; (iv) el arrendamiento de cualquier medio de transporte; y (vi) la inversión y los préstamos en el marco de la financiación participativa.

2. Obligaciones de suministro de información para plataformas digitales en el ordenamiento español

Para que se pueda producir el intercambio de información entre administraciones tributarias a escala global es necesario que las administraciones tributarias nacionales dispongan, de forma sencilla y actualizada, de información tributaria relevante que suministrar. Esto es, en última instancia, la implementación de las obligaciones de intercambio de información a nivel supranacional puede requerir la adopción de normas internas que garanticen el suministro puntual de información.

A su vez, y en función de la estrategia de política tributaria que el país escoja, se abren dos grandes posibilidades: el establecimiento de una obligación genérica de información para todas las plataformas digitales o la creación de obligaciones específicas para determinados ámbitos (por ejemplo, arrendamiento de inmuebles, ventas de bienes usados, etc.).

La necesidad de establecer una obligación informativa específica, que abarque la comunicación de datos tributarios de la propia plataforma y, fundamentalmente, los de los usuarios de la misma, se ha planteado no solo ante la necesidad de obtener información que se pueda transmitir a otros Estados, sino también como medida para evitar el fraude fiscal con carácter general.

Sánchez Huete (2017c) ha sistematizado los argumentos a favor y en contra de crear una nueva obligación informativa en el ordenamiento tributario español para las plataformas digitales de economía colaborativa, concluyendo que ni siquiera un mayor número de obligaciones informativas supone la obtención de una mayor información; ya que sería preciso adecuar su establecimiento a la eficacia que con ellas se obtiene. En concreto, este autor ha señalado que "el establecimiento de una obligación de suministro periódico de informaciones tributarias sobre operaciones masivas, pero de escasa cuantía, podría considerarse desproporcionada, atendiendo a la existencia de obligaciones a cargo del contribuyente y la posibilidad de requerimiento individualizado" (Sánchez Huete, 2017c, p. 26).

Sin embargo, consideramos necesario que se establezcan en nuestro ordenamiento específicas obligaciones informativas con relación a las plataformas digitales, porque tanto el tipo de usuarios de las mismas (en muchas ocasiones, particulares), como la inexistencia de obligaciones de retención, provocarían que la administración tributaria no tuviese información alguna sobre la gran mayoría de transacciones que se llevan a cabo a través de dichas plataformas. Por otra parte, esta información podría utilizarse para simplificar la aplicación de los tributos, permitiendo la incorporación automática de ciertos datos a las declaraciones tributarias de los usuarios de estas plataformas.

A finales del año 2017 se incorporó al ordenamiento tributario español una obligación informativa relativa a los arrendamientos de viviendas con fines turísticos. Así, el artículo 54 *ter* del Reglamento General de las actuaciones y procedimientos de gestión e inspección tributaria[5] (Real Decreto 1065/2007, 2007) tiene como objetivo establecer una obligación de información específica para personas o entidades, y en particular, para las denominadas "plataformas colaborativas" que intermedian en la cesión del uso de viviendas con fines

[5] Este artículo fue incorporado mediante el artículo undécimo del Real Decreto 1070/2017, de 29 de diciembre, por el que se modifican el Reglamento General de las actuaciones y procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos, aprobado por el Real Decreto 1065/2007, de 27 de julio, y el Real Decreto 1676/2009, de 13 de noviembre, por el que se regula el Consejo para la Defensa del Contribuyente.

turísticos con fines de prevención del fraude fiscal. Por tanto, y bajo la premisa de evitar el fraude fiscal, este precepto obliga a las plataformas digitales que intermedian en el alquiler de viviendas turísticas a proporcionar a la Agencia Tributaria española información sobre sus usuarios (tanto quienes ofrecen una vivienda, como quienes la alquilan) relativa a: sus datos personales (nombre, apellidos, documento de identidad), referencias catastrales de los inmuebles, duración de las estancias, importe de cada alquiler o la naturaleza del intercambio cuando no exista contraprestación económica.

Actualmente, esta obligación informativa no se exige, al haber sido anulada por la Sentencia del Tribunal Supremo S.T.S. 1106/2020, de 23 de julio de 2020. De todas formas, la anulación se ampara en exclusivamente en motivos formales, por considerar el Tribunal que, en virtud de la Directiva 1535/2015 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, el Estado español tendría que haber notificado a la Comisión Europea la intención de aprobar la mencionada obligación informativa. Es de suponer, por tanto, que una vez se subsane el defecto procedimental cometido por el legislador**,** esta obligación informativa se podrá establecer de nuevo.

En nuestra opinión, el legislador tributario español debería de seguir incorporando deberes de suministro de información tributaria en otros ámbitos en los que las plataformas digitales actúan de intermediarias; ya que, de esta forma, se facilitarán las labores de control por parte de las administraciones tributarias y, en última instancia, se podrá simplificar la aplicación del sistema tributario. En todo caso, el legislador tributario español se verá abocado a dicha tarea si, finalmente, se aprueba la Propuesta de Directiva del Consejo por la que se modifica la Directiva 2011/16/UE relativa a la cooperación administrativa en el ámbito de la fiscalidad (2020).

III. LA COLABORACIÓN DE LAS PLATAFORMAS DIGITALES EN LA RECAUDACIÓN DE LOS TRIBUTOS

La normativa española y la de la UE acerca de la colaboración de las plataformas digitales en la recaudación tributaria se encuentran en un estadio inicial. Si bien existen ejemplos en ciertas Comunidades Autónomas, así como en otros Estados miembros (Mories Jiménez, 2017b, p. 93), no han sido suficientes para que el legislador haya impulsado la adopción de medidas concretas dirigidas a las plataformas digitales (Comisión Europea, 2016). En España, el legislador estatal se ha limitado a regular el *crowdfunding* financiero, sin que se contemple ningún mecanismo de colaboración directa entre las plataformas y las administraciones tributarias en el ámbito de la recaudación (Ley 5/2015, 2015).

Como ha señalado Correcher Mato:

> involucrar en la recaudación tributaria a las plataformas colaborativas que intermedian en el pago, aprovechando sus particularidades, es, sin duda, uno de los instrumentos más eficaces para asegurar el deber de contribuir y la recaudación tributaria; pero también, aunque de forma indirecta, para garantizar el control tributario y superar las dificultades para identificar contribuyentes e ingresos imponibles en la economía colaborativa, amén de obtener información sobre los prestadores de servicios en este fenómeno (2018, p. 5).

En definitiva, para que se pudiese iniciar una regulación al respecto sería preciso, en primer lugar, identificar aquellas figuras impositivas ligadas a la actividad económica subyacente y, a partir de ahí, delimitar las categorías tributarias subjetivas más adecuadas que permitiesen asegurar y simplificar la recaudación y mejorar el control tributario sobre los ingresos imponibles (Correcher Mato, 2018, p. 6). Para todo ello hay que tener en cuenta las características del sector de la economía colaborativa sobre la que se quiere aplicar e incluso, el tipo de rendimiento sobre el que se va a establecer, teniendo en cuenta que el control de las obligaciones fiscales de los contribuyentes que realizan actividades ajenas a las rentas provenientes de actividades económicas son más laxas no solo en el Impuesto sobre la Renta de las Personas Físicas, sino también con relación al Impuesto sobre Sociedades (Mories Jiménez, 2017a, p. 54).

Así las cosas, tal y como ha puesto de manifiesto Machaconses García (2019, p. 201), se deben analizar tres aspectos a la hora de configurar esta obligación tributaria: (a) los tributos en cuya recaudación puede intervenir las plataformas digitales; (b) delimitar la categoría subjetiva más adecuada para la colaboración en la recaudación; y (c) concretar cómo se puede cumplir con la obligación cuando una gran parte de las plataformas digitales no son residentes fiscales en el territorio nacional. No obstante, antes de iniciar el análisis propuesto, debemos recordar el elenco de obligados tributarios previstos en la normativa tributaria.

A. Categorías subjetivas del ordenamiento tributario español

El artículo 35 de la LGT (Ley 58/2003, 2003) establece un elenco de obligados tributarios a los que

la ley de cada tributo les puede imponer el cumplimiento de obligaciones tributarias. Entre todos los supuestos mencionados en la LGT, el contribuyente se configura como la figura subjetiva sobre la que pivota el tributo en la medida en que se le imputa la obligación tributaria principal, que deriva de la realización del hecho imponible. El resto de obligados tributarios tienen un papel diferente en el cumplimiento de la obligación tributaria.

El elemento subjetivo del tributo se configura como uno de sus elementos esenciales y está sujeto a reserva de ley. De esta manera, la ley específica de cada tributo debe contener la configuración subjetiva de las plataformas digitales respecto de la obligación tributaria principal, regulando el presupuesto de hecho. Es cierto que caben otras posibilidades que no se encuadran en la figura de un obligado tributario que, tal vez, resultan más sencillas y útiles en la recaudación de los tributos. En concreto, tal y como apunta Correcher Mato (2018, p. 7), se pueden celebrar acuerdos de naturaleza convencional entre la administración tributaria y las plataformas digitales con carácter voluntario para que colaboren con la Administración, aunque dichos acuerdos siempre tendrían que estar regulados en la ley tributaria. Por ello, como aliciente para la suscripción de estos acuerdos, este mismo autor propone establecer una mención o calificación administrativa que certifique el cumplimiento de las obligaciones legales y de colaboración con los poderes públicos, teniendo en cuenta que parte del éxito de dichas plataformas se debe a la reputación de las mismas frente a sus usuarios (Correcher Mato, 2018).

Pues bien, atendiendo a los distintos obligados tributarios que existen en nuestro ordenamiento las propuestas se limitan a la figura de los retenedores, responsables y sustitutos.

La figura del sustituto se regula en el artículo 36.3 de la LGT como aquel obligado tributario que ocupa, en la relación jurídico-tributaria, el lugar del contribuyente (Ley 58/2003, 2003). Así, el sustituto queda obligado al cumplimiento de todas las obligaciones materiales y formales del contribuyente. Si bien, en la actualidad, la figura del sustituto aparece como sujeto pasivo solo en casos que se pueden calificar como marginales en el ordenamiento español, ello no obsta para que pueda ser una figura a tener en cuenta en el caso que nos ocupa.

El retenedor tiene una gran importancia práctica en impuestos como el Impuesto sobre la Renta de las Personas Físicas y el Impuesto sobre Sociedades, aunque en este último con una intensidad menor respecto del primero. El artículo 37.2 de la LGT regula la figura del retenedor como aquel que tiene la obligación de detraer e ingresar ante la administración tributaria, con ocasión de los pagos que realicen a otros obligados tributarios, una parte de su importe, a cuenta del tributo que corresponde a estos últimos (Ley 58/2003, 2003).

En todo caso, la obligación del retenedor es autónoma e independiente de la obligación tributaria principal, que le corresponde al contribuyente que soporta la retención. Esto significa que la obligación de retener tiene su propio presupuesto de hecho, íntimamente relacionado con los pagos que realiza el retenedor al retenido. Y ello produce dos efectos: en primer lugar, el retenedor está obligado a efectuar el ingreso de la retención, aunque no la haya detraído de manera efectiva de los pagos que debe hacer al contribuyente; en segundo lugar, el contribuyente que soporta la retención se deduce de su impuesto personal la cantidad retenida –o la que hubiera debido ser retenida, en el caso de que el retenedor no la hubiera practicado–. Así, el retenedor que no haya practicado la retención queda obligado frente a la Administración a ingresar el importe de las que debió practicar sin que sufra menoscabo la recaudación de los tributos.

En tercer lugar, la ley puede configurar como responsable solidario o subsidiario de la deuda del contribuyente a otras personas o entidades, tal y como se establece en el artículo 41.1 de la LGT (Ley 58/2003, 2003). La figura del responsable se encuentra íntimamente relacionada con una función de garantía, o aseguramiento del pago, de la obligación tributaria del contribuyente. Por ello, para exigir la responsabilidad será necesario, no solo que se haya realizado el presupuesto de hecho del que esta deriva, sino que sea declarada en un acto administrativo con previa audiencia del interesado. No obstante, si bien el artículo 41.5 de la LGT puntualiza que es necesario el acto administrativo de derivación de responsabilidad, también precisa que la ley puede disponer otra cosa (Ley 58/2003, 2003). Y, en efecto, en el ordenamiento tributario español se prevé, excepcionalmente, un supuesto de responsabilidad en el que no es necesario el citado acto administrativo, dicho supuesto está regulado en el artículo 9.3 del Texto Refundido de la Ley del Impuesto sobre la Renta de No Residentes (Real Decreto Legislativo 5/2004, 2004).

B. Tributos en cuya recaudación pueden intervenir las plataformas digitales

A los efectos de delimitar los impuestos en los que podría intervenir la plataforma digital facilitando las tareas de recaudación de la Administración debemos referirnos, en principio, a los supuestos en los que las plataformas intermedian en la transacción que llevan a cabo (ya sea una prestación

de servicios o una venta de bienes); si bien, cabría diferenciar los siguientes supuestos.

En primer lugar, si la plataforma actúa en nombre y por cuenta de terceros –por ejemplo, Booking– presta un servicio de mediación, por lo que hay que atender al lugar en el que se presta el servicio que se ha contratado y en Estado dónde reside el proveedor/prestador del mismo. Además, la plataforma digital puede intermediar en el pago –por ejemplo, como ocurre en el caso de Airbnb– o no –como sucede, por ejemplo, con Booking–, pudiendo en este último caso prestar otro servicio al proveedor, en concreto, garantizar que pueda cobrar el servicio en caso de cancelación del usuario, exigiéndole a este último el número de la tarjeta de crédito/débito para poder hacer la reserva.

En segundo lugar, cuando la plataforma actúa en nombre propio y por cuenta de terceros, la plataforma digital es la que factura directamente el servicio al usuario. El prestador del servicio/proveedor realiza la actividad contratada por cuenta de la plataforma sobre la base de una relación comercial. El prestador del servicio emite una factura a la plataforma digital con el coste del servicio y el IVA correspondiente, siempre que la operación esté sujeta. A su vez, la plataforma emite otra factura al usuario del servicio. En estos casos, la actuación de la plataforma no se circunscribe a la intermediación del servicio, sino que va más allá, porque es ella quien presta el servicio.

A la vista de los tributos en los que la plataforma podría participar como obligado tributario distinto del contribuyente, debemos descartar de nuestro análisis al IVA, en la medida en que la repercusión es un deber para el contribuyente, quedando el adquirente obligado a soportarla. La LGT y la Ley del IVA convierten a la repercusión en una operación con relevancia jurídico-tributaria, ya que no se circunscribe a las relaciones entre privados (Ley 58/2003, 2003; Ley 37/1992, 1992). En concreto, el obligado a repercutir y el obligado a soportar la repercusión son sujetos de una obligación prevista en una norma tributaria, de tal manera que las controversias que puedan surgir se sustancian exactamente igual que otros tributos, es decir, por la vía de los recursos contra actuaciones de la administración tributaria. Asimismo, en el IVA, el sujeto obligado a soportar la repercusión es el titular de la capacidad económica que se quiere gravar, pero ante la Administración el contribuyente formal es el obligado a repercutir. La propia LGT establece que "el repercutido no está obligado al pago frente a la administración tributaria" (Ley 58/2003, 2003, art. 38), ni siquiera en caso de que el contribuyente no haya practicado la repercusión ni haya ingresado el tributo.

Por tanto, el papel de las plataformas digitales como obligadas tributarias, no a título de contribuyentes, se circunscribe a los impuestos directos, como el Impuesto sobre Sociedades, el Impuesto sobre la Renta de las Personas Físicas, el Impuesto sobre la Renta de No Residentes, así como aquellos impuestos autonómicos cuyo objeto es gravar las estancias en establecimientos turísticos. Es decir, nos referimos a los impuestos que gravan los rendimientos obtenidos por los proveedores y aquellos impuestos que gravan a los usuarios, en la actualidad, limitado a las estancias, aunque, sin ánimo de despertar la imaginación del legislador pueden existir otros hechos imponibles.

En definitiva, los impuestos a los que nos referimos en los que las plataformas digitales pueden ser colaboradores se limitan a dos ámbitos: (a) aquellos que gravan los beneficios provenientes de la actividad económica de los prestadores del servicio tales como el Impuesto sobre Sociedades, el Impuesto sobre la Renta de las Personas Físicas o el Impuesto sobre la Renta de No Residentes (queda excluido el IVA puesto que por la propia naturaleza el obligado a repercutir tiene la naturaleza de obligado tributario; y (b) aquellos impuestos que gravan a los usuarios de servicios calificados como economía colaborativa, tales como la estancia en establecimientos turísticos.

Como hemos mencionado anteriormente, en la medida en que el control tributario que ejerce la Administración sobre las personas jurídicas tiene más intensidad respecto de aquellas personas físicas que realizan el mismo tipo de actividades, va a influir a la hora de configurar el papel de las plataformas digitales como obligados tributarios en la recaudación de todos estos impuestos. De este modo, se nos ocurre que en el ámbito del Impuesto sobre la Rentas de las Personas Físicas se podría regular una fuente de renta específica distinta de los rendimientos de capital mobiliario o de actividades económicas para establecer un mayor control y facilitar la actuación de las plataformas digitales (Mories Jiménez, 2017b, pp. 101-102).

C. Las plataformas digitales como obligados tributarios

Tras haber señalado las obligaciones tributarias que surgen tanto para las plataformas como para los usuarios de las mismas y las categorías de obligados tributarios, la siguiente cuestión es dilucidar si las plataformas digitales pueden colaborar en la recaudación y garantizar el pago de las obligaciones tributarias de sus usuarios.

Pues bien, en el caso de los proveedores que actúan por cuenta de la plataforma, como ocurre en

el caso de Uber, la plataforma al proceder al pago de las cuantías adeudas por el servicio prestado, siempre que la renta se encuentre sujeta, tiene la obligación de retener la cantidad establecida en la Ley del Impuesto sobre la Renta de las Personas Físicas o, en su caso, en el Impuesto sobre Sociedades, según los proveedores sean una persona física o jurídica. Como ha indicado Correcher Mato respecto de la figura del retenedor, "la retención y el posterior ingreso permite a la administración tributaria tener contraladas las operaciones realizadas y los sujetos involucrados" (2018, p. 5). Sin embargo, nos surgen algunas dudas respecto de la obligación de retener en el caso de que la plataforma sea una simple intermediaria en el pago y, por otra parte, que no tenga su residencia fiscal en territorio español.

Respecto de la primera cuestión planteada, si la plataforma paga al proveedor por cuenta y orden del usuario, se considera como una mera intermediaria en el pago de los servicios prestados, y, por tanto, no tiene la obligación de retener[6]. En el segundo supuesto planteado, que la plataforma digital no tenga su residencia en territorio español, tenemos que distinguir dos supuestos:

(i) Que la plataforma retribuya a los proveedores porque presta los servicios en nombre propio.

(ii) Que sean los proveedores los que retribuyan a la plataforma digital por el servicio prestado de intermediación.

Pues bien, si la plataforma retribuye por los servicios prestados por los proveedores en territorio español, solo tiene obligación de retener si los pagos realizados a los proveedores constituyen un gasto deducible porque las rentas de la plataforma digital tributan en territorio español, aunque se hayan obtenido sin mediación de establecimiento permanente y siempre que se puedan calificar como prestaciones de servicios porque no se pueden calificar de otra manera. El legislador se refiere a aquellos rendimientos calificados de prestaciones de servicios utilizados en territorio español porque sirven a actividades económicas realizadas en territorio español o se refieran a bienes situado en este, siempre que lo pagos realizados tengan la consideración de gasto deducible de los ingresos brutos[7]. La explicación de porqué el legislador solo prevé la retención respecto de los pagos deducibles, según el artículo 24.2 del Texto Refundido de la Ley del Impuesto sobre la Renta de No Residentes (Real Decreto Legislativo 5/2004, 2004), radica en que regular la retención sobre otras rentas obtenidas por no residentes sin establecimiento permanente no supone un mayor control por parte de la administración tributaria española y, por ende, de lucha contra el fraude fiscal, porque el pagador no residente no tiene obligaciones formales en nuestro país.

En el segundo caso, los proveedores son los que pagan y los que tienen la obligación retener a la plataforma digital si tributase en territorio español porque realiza su actividad a través de un establecimiento permanente. La realidad es que una gran parte de las plataformas digitales tienen su residencia fiscal en otros estados distintos del español, por lo tanto, mientras no se regule la presencia digital significativa para someter a tributación las rentas obtenidas en el territorio dónde se produce el consumo de los bienes o servicios, difícilmente se les va a poder retener.

En definitiva, en la medida en que las plataformas digitales no residentes se encuentran en el primer caso, es decir que no son meras intermediarias y las rentas obtenidas en territorio español se puedan calificar como prestaciones de servicios, existe la obligación de retener a los proveedores. Esto significa que, si no se produce una modificación legislativa, la figura del retenedor queda circunscrita a supuestos muy concretos y, por tanto, supone seguir indagando en otras posibilidades de obligados tributarios.

Cuando nos referimos a la figura del sustituto del contribuyente, en el caso de las plataformas digitales, ¿puede existir un sustituto del contribuyente de una parte del hecho imponible, es decir de un determinado rendimiento? La respuesta solo puede ser negativa, porque el sustituto del contribuyente, tal y como se ha señalado anteriormente, se coloca *ope legis* en lugar de este último, por tanto, del hecho imponible en su totalidad, no de una parte del mismo, al igual que ocurre en el caso de las rentas gravadas por el Impuesto sobre la Renta de las personas físicas. Es verdad que se ha abogado por la figura del sustituto en la medida en que cumple con todas las obligaciones materiales y formales del contribuyente, por lo que resulta más fácil que la plataforma declare las operaciones y servicios operados por los proveedores lo que supone no solo garantizar el pago del tributo, sino que la Administración pueda

[6] *Cfr.* artículo 99 de la Ley del Impuesto sobre la Renta de las Personas Físicas (Ley 35/2006, 2006) y artículo 76 del Reglamento del Impuesto sobre la Renta de las Personas Físicas (Real Decreto 439/2007, 2007).

[7] *Cfr.* artículos 24 y 31 de la Ley del Impuesto sobre la Renta de las Personas Físicas (Ley 35/2006, 2006).

controlar las operaciones realizadas y los sujetos que intervienen[8].

Sin embargo, a pesar de las buenas intenciones, la realidad jurídica impide que las plataformas digitales puedan ser sustitutos, salvo en algunos tributos. Por ejemplo, aquellos impuestos autonómicos que gravan la estancia en establecimientos turísticos. Las plataformas digitales podrían configurarse como sustitutos de los contribuyentes, pero siempre que medien en el pago –por ejemplo, el caso de Airbnb–, lo que supondría una simplificación en la recaudación, al configurarse el impuesto como instantáneo (Mories Jiménez, 2017b, p. 127). Es cierto que, en esos casos, la plataforma tendría que exigir el pago del tributo con antelación a la realización del hecho imponible, teniendo en cuenta que además puede cancelarse la estancia. Si la plataforma ni siquiera media en el pago –por ejemplo, Booking–, resulta más difícil considerarlas como sustituta de los contribuyentes. Tal vez, por este motivo, las leyes autonómicas que gravan las estancias turísticas regulan como sustitutos a los titulares de la explotación de establecimientos o equipamientos, quedando las plataformas digitales como responsables solidarios, tal y como veremos posteriormente.

Además de todo ello, surgen otras dificultades para considerar a las plataformas digitales como sustitutos (Correcher Mato, 2018, p. 11). Solo en el caso de que la plataforma digital tenga su residencia en España, el pago queda asegurado y se facilita a la Administración la información tributaria de la operación. Si la plataforma digital tiene su residencia en otro Estado, no parece posible que la mejor figura sea como sustituto si lo que se pretende es garantizar la recaudación, a no ser que le obligue a nombrar un representante que, tal y como veremos posteriormente, puede considerarse contrario a la libre circulación en la UE.

Tal y como hacíamos mención anteriormente, la figura del responsable también permite garantizar el pago del tributo, por lo que la LGT, así como otras normas tributarias regulan los presupuestos de hecho de la responsabilidad, que solo se puede declarar, tal y como contempla el artículo 174 de la LGT (Ley 58/2003, 2003), una vez que la obligación tributaria principal se encuentra liquidada y alcanzará a la totalidad de la deuda tributaria exigida en período voluntario. Hasta el momento, las plataformas digitales han sido calificadas como responsables en los impuestos autonómicos que gravan las estancias en establecimientos turísticos. Más allá de la calificación de la responsabilidad como solidaria –impuesto catalán– o subsidiaria –impuesto balear–, el presupuesto de hecho de ambos impuestos se asemeja; es decir, las plataformas digitales responden del pago del impuesto del contribuyente cuando hacen de intermediarias ente este y los establecimientos. Resulta esclarecedor que nos hallamos ante un supuesto de responsabilidad genuino a diferencia de la mayoría de los supuestos regulados en el artículo 42 y 43 de la LGT (Ley 58/2003, 2003), en los que el responsable omite determinadas obligaciones o actúa poniendo en peligro el crédito tributario.

¿Se puede regular un supuesto de responsabilidad cuando la plataforma digital actúa en nombre y por cuenta de terceros con relación a los rendimientos que obtienen los proveedores por la actividad económica que realizan? En una gran parte de los supuestos la intervención de las plataformas digitales no se limita a poner en contacto al usuario-proveedor, sino que también suelen garantizar o mediar en el pago en nombre del usuario, lo que les reporta una gran información sobre los servicios que finalmente se prestan por parte del proveedor, así como de las retribuciones que perciben. El ejemplo más claro lo tenemos en la regulación del impuesto sobre estancias turísticas.

A nuestro juicio, se podría establecer que las plataformas digitales puedan ser responsables subsidiarias en atención al siguiente presupuesto de hecho; cuando los ingresos percibidos por los proveedores, por ejemplo, en más de un 75%, provengan de servicios prestados a través de la intermediación de una o varias plataformas digitales. En ese caso, habría que distinguir si el proveedor es una persona jurídica, se atendería al conjunto de las rentas sometidas al Impuesto sobre Sociedades; respecto de las personas físicas, el 75% debe referirse a las rentas obtenidas por esta actividad, se califiquen como rendimientos de actividades económicas o del capital, con independencia de la cuantía de otras rentas obtenidas como, por ejemplo, las que provienen del trabajo.

Lógicamente, la declaración de responsabilidad solo sería posible en caso de que los proveedores no cumplieran con sus obligaciones tributarias en su totalidad y se pusieran a descubierto en un procedimiento inspector. Asimismo, este supuesto de responsabilidad no alcanzaría a las sanciones que pudieran imponerse, en su caso, al contribuyente. La opción de regular la responsabilidad como subsidiaria supone para los responsables una garantía ya que solo hacen frente al pago de la obligación tributaria principal cuando el contribuyente haya

[8] *Cfr*. Comité Económico y Social Europeo (Dictamen 2019/C 353/04, 2019).

sido declarado insolvente, aunque dificulta que el responsable pueda resarcirse del cumplimiento de la responsabilidad.

De este modo, la plataforma no solo ayuda a que exista un control tributario de los servicios que se prestan a través de la plataforma digital, proporcionando el rastreo de los ingresos percibidos. Es cierto que, al establecer un porcentaje tan alto, un 75% en su conjunto, con independencia de que provenga de una o varias plataformas por lo que resulta inocuo que el proveedor fragmente a través de diferentes plataformas la oferta de sus servicios. Además, una vez implantado este supuesto de responsabilidad, serviría para que las propias plataformas excluyeran a aquellos proveedores que no cumplan con sus obligaciones tributarias exigiendo, por ejemplo, un certificado tributario.

A pesar de esta propuesta y con independencia de que solo la ley permite regular la responsabilidad, nos hallamos ante varias dificultades. La primera es que la responsabilidad se declara a través de un procedimiento regulado en los artículos 174 y 175 de la LGT (Ley 58/2003, 2003), con la única salvedad prevista en el Texto Refundido de la Ley del Impuesto sobre la Renta de No Residentes (Real Decreto Legislativo 5/2004, 2004). En el caso de que la Administración tenga que declarar la responsabilidad a un conjunto más o menos grande de plataformas digitales, supone un coste administrativo que puede ser superior a la cuantía de la deuda por la que se declara la responsabilidad, sobre todo cuando el proveedor es una persona física. A ello hay que sumarle la dificultad de declarar la responsabilidad a plataformas digitales que no son residentes en España y que, en ese caso, tendrían que nombrar un representante en territorio español. A los efectos de solventar la primera cuestión, se podría regular, al igual que ocurre en el Impuesto sobre la Renta de No Residentes, que la declaración de responsabilidad la realice la Administración, sin necesidad de procedimiento del artículo 174 de la LGT (Ley 58/2003, 2003), y quedando limitada al conjunto las rentas anuales obtenidas por el pagador en las que haya intervenido la plataforma digital.

Más allá de los supuestos expresamente previstos en la LGT de obligados tributarios, algunas Comunidades Autónomas han regulado una figura calificada como "asistentes a la recaudación", que tal y como se prevé en la Ley 5/2017 (2017), por la que plataformas digitales de manera voluntaria, a través de acuerdos o convenios, colaboran con la agencia tributaria catalán para facilitar el cumplimiento de las obligaciones tributarias derivadas del impuesto sobre estancias turísticas[9]. Como no podía ser de otra manera, las plataformas que así lo deseen pueden presentar una solicitud en la Agencia tributaria catalana y firmar un convenio de colaboración, aunque para poder habilitarlas como asistentes resulta imprescindible que exista una auditoria de los sistemas informáticos que utilizan para poder garantizar la adecuación de los mismos para la correcta aplicación del impuesto. A partir de ese momento, la plataforma puede presentar y hacer el pago de las autoliquidaciones de los sujetos pasivos sustitutos de quien tenga concedido el consentimiento para que actúe en su nombre. Eso supone que los propietarios de los establecimientos y equipamientos turísticos presten su consentimiento previo a ello.

Esta figura de 'asistentes a la recaudación' puede facilitar a la administración tributaria en la aplicación de las funciones de recaudación. No obstante, esta figura implica un coste administrativo para la plataforma que puede suponer un obstáculo para conseguir la colaboración de estas. Tal vez, para alentar la participación de las plataformas digitales y que el coste de la colaboración no lo asuma indirectamente el proveedor o el usuario por un aumento en la tarifa que pagan a la plataforma, se podría regular la posibilidad de que un porcentaje de la recaudación obtenida sufrague los costes administrativos de la plataforma.

Como vemos existen distintas soluciones que se pueden adoptar por parte del legislador, lo que va a comportar modificaciones legislativas de gran calado en varios impuestos. Tal vez, lo más fácil es establecer una obligación específica de retención de las plataformas digitales, incluso cuando medien en el pago de rentas que se encuentran sujetas a un determinado tributo, ya que hoy por hoy no existe la obligación de retener. Lucas Durán (2017, p. 165) ha afirmado que la creación de un supuesto específico de reten-

[9] Esta figura se ha utilizado en distintos países. En concreto, en Holanda se ha permitido que los municipios establezcan acuerdos de colaboración con las plataformas que operan en el sector del alojamiento para que faciliten el pago de tributos turísticos en nombre de los prestadores de los servicios. En Francia, las plataformas facilitan el pago de las tasas turísticas en nombre de los prestadores de servicios, o son utilizadas para recaudar impuestos de los prestadores individuales. En Estonia se ha conseguido que las plataformas colaboren proporcionando información acerca de las transacciones registradas a efectos de que las autoridades fiscales puedan presentar borradores de declaraciones tributarias a los prestados de servicios. Véase Navarro Egea (2017, p. 527).

ción a cuenta resultaría más eficiente que las propias obligaciones específicas de información, porque una retención practicada sobre un pago en efectivo proporciona la misma información que la primera y, además, supone una fuente de financiación continuada para la Hacienda Pública a medida que se realizan los pagos. Ahora bien, hay que tener en cuenta que, para poder llevar a cabo esta retención, la renta debe estar sujeta y no exenta. A ello hay que sumarle que en el caso de que la plataforma digital no tenga su residencia en España, el cumplimiento del deber de retener puede ser más difícil.

D. Plataformas digitales no residentes

Como hemos observado en los apartados anteriores, uno de los aspectos más complejos en la regulación de las plataformas digitales como obligados tributarios o, incluso, como asistentes en la recaudación, es la imposición de obligaciones tributarias cuando no tienen la consideración de residentes en territorio español.

Las obligaciones de las entidades no residentes difieren cuando actúan con o sin establecimiento permanente. Pues bien, en el caso que nos ocupa, con la legislación vigente y a la espera de la regulación de la presencia digital significativa, las plataformas digitales no residentes actúan, normalmente, sin establecimiento permanente. Para poder determinar las obligaciones formales y materiales que se les puede exigir a las plataformas digitales como obligados tributarios hay que distinguir, tal y como hemos analizado en apartados anteriores, cuando actúa en nombre propio, pero por cuenta de terceros, o en nombre y por cuenta de terceros. Sea como sea, la dificultad en ambos casos radica en la no residencia de la plataforma digital. A ello hay que sumarle que, con independencia de que se puedan producir cambios normativos como alguno de los propuestos en el apartado anterior, con la legislación actual la plataforma digital se encuentra abocada a nombrar un representante en territorio español, tal y como se establece en el artículo 10 del Texto Refundido de la Ley del Impuesto sobre la Renta de No Residentes (Real Decreto Legislativo 5/2004, 2004). El mencionado precepto prevé que, en el caso de que el no residente –en nuestro caso, las plataformas digitales– realice actividades o explotaciones económicas en España, tiene obligación de nombrar un representante en España. No obstante, el Tribunal de Justicia de la Unión Europea ha considerado que la obligación de nombrar un lugar fijo o un representante para un cumplimiento de obligaciones de no residentes puede vulnerar la libre prestación de servicios[10].

A pesar de ello, a nuestro juicio, no resulta tan gravoso que la plataforma pueda nombrar como representante a otra sociedad del grupo residente en territorio español. Una gran mayoría de las plataformas, tales como Booking, Uber, etc., tienen una sociedad residente en España que normalmente solo se ocupa de tareas de publicidad, marketing o logística; mientras que otras sociedades de la plataforma que intervienen en el contrato entre usuarios y plataforma o en el servicio de pago, tienen su sede en otros Estados miembros de la UE tales como Irlanda u Holanda. En estos casos, la sociedad española, pese a ser residente, no interviene en la gestión del pago, pero se le puede nombrar representante de la sociedad no residente que es la obligada a hacer frente a la obligación material (Mories Jiménez, 2017b, p. 116).

No obstante, la postura que mantiene el Tribunal de Justicia se puede matizar porque tal vez, efectivamente, no siempre sea necesaria la figura del representante del no residente. Pero para ello, resulta imprescindible la colaboración entre Estados como ocurre en la UE, dónde se pueden exigir obligaciones tributarias, incluidas las sanciones, a los residentes de otros Estados cuando en el Estado fuente no tenga rentas o patrimonio embargable (Sánchez Huete, 2017a, p. 11)[11]. Fuera de la UE tanto el Convenio sobre Asistencia Administrativa Mutua en Asuntos Fiscales, como el Modelo de Convenio de la OCDE, prevén la asistencia mutua en materia de recaudación y cobro de créditos.

Lo que no hay lugar a dudas es que la información que proporcionan los pagadores de las rentas abonadas resulta vital para una correcta aplicación del sistema tributario; porque, de esa manera, pueden controlarse los rendimientos respecto de los cuales la Administración no tiene información

[10] Véase Sentencia del Tribunal de Justicia de la Unión Europea de 11 de diciembre de 2014. En esta sentencia el Tribunal consideró que la obligación de nombrar un representante residente fiscal en territorio español resulta desproporcionada por ir más allá de lo necesario para lograr el objetivo perseguido, dado que existen mecanismos de cooperación entre las administraciones tributarias (Comisión Europea c. Reino de España, Caso C-576/13, 2014).

[11] *Cfr*. Directiva 2010/24/UE del Consejo de la Unión Europea, de 16 de marzo de 2010, sobre la asistencia mutua en materia de cobro de los créditos correspondientes a determinados impuestos, derechos y otras medidas; Directiva 2011/16/UE, de 15 de febrero de 2011, relativa a la cooperación administrativa en el ámbito de la fiscalidad y por la que se deroga la Directiva 77/799/CEE.

por parte de los sujetos pasivos. Por tal motivo, las obligaciones de retención e ingreso con relación a pagos realizados a contribuyentes en España –personas físicas o jurídicas–, deberían modificarse en el Impuesto sobre la Renta de las Personas Físicas, en el Impuesto sobre Sociedades y, por supuesto, en el Impuesto sobre la Renta de No Residentes. Solo de esta manera, la administración tributaria podría verificar la efectiva tributación de tales rentas, sin tener que solicitar a dichas plataformas –entidades no residentes–, los oportunos datos con relevancia fiscal a través de requerimientos individualizados respecto de cada plataforma y periodo impositivo, siempre que exista un convenio de doble imposición que contenga las oportunas cláusulas de intercambio de información con el Estado de residencia de la plataforma.

IV. CONCLUSIONES

Las especiales características que presentan las plataformas digitales que intermedian en prestaciones de servicios o en la venta de bienes las convierten idóneas colaboradoras de las administraciones tributarias a la hora de prestar asistencia y colaboración a los usuarios de las mencionadas plataformas en el cumplimiento de sus obligaciones tributarias. Apremia, en todo caso, articular vías para lograr dicha asistencia y colaboración, voluntaria o imperativa, por parte las plataformas digitales; porque, solo así, se podrá avanzar en la simplificación y en el control de la aplicación de los tributos, garantizando la efectividad del deber de contribuir.

El establecimiento de específicos deberes de información tributaria, tanto de carácter nacional como supranacional, en virtud de los cuales las plataformas digitales –en particular, las de intermediación– se viesen obligadas a proporcionar información tributaria relevante sobre las actividades económicas desarrolladas por sus usuarios –sobre todo, cuando los usuarios son particulares–, tendría un impacto muy positivo en la correcta aplicación de los tributos; y, en última instancia, en el incremento de los ingresos públicos estatales. No obstante, y en primer lugar, debería aclararse el tratamiento fiscal de ciertos modelos de negocio que han surgido al amparo de las plataformas digitales.

Por lo que se refiere a la colaboración de las plataformas digitales en la recaudación tributaria, y desde una perspectiva de pura eficiencia administrativa y racionalidad de los procedimientos administrativos, aprobar en el Impuesto sobre la Renta de las Personas Físicas, en el Impuesto sobre Sociedades y en el Impuesto sobre la Renta de No Residentes (Impuesto a la Renta sobre Personas Físicas), una obligación de retener facilitaría extraordinariamente la gestión tributaria de las rentas pagadas tanto a residentes, como no residentes.

En todo caso, y más que establecer un supuesto específico de representación en el caso de las plataformas digitales no residentes a los efectos de poder retener, sería deseable alcanzar acuerdos de colaboración de las plataformas digitales con la administración tributaria española. La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, podría servir de cauce legal para promover esta colaboración a las plataformas digitales; lo que, según Sánchez Huete, "supondría un canal de información para la administración tributaria y para las entidades, en la medida en que estas podrían informar a sus clientes de las obligaciones tributarias existentes" (2017a, p. 13).

Por último, y aunque parezca una obviedad, ninguna de estas propuestas parecen realizables si, por una parte, no se involucra a todas las plataformas digitales y no solo aquellas relacionadas –como ha ocurrido hasta ahora– con el alquiler de viviendas por períodos cortos, o con fines turísticos. Y, por otra parte, la regulación de estas medidas tendría que adoptarse a nivel, al menos europeo, lo que permitiría un mejor control–recaudación de las rentas que se obtienen utilizando las plataformas digitales y, por ende, reforzando la lucha contra el fraude fiscal.

REFERENCIAS

Antón Antón, A. (2017). Implicaciones fiscales de la economía colaborativa en la era digital. En S. Moreno González (dir.) & J.A. Gómez Requena (ed.), *Tendencias y desafíos fiscales de la economía digital* (pp. 561-588). Thomson Reuters Aranzadi.

(2019). El ordenamiento tributario frente a los retos de los modelos de economía colaborativa surgidos en el contexto de la economía digital. En I. Bilbao Estrada & A. Antón Antón (dirs.), *Retos y oportunidades de la administración tributaria en la era digital* (pp. 179-214). Thomson Reuters Aranzadi.

(2020). El papel de las plataformas de economía colaborativa en el control de focos tradicionales de economía sumergida. En A. García Martínez & T. García Luis (dirs) & M. Lucas Durán (coord.), *Desafíos fiscales de actualidad - Documentos de Trabajo del Instituto de Estudios Fiscales 5/2020* (pp. 243-261). Instituto de Estudios Fiscales.

Beretta, G. (2018). VAT and the Sharing Economy. *World Tax Journal*, *10*(3).

Bilbao Estrada, I. (2018) Fiscalidad directa del consumo colaborativo, deberes de información y derecho comparado. En J. Pedreira Menéndez (dir.), *Fiscalidad de la colaboración social* (pp. 237-262). Thomson Reuters Aranzadi.

Correcher Mato, C. J. (2018). Economía colaborativa y recaudación tributaria: especial consideración al papel de la plataforma. *Quincena Fiscal*, (22), 81-214.

Falcón y Tella, R. (2014). La tributación de UBER (plataforma de servicios de transporte en vehículos particulares). *Quincena Fiscal*, (13), 11-16.

Lucas Durán, M. (2017). Problemática jurídica de la economía colaborativa: especial referencia a la fiscalidad de las plataformas. *Anuario Facultad de Derecho de la Universidad de Alcalá*, (10), 131-172.

(2018). Ventas entre particulares a través de plataformas de internet: su fiscalidad. *Revista de Contabilidad y Tributación CEF*, (419), 125-148.

Machaconses García, E. (2019). Las plataformas digitales: protagonistas actuales del Derecho Tributario. En P. Alguacil Mari (dir.) & S. Montesinos Oltra (coord.), *Aspectos jurídicos y fiscales de la economía colaborativa* (pp. 175-214). Tirant lo Blanch.

Montesinos Oltra, S. (2016). Los actores de la economía colaborativa desde el punto de vista del Derecho tributario. *Revista Economía Industrial (Ejemplar dedicado a economía colaborativa)*, (402), 47-54.

Mories Jiménez, M.T. (2017a). La implantación de un nuevo régimen fiscal en Italia para los alquileres de inmuebles a corto plazo en el impuesto sobre la renta como medida de control de plataformas inmobiliarias. En M. Lucas Durán & C. García-Herrera Blanco (dirs.) & A. del Blanco García (coord.), *Fiscalidad de la economía colaborativa: especial mención a los sectores del alojamiento y del transporte - Documentos de Trabajo del Instituto de Estudios Fiscales 15/2017* (pp. 51-63). Instituto de Estudios Fiscales.

(2017b). La polémica implantación del nuevo régimen fiscal *per locazioni brevi* en Italia: nuevas obligaciones para los intermediarios y las plataformas de alojamiento. *CIRIEC-España, Revista Jurídica de economía social y cooperativa*, (31), 93-136.

Navarro Egea, M. (2017). La economía colaborativa ante la Hacienda Pública. En R. Alfonso Sánchez & J. Valero Torrijos (dirs.), *Retos jurídicos de la economía colaborativa en el contexto digital* (pp. 523-543). Thomson Reuters Aranzadi.

Organización para la Cooperación y el Desarrollo Económicos [OCDE] (2010). *Modelo de Convenio Tributario sobre la Renta y sobre el Patrimonio. Versión abreviada*. https://www.globbal.co/wp-content/uploads/2018/04/Modelo-de-CDI-OCDE-versi%C3%B3n-abreviada.pdf

(2018). *Resumen de los desafíos fiscales derivados de la digitalización: Informe provisional 2018*. https://www.oecd.org/tax/beps/resumen-desafios-fiscales-derivados-de-la-digitalizacion-informe-provisional-2018.pdf

Pastor del Pino, M. C. (2017). Economía colaborativa: situación, problemas tributarios y vías de actuación. *Crónica Tributaria*, (164), 155-183.

(2019). Las plataformas colaborativas como sujetos de colaboración social en la aplicación de los tributos. En I. Bilbao Estrada & A. Antón Antón (dirs.), *Retos y oportunidades de la administración tributaria en la era digital* (pp. 215-238). Thomson Reuters Aranzadi.

Rozas Valdés, J. A. (2017). ¿Hacia un Impuesto sobre actos jurídicos digitales? En M. Lucas Durán & C. García-Herrera Blanco (dirs.) & A. del Blanco García (coord.). *Fiscalidad de la economía colaborativa: especial mención a los sectores de alojamiento y transporte - Documentos de Trabajo del Instituto de Estudios Fiscales 15/2017* (pp. 126-150). Instituto de Estudios Fiscales.

Ruiz Garijo, M. (2018). La fiscalidad de los bancos de tiempo - Un debate abierto. En J. Pedreira Menéndez (dir.) & M.M. Pascual González (coord.), *Fiscalidad de la colaboración social* (pp. 181-197). Thomson Reuters Aranzadi.

Ruiz Hidalgo, C. (2019). Lugar de realización en el IVA de los servicios de intermediación prestados por vía electrónica en la economía colaborativa. *Diritto e Pratica tributaria internazionale*, (4), 1041-1052.

Sánchez Huete, M. A. (2017a). Cuestiones tributarias y economía colaborativa. *Quincena Fiscal*, (18), 89-116.

(2017b). Riesgo tributario y economía colaborativa. En M.C. Rodríguez-Piñero Royo & M. Hernández Bejarano (dirs.), *Economía colaborativa y trabajo en plataforma* (pp. 103-144). Bomarzo.

(2017c). Economía colaborativa: información y control tributario. En M. Lucas Durán & C. García-Herrera Blanco (dirs.) & A. del Blanco García (coord.), *Fiscalidad de la economía colaborativa: especial mención a los sectores del alojamiento y del transporte - Documentos de Trabajo del Instituto de Estudios Fiscales 15/2017* (pp. 16-36). Instituto de Estudios Fiscales.

Siota Álvarez, M. (2020). *La fiscalidad del transporte colaborativo de personas*. Thomson Reuters Aranzadi.

Vega García, A. (2017). Retos fiscales de la economía colaborativa. En S. Moreno González (dir.) & J.A. Gómez Requena (ed.), *Tendencias y desafíos fiscales de la economía digital* (pp. 589-604). Thomson Reuters Aranzadi.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Caso C-576/13, Comisión Europea c. Reino de Esp., ECLI:EU:C:2014:2430 (dic. 11, 2014).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones "Una Agenda Europea para la economía colaborativa", COM (2016) 356 final (jun. 2, 2016).

Convenio sobre Asistencia Administrativa Mutua en Asuntos Fiscales, Consejo Europeo, 25 de enero de 1988.

Dictamen 2018/C 081/09 del Comité Económico y Social Europeo sobre la «Fiscalidad de la economía colaborativa — Análisis de posibles políticas impositivas ante el crecimiento de la economía colaborativa», 2018 O.J. (C 81/65) (UE).

Dictamen 2019/C 353/04 del Comité Económico y Social Europeo sobre "La fiscalidad de la economía digitalizada", 2019 O.J. (C 353/17) (UE).

Directiva 1535/2015 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, 2015 O.J. (L 241) 1.

Directiva 2010/24/UE del Consejo, de 16 de marzo de 2010 , sobre la asistencia mutua en materia de cobro de los créditos correspondientes a determinados impuestos, derechos y otras medidas, 2010 O.J. (L 84) 1.

Directiva 2011/16/UE del Consejo de 15 de febrero de 2011 relativa a la cooperación administrativa en el ámbito de la fiscalidad y por la que se deroga la Directiva 77/799/CEE, 2011 O.J. (L 64) 1.

Ley 37/1992, Ley del Impuesto sobre el Valor Añadido (B.O.E. 1992, 37) (Esp.).

Ley 58/2003, Ley General Tributaria (B.O.E. 2003, 58) (Esp.).

Ley 35/2006, Ley del Impuesto sobre la Renta de las Personas Físicas y de modificación parcial de las leyes de los Impuestos sobre Sociedades, sobre la Renta de no Residentes y sobre el Patrimonio (B.O.E. 2006, 35) (Esp.).

Ley 27/2014, Ley del Impuesto sobre Sociedades (B.O.E. 2014, 27) (Esp.).

Ley 5/2015, Ley de fomento de la financiación empresarial (B.O.E. 2015, 5) (Esp.).

Ley 39/2015, Ley del Procedimiento Administrativo Común de las Administraciones Públicas (B.O.E. 2015, 39) (Esp.).

Ley 5/2017, Ley de medidas fiscales, administrativas, financieras y del sector público y de creación y regulación de los impuestos sobre grandes establecimientos comerciales, sobre estancias en establecimientos turísticos, sobre elementos radiotóxicos, sobre bebidas azucaradas envasadas y sobre emisiones de dióxido de carbono (B.O.E. 2017, 5) (Esp.).

Propuesta de Directiva del Consejo por la que se modifica la Directiva 2011/16/UE relativa a la cooperación administrativa en el ámbito de la fiscalidad, COM (2020) 314 final (jul. 15, 2020).

Real Decreto Legislativo 5/2004, por el que se aprueba el texto refundido de la Ley del Impuesto sobre la Renta de no Residentes (B.O.E. 2004, 5) (Esp.).

Real Decreto 439/2007, por el que se aprueba el Reglamento del Impuesto sobre la Renta de las Personas Físicas y se modifica el Reglamento de Planes y Fondos de Pensiones, aprobado por Real Decreto 304/2004, de 20 de febrero (B.O.E. 2007, 439) (Esp.).

Real Decreto 1065/2007, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos (BO.E. 2007, 1065) (Esp.).

Reglamento 904/2010 del Consejo, de 7 de octubre de 2010, relativo a la cooperación administrativa y la lucha contra el fraude en el ámbito del impuesto sobre el valor añadido, 2010 O.J. (L 268) 1 (UE).

S.T.S., 23 de julio de 2020, (No. 1106/2020) (Esp.).

10.18800/themis.202101.011

TRIBUTACIÓN DE CRIPTOMONEDAS Y OTROS CRIPTOACTIVOS: ANÁLISIS COMPARADO

TAXATION OF CRYPTOCURRENCIES AND OTHER CRYPTOASSETS: COMPARATIVE ANALYSIS

Martín Alonso La Rosa Almenara*
Rodrigo, Elías & Medrano

In recent years, a new asset class is gaining momentum which emerged as a response to the economic crisis of 2008, the technology that is behind these assets depend on blockchain technology and cryptography, by using a decentralized network so the users of such networks can freely transfer value -using cryptocurrencies or crypto-assets, without having to depend on an intermediary that centralizes and registers all the transactions.

This article analyses the current state of the taxation of cryptocurrency or crypto assets in Peru having as an initial reference point a recent study conducted by the OECD.

Keywords: Cryptocurrencies; cryptoassets; blockchain technology; Income Tax; Value Added Tax.

En los últimos años, se ha popularizado una nueva clase de activos que surgieron como respuesta a la crisis económica del 2008, la tecnología detrás de estos activos consiste en el uso de blockchain *y criptografía, por medio de una red descentralizada para que los usuarios de dichas redes puedan transferir libremente valor, utilizando criptomonedas o criptoactivos, sin la necesidad de acudir a un intermediario que centralice y registre todas las operaciones.*

El presente artículo aborda el estado actual de la tributación de criptomonedas y otros criptoactivos en el Perú tomando como punto de referencia un reciente trabajo de la OCDE.

Palabras clave: Criptomonedas; criptoactivos; tecnología de cadena de bloques; Impuesto a la Renta; Impuesto General a las Ventas.

* Abogado. Asociado del Estudio Rodrigo, Elías & Medrano Abogados (Lima, Perú). Contacto: mlarosa@estudiorodrigo.com

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 13 de enero de 2021, y aceptado por el mismo el 17 de mayo de 2021.

I. INTRODUCCIÓN

A enero de 2021, existen 8,257 criptomonedas cuya capitalización total de mercado asciende a un billón de dólares americanos, siendo Bitcoin la que lidera el referido mercado al representar el 69% de dicho valor (CoinMarketCap, 2021). Las criptomonedas presentan una serie de dificultades para los legisladores a nivel global, toda vez que existen disparidades significativas entre las características y la funcionalidad económica de cada una de ellas respecto de las otras. Esta falta de uniformidad genera una serie de dificultades a los legisladores a nivel global, quienes se encuentran en la búsqueda de las mejores fórmulas legislativas para abordar las implicancias regulatorias y tributarias a las que deberían sujetarse esta nueva clase de activos.

En los últimos años, varias instituciones de índole regulatorio y administraciones tributarias de diversos Estados han emitido opiniones, guías y recomendaciones buscando describir las implicancias legales que pueden derivarse de estos nuevos activos.

En octubre de 2020, la Organización para la Cooperación y el Desarrollo Económicos (en adelante, OCDE) preparó el documento denominado Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues[1] para la reunión de los ministros de economía y gobernadores de los bancos centrales de los países pertenecientes al G20. Este documento abarca un análisis comprensivo de los riesgos que presentan las criptomonedas y otros criptoactivos, así como las medidas que, a la fecha, más de cincuenta Estados han adoptado respecto de las implicancias tributarias aplicables a este tipo de activos.

En el presente artículo, se analizarán las últimas y más relevantes aproximaciones de índole tributario que diversos Estados han adoptado con relación a las criptomonedas y otros criptoactivos, a fin de describir los posibles regímenes tributarios que, eventualmente, podrían ser introducidos en la legislación peruana, así como detallar una serie de advertencias y recomendaciones que debiera tomar en cuenta el legislador al momento de recoger o diseñar el régimen correspondiente.

II. ORIGEN Y CARACTERIZACIÓN DE LAS CRIPTOMONEDAS Y CRIPTOACTIVOS

A. Origen y modalidades de creación de nuevas criptomonedas y criptoactivos

En la actualidad, las transacciones financieras requieren de un intermediario que pueda ejecutar la operación por instrucción de sus clientes y, en paralelo, mantener el registro de todas las transacciones que se realizan a través de su institución. A través del sistema financiero tradicional, las instituciones bancarias son las encargadas de mantener el registro de dichas transacciones y son quienes garantizan que la información derivada de las mismas sea certera y se mantenga segura.

Los que apoyan el surgimiento de las criptomonedas y otros criptoactivos sostienen que los referidos intermediarios financieros tradicionales presentan una serie de inconvenientes que pueden desincentivar que un segmento de la población acceda a servicios financieros. Dichos inconvenientes, principalmente, serían los siguientes: (i) distribución injusta del valor; (ii) comisiones que encarecen las transacciones financieras; (iii) limitaciones a la movilidad del capital; (iv) los intermediarios actúan como *gatekeepers,* toda vez que tienen la capacidad de prevenir la participación de actores en el sistema financiero; y (v) limitaciones a la privacidad personal de los clientes frente a los intermediarios.

Ante ello, y luego de la crisis económica del año 2008, en el artículo denominado Bitcoin: A Peer-to-Peer Electronic Cash System se propuso un sistema de dinero electrónico que funcionaría de persona a persona –es decir, para que opere como una suerte de dinero privado– sin la participación de intermediarios (Nakamoto, 2008). Con ello se propuso instaurar un sistema que permitiría la realización de transferencias financieras sin que se incurran en costos de intermediación, ni que haya intromisiones o limitaciones impuestas por los intermediarios u otros terceros, tales como aquellas provenientes de los bancos centrales y otras instituciones públicas.

En el 2009, se lanzó la primera criptomoneda del mundo, Bitcoin, que se basaría en la primera aplicación a gran escala de la tecnología de cadena de bloques (*blockchain*)[2] en el mundo real. Así, dicha

[1] Resulta de suma importancia destacar que la propia OCDE ha descrito que este documento constituye uno de investigación y, como tal, no constituye una guía ni sugerencia para efectos de la adopción de medidas legislativas concretas por aquellos Estados que aún desean introducir normas vinculadas a esta nueva clase de activos.

[2] Según señalan Houben y Snyers (2018, p. 15), una cadena de bloques es un tipo particular de estructura de datos utilizada en algunos registros descentralizados que almacenan y transmiten datos en paquetes denominados "bloques",

cadena de bloques es una subcategoría del concepto de red descentralizada, la cual depende de un registro descentralizado (*distributed ledger technology),* que es definido como

> […] a novel and fast-evolving approach to recording and sharing data across multiple data stores (ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes[3] (Banco Mundial, 2017, p. 1)[4].

Como se puede apreciar, la referida tecnología permite que las transacciones y los datos se registren y sean compartidos de manera sincronizada y descentralizada, a través de los partícipes de la red (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2020). En ese sentido, cualquier modificación que se quiera realizar a la información que contiene la red únicamente podría ejecutarse si se cuenta, previamente, con la autorización y el consenso de una mayoría de sus partícipes. En otras palabras, nadie tiene las facultades para modificar los datos recogidos en la red, ni siquiera instituciones gubernamentales.

Con la introducción de nuevas criptomonedas y criptoactivos en los años posteriores al lanzamiento de Bitcoin, se establecieron nuevos mecanismos de consenso para realizar la validación de operaciones y transacciones que se canalizan a través del registro descentralizado.

La descripción de estos nuevos mecanismos de consenso[5] es de suma importancia, puesto que demuestran las características operativas de las redes y cómo se retribuye –mediante la creación y entrega de criptomonedas o criptoactivos– a los validadores que participan en dichas redes, ello a fin de que dichos partícipes tengan incentivos económicos para destinar recursos a estas cadenas de bloques (Massachusetts Institute of Technology, 2018).

Tal y como indica la OCDE[6] (2020), los mecanismos de consenso más comunes son los siguientes:

a) **Sistema de comprobación vía trabajo *(proof of work system)*:** basado en ecuaciones matemáticas, típicamente difíciles de resolver, pero cuya comprobación puede ser fácilmente verificada. Para resolver las referidas ecuaciones los validadores utilizan recursos computacionales que, para su adecuada operatividad, requieren de un alto consumo de electricidad.

---

los cuales se encuentran interconectados en una cadena digital. Este tipo de tecnología utiliza métodos de criptografía y algoritmos para que se registre dicha información en los bloques mencionados y dicha información se encuentre sincronizada a lo largo de toda la red, gozando la misma de inmutabilidad.

3 En la literatura especializada se define a los nodos como "[m]embers or systems of a consensus network or a server that holds a replicated copy of the ledger and can have varying roles: to issue, verify, receive, inform, etc. For all intents and purposes, a node can be a virtual machine (VM) instance" (Seibold & Samman, 2016, p. 1).

Traducción libre: "miembros o sistemas de una red consensuada o un servidor que mantiene una copia replicada del registro y puede tener diversos roles: emitir, verificar, recibir, informar, entre otros. Para todos los propósitos, un nodo es una máquina virtual".

4 Traducción libre:

> […] un enfoque novedoso y de rápida evolución para registrar y compartir datos a través de diversos almacenes de datos (registros), que cada uno cuenta con exactamente los mismos registros de los datos y que son colectivamente mantenidos y controlados por una red descentralizada de servidores informáticos, que se denominan nodos.

5 Seibold y Samman (2016) definen los mecanismos de consenso de la siguiente manera:

> A method of authenticating and validating a value or a transaction on a Blockchain or a distributed ledger without the need to trust or rely on a central authority. Consensus mechanisms are central to the functioning of any blockchain or distributed ledger […]. In distributed ledgers, a consensus mechanism is the way in which a majority (or, in some mechanisms, all) of network members agree on the value of a piece of data or a proposed transaction, which updates the ledger. In other words, a consensus mechanism is a set of rules and procedures that maintains a coherent set of facts among the participating nodes (pp. 1-3).
>
> Traducción libre:
>
> Un método de autenticación y validación de valor o transacciones en una cadena de bloques o una red descentralizada sin que se requiera confiar o depender de una autoridad centralizada. Los mecanismos de consenso son centrales a la operatividad de cualquier cadena de bloques o red descentralizada […]. En registros descentralizados, un mecanismo de consenso es la forma en que una mayoría (o en algunos mecanismos, todos) perteneciente a una red acuerda en el valor de una parte de la información –data– o respecto de una transacción propuesta, que luego es actualizada al registro. En otras palabras, un mecanismo de consenso es un conjunto de reglas y procedimientos que mantienen un orden coherente de hechos entre los nodos participantes (pp. 1-3).

6 Existen otros mecanismos de consenso no tan comunes como, por ejemplo, *proof of history,* inherente a la plataforma de Solana o el *proof of authority,* utilizado por la plataforma de VeChain, entre otros. Es más, existen sistemas híbridos que reúnen características de los sistemas de consenso que actualmente se vienen utilizando. Sin embargo, consideramos que su análisis excedería el propósito de este trabajo.

Así, los validadores o mineros *(miners)* utilizan sus computadoras para mantener actualizado el registro descentralizado y, a cambio, reciben como compensación monedas digitales recién creadas, pudiendo obtener, además, comisiones por el registro de transacciones al bloque (Van Adrichem, 2019).

No obstante, el referido esfuerzo se realiza en un contexto competitivo en el que cada validador debe competir contra los otros mineros, ya que cada validación completada resulta en el pago al primer validador de (i) nuevas criptomonedas o criptoactivos, y/o (ii) una comisión por la validación de la transacción, equivalente a un porcentaje del valor de la operación procesada, que es descontada de la propia transferencia.

b) **Sistema de comprobación vía participación *(proof of stake system)*:** reconoce derechos de validación a los usuarios-forjadores según la cantidad de criptomonedas o criptoactivos asignados a la red de bloques. En estos sistemas, los validadores son denominados forjadores o partícipes (*forgers o stakers)*.

Así, la participación se mide según la cantidad de criptomonedas o criptoactivos de titularidad del forjador, el período de tenencia de estos y la cantidad de activos que se asignan en la cadena de bloques, como si se tratara de una suerte de garantía de depósito, similar a la figura del *escrow*.

En ese sentido, se requiere a los forjadores que asignen una cantidad mínima en la cadena de bloques para que puedan participar en el proceso de validación. En otras palabras, estos partícipes, al asignar sus criptomonedas o criptoactivos para gozar del derecho a validar transacciones, tienen la posibilidad de recibir –como contraprestación– nuevas criptomonedas o criptoactivos como consecuencia del proceso de validación.

Ahora bien, existen otras modalidades por las cuales un usuario puede adquirir criptomonedas o criptoactivos recién creadas, las que describimos a continuación:

a) ***Airdrop*:** consiste en una forma en que se distribuyen y otorgan nuevas criptomonedas o criptoactivos a título gratuito a favor de los usuarios. Cabe destacar que, quienes adquieren dichos activos no pagan precio alguno como contraprestación a favor de un tercero. Típicamente, esta modalidad de creación se utiliza para popularizar la existencia de este tipo de activos en determinadas comunidades y para incrementar las condiciones de liquidez en las etapas iniciales de nuevos proyectos (Van Adrichem, 2019).

Sin embargo, existen situaciones particulares en que se ejecutan *airdrops*, otorgándose nuevas criptomonedas a los usuarios que participan en una red determinada, en el marco de una bifurcación dura *(hard fork)* que lo precede[7]. En términos del Internal Revenue Service de Estados Unidos de América: "A hard fork is unique to distributed ledger technology and occurs when a cryptocurrency on a distributed ledger undergoes a protocol change resulting in a permanent diversion from the legacy or existing distributed ledger" (2019, p. 2)[8].

Los *hard fork* conllevan la división de una red sobre la que opera una moneda digital para crear una segunda moneda que opera en paralelo a la original. Así, los titulares de la moneda digital original recibirían, como resultado de un *hard fork*, una moneda digital nueva, sin que dicho titular tenga que efectuar pago de precio alguno.

b) **Oferta primaria de monedas o *initial coin offering*** (en adelante, ICO): consiste en la emisión de nuevas criptomonedas o criptoactivos, por entidades específicas, sin que medie los procesos de validación antes descritos y, típicamente, se entregan a cambio de otros activos de este tipo o contra la entrega de divisas tradicionales.

B. Caracterización de las criptomonedas y criptoactivos

La cuestión de mayor relevancia para efectos de identificar el tratamiento tributario ideal para abordar las criptomonedas y criptoactivos, es la

[7] Cabe destacar que, mediante las bifurcaciones blandas (*soft forks*), también se actualiza el protocolo utilizado por los usuarios, pero, como dicha actualización debe ser adoptada por todos los miembros, no se crea ni entrega una nueva criptomoneda o criptoactivo a favor de los partícipes.

[8] Traducción libre:

> La referida bifurcación es inherente y única a la tecnología de registro descentralizado y solo acontece cuando el protocolo de una criptomoneda o criptoactivo es sometido a una modificación que resulta en una desviación del registro descentralizado original o legado.

identificación de las características y naturaleza de cada uno de estos activos (Cipek, 2020). Dicha labor es sumamente compleja puesto que, si bien las criptomonedas y criptoactivos guardan determinadas similitudes (se basan en tecnología de cadena de bloques y criptografía), también cuentan con diferencias sustanciales que dificultan una clasificación unitaria para este nuevo grupo de activos.

En términos generales, la categoría de criptoactivos abarca todos los activos que se almacenan en registros descentralizados y, como tal, subsume el concepto de criptomonedas, así como también aquellos activos identificados y aludidos como ilíquidos como, por ejemplo, los *security tokens* y *utility tokens*.

Son diversas las clasificaciones que han surgido a lo largo de los últimos años y que han sido utilizadas por las autoridades regulatorias y tributarias de alrededor del mundo. Ello se ha dado en un contexto en el que dichas instituciones han considerado que esta nueva clase de activos debían sujetarse a un marco legal general –sin reglas específicas para abordar las particularidades que se asocian a estas– lo cual ha ocurrido tanto en el ámbito regulatorio como en el tributario.

En cuanto al marco tributario aplicable a este tipo de activos, una calificación previa por parte de las autoridades regulatorias ha tendido a facilitar dicha labor para las administraciones tributarias. Desafortunadamente, como ya ha sido advertido por la doctrina (OCDE, 2020), parecería que dichas calificaciones se han dado tomando en consideración únicamente las características y naturaleza referida a Bitcoin, lo cual, ciertamente, puede llevar a la adopción de regímenes tributarios inapropiados para abordar otras criptomonedas o criptoactivos.

Sin perjuicio de ello, tal y como indica la OCDE (2020), los reguladores e investigadores han estado clasificando estos activos, según su función económica, en tres categorías principales:

a) ***Payment tokens* (monedas digitales):** Pueden utilizarse como medios de pago para que sus titulares puedan adquirir bienes y servicios, aunque también resulta factible que este tipo de activos puedan servir como una representación que permita almacenar un valor hasta operar como una unidad de medida referencial.

b) ***Security tokens:*** Se han diseñado para que se comporten como activos tradicionales que son mantenidos por inversionistas para gozar de una apreciación futura o, incluso, de recibir un rédito. Se podrían asemejar a valores mobiliarios siempre y cuando sean considerados como tales bajo la legislación correspondiente.

c) ***Utility tokens*:** Su funcionalidad consiste en que puedan utilizarse para facilitar el intercambio o el acceso del público a determinados bienes o servicios, que son ofrecidos por plataformas específicas.

Sobre el particular, este trabajo se ceñirá al tratamiento tributario de las monedas digitales, concepto que abarca la mayor cantidad de criptomonedas circulantes, y cuyas características son las que pueden ocasionar mayor dificultad al momento de realizar su calificación tributaria. Nótese que, en el caso estricto de los *security tokens*, si un criptoactivo se encontrara bajo esta definición, su clasificación, conceptualmente, no debería ser tan compleja, puesto que se le debería extender el tratamiento aplicable a los valores mobiliarios tradicionales (previa modificación legislativa que los considere como tales). Asimismo, en el caso de *utility tokens*, de operar y encontrarse estructuradas de la forma antes descrita, su tratamiento regulatorio y tributario, al menos teóricamente, debiera ser equiparado al trato que reciben las operaciones de intercambio de divisas tradicionales.

Sin perjuicio de ello, existen monedas digitales que podrían reunir características de cada una de las clasificaciones descritas. En ese caso, se deberá efectuar un análisis minucioso a fin de identificar el tratamiento regulatorio y tributario correspondiente.

Ahora bien, auditoras contables, a nivel internacional, han analizado la clasificación contable de este nuevo tipo de activos, remitiéndose a las disposiciones generales de las normas contables, toda vez que no existe norma alguna ni lineamiento específico que aborde la calificación de estos. Así, según los principios contables generales, la clasificación de los activos debe efectuarse en función a sus propiedades económicas. Además, una clasificación adecuada del activo requerirá la verificación del propósito económico, los derechos y obligaciones asociados al activo, y la manera en que el valor intrínseco se forma (OCDE, 2020)[9].

[9] Según la OCDE (2020, p. 15):

> Different types of tokens will require a different type of classification for accounting purposes and tax purposes. For example, a security token, which provides the owner with a contractual right to cash or another financial asset, could

En la actualidad, la mayoría de los Estados consideran a las monedas digitales como una modalidad de propiedad para efectos tributarios (OCDE, 2020). Como hemos venido señalando, la agrupación de todas las monedas digitales bajo una misma clasificación puede ocasionar problemas sustanciales en un futuro y, por tanto, este tipo de aproximaciones debe ser constantemente evaluada y modificada cuando corresponda.

Así, al no existir consenso a nivel global respecto de la caracterización de estos activos, existen Estados que han optado por considerarlos como activos intangibles, mientras otros, de manera minoritaria, los han calificado como *commodities* o instrumentos financieros (OCDE, 2020)[10]. Por lo tanto, cualquiera de las clasificaciones descritas puede resultar aplicable y acertada, pero ello dependerá de la moneda digital que se esté analizando. Ciertamente, pretender extender una clasificación absoluta sobre una moneda digital u otra será más complejo en aquellos casos en el que dicho activo reúna características de más de una de las clasificaciones identificadas, al tratarse de una suerte de híbrido.

En ese contexto, en la siguiente sección se describirá las principales implicancias tributarias que han sido extendidas a las monedas digitales (excluyendo de dicho análisis a las *security* y *utility tokens,* puesto que, como se ha señalado, su clasificación para propósitos tributarios debiera resultar más sencilla, ya que, conceptualmente, las características de estos tipos de monedas digitales se asemejan a las de los valores mobiliarios y divisas tradicionales, respectivamente).

III. ANÁLISIS DESCRIPTIVO REALIZADO POR LA OCDE: TRIBUTACIÓN DE MONEDAS DIGITALES

La OCDE (2020) al realizar la investigación sobre esta materia identificó que, en la actualidad, algunas de las diversas jurisdicciones participantes han determinado el tratamiento tributario aplicable a las monedas digitales en función a cada una de las distintas operaciones que pueden darse con esta clase de activos. Las distintas operaciones que se detallaran en este apartado pueden ser divididas en dos categorías: originarias y secundarias. Las primeras consisten en aquellas operaciones que originan la adquisición de monedas digitales recién creadas. En cambio, las secundarias consisten en la adquisición de monedas digitales que son transferidas por terceros, generalmente, mediante la compraventa.

Cabe indicar que, en términos generales, los Estados que han participado en este estudio, consideran que las monedas digitales son activos respecto de los cuales los titulares ostentan derechos de propiedad y, en ese contexto, serían susceptibles de recibir un tratamiento equiparable al de otros activos de características similares (OCDE, 2020).

A. Tratamiento tributario vinculado al otorgamiento de monedas digitales recién creadas

Como se ha señalado, las monedas digitales pueden originarse de diversas maneras, siendo en función a las modalidades de adquisición primaria de estos activos que instituciones gubernamentales de varios Estados han establecido las implicancias tributarias que resultarían aplicables en estas etapas iniciales, las cuales describimos a continuación:

1. Minería

Los mineros crean bloques digitales a través de la solución de problemas matemáticos (algoritmos), sirviéndose únicamente de las capacidades computacionales de sus ordenadores (Bergman, 2018). Se trata de una actividad automatizada, sin una intervención humana relevante para efectos de la resolución de los algoritmos.

Ciertamente, el proceso para mantener el registro descentralizado requiere de recursos computacionales de dicho minero y, como tal, este incurre

be considered as a financial asset subject to International Financial Reporting Standards (IFRS) 9 (PWC, 2019); while utility tokens, which represent a right to receive future goods or services, can be considered as a prepayment for those goods and services, and could therefore be treated as such under IFRS 15 (KPMG, 2019).

Traducción libre:

Diferentes tipos de monedas requerirán distintos tipos de clasificaciones para propósitos contables y tributarios. Por ejemplo, un *security token*, que proporciona a su titular derechos contractuales a solicitar efectivo u otro activo financiero, pueden ser considerados como un 'activo financiero' comprendido por la Norma Internacional de Información Financiera 9; mientras que los *utility tokens*, que representan un derecho a recibir un bien o servicio futuro, pueden ser considerados como un pago anticipado por la adquisición de dichos bienes y servicios, y como tales pueden ser tratados bajo la Norma Internacional de Información Financiera 15.

[10] Apartándose de dichos criterios de interpretación, se tiene a Italia que ha equiparado a las criptomonedas como si fueran divisas extranjeras, mientras que, por otro lado, se tiene a Polonia que las ha considerado como una representación de valor digital.

en costos de mantenimiento, electricidad, ventilación, enfriamiento, así como en costos para la adquisición de los equipos de procesamiento de datos necesarios para que dichos ordenadores operen adecuadamente. A cambio de ello, y una vez que las computadoras hayan validado los bloques, el validador recibe como contraprestación una moneda digital recién creada y, en algunos casos, recibirá comisiones representadas por divisas tradicionales, dependiendo de la cadena bloques sobre la que esté operando, como resultado de anotar transacciones que se realicen a través de la red.

a. *Personas jurídicas*

En la actualidad, la minería es principalmente realizada por empresas y, así, el tratamiento tributario aplicable es más fácil de identificar puesto que las monedas digitales que reciban se encontrarían sujetas al impuesto a la renta corporativo. Ciertamente, los gastos y costos asociados a la obtención de dichas monedas digitales serían deducibles para determinar la base imponible del impuesto, toda vez que dichos egresos estarían destinados a la obtención de rentas gravadas (OCDE, 2020).

Sin perjuicio de lo indicado, algunos Estados consideran que cuando una empresa recibe una moneda digital como resultado de la minería, esta operación se encuentra fuera del ámbito de aplicación del impuesto a la renta corporativo[11]. Dicha línea argumentativa se basa en que la obtención originaria de la moneda digital califica como un evento no comprendido por sus legislaciones del impuesto a la renta y que el evento gravable recién se verificaría con ocasión a la futura enajenación de dicho activo.

Ahora bien, en cuanto al impuesto al valor agregado (en adelante, IVA), existen dos posiciones que han surgido con relación a los alcances de la Directiva del IVA (Directiva 2006/112/CE, 2006) de la Unión Europea, con relación al tratamiento aplicable a la adquisición de monedas digitales vía la realización de las operaciones de minería:

- **Primera posición**: La adquisición de monedas digitales vía la realización de las operaciones de minería estaría fuera del ámbito de aplicación del impuesto. Ello debido a que no se apreciaría una relación directa entre la prestación del servicio de verificación y el pago de una retribución por parte de un usuario específico a favor de un proveedor determinado[12]. En otras palabras, el hecho que un validador efectúe estos servicios a favor de los usuarios de la cadena de bloques no siempre conlleva al pago de una retribución por parte del usuario que ha gozado de dicho servicio; o,

- **Segunda posición**: Las operaciones de minería califican como servicios gravados con el impuesto, puesto que el minero realiza actividades de validación, en términos generales, a favor de usuarios que realizan transacciones que deben registrarse en la cadena de bloques[13].

Como se puede apreciar, actualmente existen posiciones distintas a nivel de la Unión Europea que pueden llevar a tratamientos opuestos respecto de una misma operación de minería, dependiendo el régimen fiscal aplicable de la jurisdicción donde se encuentre el minero.

b. *Personas naturales*

La minería de monedas digitales puede fácilmente ser realizada por personas naturales, las que solo requieren de un local, computadora, luz e internet. Una vez implementado dicho sistema, con la simple instalación de un programa informático o accediendo a proveedores que centralizan el servicio, el validador puede iniciar el minado de nuevas monedas digitales.

A nivel internacional, se suele distinguir entre aquellas personas naturales que realizan esta actividad de manera esporádica, de aquellas otras que lo hacen con fines comerciales o empresariales. En este último caso, el tratamiento tributario debiera ser el mismo que aquel descrito para el caso de empresas.

No obstante, más problemático es el caso de aquellas personas naturales que califican como no habituales en la actividad de minería de monedas digitales. Existen legislaciones que han considerado

[11] Según la OCDE (2020), los Estados que han adoptado esta posición serían Croacia, Dinamarca, Eslovaquia, Estonia, Francia, Letonia, Lituania, Polonia, República Checa y Singapur.

[12] Los Estados que seguirían esta posición son Alemania, Eslovenia, Irlanda y Suecia.

[13] De acuerdo con la OCDE (2020), se tienen posiciones que sostienen que los referidos servicios de validación pueden encontrarse exentos de este impuesto bajo las siguientes premisas: (i) Si es que se puede considerar que estas operaciones se encuentran directamente vinculadas con 'divisas' bajo el numeral (1)(e) del artículo 135 de la Directiva; o (ii) si se sostiene que estas actividades sirven como funciones esenciales de una actividad exenta (transferencia de monedas digitales), ello en función a lo dispuesto en el numeral (1)(d) del artículo 135 de la Directiva.

que las monedas digitales recibidas por este tipo de personas naturales deben ser tratadas como rentas derivadas de la prestación de servicios independientes y, como tal, gravadas conforme a las reglas del impuesto a la renta aplicables a este tipo de rentas, es decir, derivadas de la prestación de servicios[14]. Algunos de los Estados que han adoptado esta posición permiten el reconocimiento de los incurridos para obtener la renta neta gravada con el impuesto a la renta.

Cabe destacar que, por ejemplo, la administración tributaria de Noruega ha considerado que la renta en estos escenarios se determina en función al valor de mercado de la moneda digital a la fecha en que el minero recibe la moneda extraída (Skatteetaten, s/f). A su vez, dicho valor de mercado constituiría el costo computable del minero sobre la moneda digital que ha recibido.

Por su parte, otros Estados consideran que la entrega de nuevas monedas digitales en los supuestos de minería, a personas naturales no habituales, constituye un beneficio que se encuentra fuera del ámbito de aplicación de del impuesto (OCDE, 2020). Como se indica más adelante, los Estados que han adoptado esta posición consideran que el primer evento gravado con el impuesto se verificará cuando se enajenen las monedas digitales a terceros.

En el caso de personas naturales no habituales, el tratamiento adoptado mayoritariamente por los Estados consiste en considerar que las actividades de minería no constituyen un evento gravado con el IVA, ya que para propósitos de la estructura técnica de este impuesto, no se estaría realizando la operación de minado en el marco del desarrollo de una actividad empresarial (es decir, desde un punto de vista teórico, la hipótesis de incidencia del impuesto no se verificaría) (Skatteetaten, s/f).

2. *Forging* o *staking*

Como se ha indicado, a diferencia de la minería, el *forging o staking* depende de un sistema, denominado *proof of stake,* que requiere del validador que asigne una cantidad determinada de unidades de una moneda digital particular por un período específico. Posteriormente, el sistema elige parcialmente, al azar, entre todos los participantes de la red, quién será considerado como el creador de un bloque determinado (Bergman, 2018). Así, la idea detrás de este sistema consiste en incentivar –mediante la entrega de monedas digitales– a aquellos validadores que han designado al proceso de validación, la mayor cantidad de este tipo de activos, pues las unidades que les serán pagadas son proporcionales a la cantidad de activos inmovilizados (*staked*).

Existen quienes asimilan esta figura a la de las cuentas de depósito en garantía (o *escrows*), toda vez que, si el sujeto validase una transacción fraudulenta, aquel podría perder sus monedas digitales e, incluso, ser sancionado, impidiéndosele participar como validador en dicha red (Bergman, 2018). En este sentido, este sistema buscaría incentivar a estos sujetos para que únicamente validen aquellas operaciones que resultan propias y reales pues, de lo contrario, podrían asumir un gran perjuicio económico (Bergman, 2018).

Cabe mencionar que no todos los modelos de *staking* implican que el validador asuma un riesgo respecto de las monedas digitales que le otorgan el derecho a participar en una red como validador, toda vez que, en algunos de estos esquemas, bastará que el titular cuente con una cantidad determinada de monedas digitales para participar, sin que deba asignarlas en garantía.

Se debe indicar que, sobre este método de creación de monedas digitales, existen escazas fuentes académicas que hayan analizado y desarrollado su tratamiento. Sin embargo, la administración tributaria de Finlandia ha señalado que estas operaciones generan, para fines tributarios, un rendimiento de activos existentes, sujeto al régimen de ganancias de capital, verificándose el hecho imponible en el momento en que el validador adquiere el control de la nueva moneda. Bajo esta posición,

[14] Esta sería la actual posición del Internal Revenue Service de los Estados Unidos de América que, a través del Notice 2014-21, estableció lo siguiente:

> If a taxpayer's "mining" of virtual currency constitutes a trade or business, and the "mining" activity is not undertaken by the taxpayer as an employee, the net earnings from self-employment (generally, gross income derived from carrying on a trade or business less allowable deductions) resulting from those activities constitute selfemployment income and are subject to the self-employment tax (2014, p. 4).

Traducción libre:

> Si la minería de monedas digitales efectuada por un contribuyente deriva de un oficio o negocio y la actividad de ´minería´ realizada por el contribuyente en calidad de un empleado, los ingresos netos provenientes del trabajo independiente (generalmente, ingreso bruto obtenido por realizar un oficio o negocio descontando las deducciones permitidas) resultantes de dichas actividades, constituyen ingresos por la realización de actividades como independientes y, en ese sentido, se sujetan al impuesto a los trabajadores independientes.

el ingreso se asemejaría a una suerte de dividendo en especie (Veroskatt, 2020).

Sin perjuicio de lo anterior, existen quienes consideran que este ingreso podría ser considerado como una comisión por validar transacciones derivadas de una actividad similar a la minería (Bergman, 2018). Esta última posición sería la que ha adoptado la Administración Tributaria de Australia, al tratar a las monedas digitales recibidas en estos casos como ingresos ordinarios (Australian Taxation Office, 2020).

En el caso de personas jurídicas, sea que las monedas digitales sean asimiladas a un dividendo en especie o un ingreso proveniente de una actividad empresarial, dichas rentas estarán gravadas con el impuesto a la renta. Sin embargo, la calificación de la renta bajo una u otra teoría podría conllevar la aplicación de distintas reglas determinativas de la renta, como es el de aquellas relativas a las deducciones, créditos, entre otras disposiciones específicas que se deberá analizar en cada jurisdicción[15].

Es evidente que, en el caso de Australia, la administración tributaria ha considerado que las monedas digitales recibidas por el *forger,* persona natural, constituyen ingresos ordinarios sujetos al impuesto a la renta. La renta se determinaría según el valor de mercado de las monedas recibidas, el que pasaría a representar para el contribuyente el costo computable que pasará a tener sobre dichos activos.

3. *Airdrops*

En los *airdrops*, el emisor, sin recibir contraprestación alguna, otorga monedas digitales a varios miembros de la comunidad en función a diversos criterios. Por ejemplo, bajo esta modalidad se suele otorgar monedas digitales a aquellos usuarios que cuentan con una cantidad determinada de otras monedas digitales. También se ha entregado monedas digitales a usuarios que han enlazado la información de sus cuentas de redes sociales con las del emisor (con el propósito de promocionar una moneda digital en particular). Nótese que el otorgamiento de monedas digitales en estos casos tiene lugar a título gratuito; es decir, el emisor no recibe contraprestación alguna a cambio de las monedas que entrega (Van Adrichem, 2019).

Existen dos posiciones respecto del tratamiento tributario que corresponde a los *airdrops:*

- **Primera posición**: la administración tributaria de los Estados Unidos de América ha considerado que las monedas digitales entregadas en el marco de un *airdrop* tributan como un ingreso ordinario, pero, únicamente, a partir del momento en que se adquiere el dominio y control sobre las monedas digitales, no así antes (Chandrasekera, 2020). En otras palabras, el hecho imponible se verifica cuando el usuario cuenta con todas las facultades para poder disponer de la moneda digital (US Internal Revenue Services, 2019).

- **Segunda posición**: la administración tributaria del Reino Unido ha considerado que las monedas digitales entregadas en el marco de un *airdrop* no constituirán renta gravada con el impuesto cuando: (i) el usuario no preste servicio alguno a cambio de la moneda o (ii) la obtención de las monedas se deba a razones ajenas a un oficio o actividad empresarial (HM Revenue & Customs, 2019).

Ciertamente, si una persona jurídica fuera a obtener monedas digitales a título gratuito, es probable que las legislaciones de los diversos Estados consideren que dicho beneficio constituye una renta gravable. En cambio, en el caso de personas naturales, tenemos el caso del Reino Unido que lo ha considerado como un ingreso inafecto, siempre que el adquirente efectivamente los reciba a título gratuito.

Por su parte, se debe indicar que los Estados aún tienen por definir si es que existen implicancias en el IVA con relación a los *airdrops* de monedas digitales.

4. Oferta primaria de monedas

Como se ha indicado, en un ICO el emisor cuenta con parte o el total de las monedas digitales que serán posteriormente vendidas al público (Van Adrichem, 2019). La adquisición de monedas digitales en el marco de los ICO puede realizarse contra la entrega (en pago) de otras monedas digitales o a cambio de una divisa tradicional. Para algunos autores, un ICO se asemeja a una oferta pública primaria de valores mobiliarios, puesto que ambos se utilizan para que una sociedad obtenga fondos para la realización de sus actividades (Chester, 2017).

En cuanto al tratamiento tributario aplicable, parecería que los Estados han venido tratando

[15] Por su parte, a la fecha de elaboración de este trabajo, no se cuenta con una literatura académica que analice el tratamiento de estas actividades en el ámbito del IVA.

este tipo de operaciones como una enajenación de monedas digitales por parte del emisor a un tercero y, como tal, dicho tratamiento podría implicar que el emisor deba reconocer en dicha oportunidad una ganancia de capital gravada con el impuesto a la renta.

B. Tratamiento tributario de la enajenación de monedas digitales

La mayoría de los Estados que han participado en el trabajo de investigación de la OCDE consideran que la enajenación de monedas digitales constituye un hecho imponible gravado con el impuesto a la renta. La OCDE ha identificado que el tratamiento tributario podría variar en función al motivo por el cual se realiza la enajenación de la moneda digital; es decir, si la misma se transfiere a cambio de una divisa tradicional, otra moneda digital, o se paga como contraprestación por la adquisición de un bien o un servicio (OCDE, 2020).

Por su parte, existen algunos Estados que consideran que la enajenación de monedas digitales efectuada por personas naturales no constituye un hecho imponible gravado con el impuesto a la renta (OCDE, 2020). En ese contexto, la administración tributaria de Portugal ha concluido que el intercambio de monedas digitales no constituye un evento susceptible de generar renta gravada, ya que la referida operación no se encuentra comprendida dentro de la definición de rentas susceptibles de producir ganancias de capital o rentas derivadas del capital (Informação Vinculativa 5717/2015, 2015). Sin perjuicio de ello, dicha administración ha señalado que, si la moneda digital es entregada como contraprestación por una actividad profesional o empresarial, el tratamiento tributario variaría (es decir, se generaría renta gravada con el impuesto a la renta).

La administración tributaria de Italia ha considerado que la permuta de monedas digitales por personas naturales constituye una operación, por lo general, no sujeta al impuesto a la renta (Risoluzione 72/E, 2016). Sin perjuicio de ello, si es que la operación fuera a calificar como especulativa, el tratamiento tributario sería distinto, equiparando este tipo de operaciones a un intercambio entre divisas tradicionales. Se considera que, para dichos propósitos, una operación califica como especulativa si es que: (i) en un ejercicio fiscal, y (ii) durante siete días consecutivos, el valor de las monedas digitales que son de titularidad del usuario supera la suma de € 51 000, aproximadamente. Asimismo, podría originarse un evento gravado si es que el titular enajena monedas digitales durante siete días consecutivos, cuyas operaciones resultan en una generación de ingresos que superan, aproximadamente, la suma antes indicada.

Tal y como señala la OCDE, el que los Estados hayan optado por no gravar con el impuesto a la renta los ingresos que puedan derivarse del intercambio de monedas digitales, se debe a diversas razones. Una de ellas consistiría en una posición pragmática para evitar las complejidades asociadas a la determinación del valor de mercado (al tener que comparar estos activos con divisas tradicionales, qué tipo de cambio debería utilizarse, etc.), dado que ello puede ser sumamente complejo en operaciones de intercambio que involucran distintas monedas digitales (OCDE, 2020). Otra razón que indica sería que diversos Estados están adoptando como estrategia una postura de esperar y mirar *(wait and see approach)* para incentivar a sus ciudadanos a continuar invirtiendo en esta nueva clase de activos.

En este contexto, es evidente que la enajenación de monedas digitales realizada por personas jurídicas, generalmente, será considerada como una operación susceptible de generar ganancia de capital gravada con el impuesto, siendo factible el reconocimiento del costo computable asociado a las mismas a fin de determinar la renta neta sobre la cual aplicará el impuesto.

En cambio, en el caso de personas naturales que transfieren monedas digitales, parecería que la posición actual consiste en, primero, determinar las razones que originan la operación de transferencia (por ejemplo, si se transfiere a cambio de una divisa tradicional, por otra moneda digital, o se recibe como contraprestación por la adquisición de un bien o un servicio) y, a partir de ello, establecer el tratamiento tributario aplicable.

Por su parte, en cuanto al IVA que podría resultar aplicable en la enajenación de monedas digitales (sea por personas jurídicas o naturales), parecería que los Estados, según la OCDE (2020), estarían considerando que estas operaciones se encuentran fuera del ámbito de aplicación del impuesto o exentas del mismo.

C. Problemática asociada a la determinación del valor de mercado y costo computable de las monedas digitales

Actualmente, el precio de las monedas digitales es altamente volátil. Dicha volatilidad en los precios dificulta la correcta determinación del valor de mercado de estos activos para efectos tributarios. Asimismo, dicha cuantificación resulta importante, tanto para los transferentes como para los adquirentes, siendo estos últimos quienes deberán

identificar el costo computable derivado de dichas adquisiciones. Dicho costo debería ascender al valor de mercado de dicha moneda digital a la fecha en que ha acontecido la operación (de compra o venta). Ello puede resultar complejo en mercados altamente volátiles, puesto que el precio de estos activos puede cambiar drásticamente en un mismo día.

La determinación del costo computable es aún más importante en aquellos escenarios de minería, *forging o staking,* o *airdrops*. Especialmente, en aquellas jurisdicciones que consideran que los usuarios que reciben las monedas digitales, en estas ocasiones, han generado un evento gravado.

Por su parte, también existen diversos criterios en cuanto a las reglas que deben resultar aplicables para identificar el costo computable de las monedas digitales que han sido adquiridas en diversas ocasiones (es decir, a diferentes precios de compra). Ello resulta de suma importancia, toda vez que la determinación de la base imponible sobre la cual aplicaría el impuesto a la renta en las posteriores enajenaciones, parciales o totales, debe permitir la correcta asignación del costo correspondiente a la parte de las monedas que se transfieren.

Cabe destacar que la OCDE ha descrito que es probable que la razón por la que algunos Estados han optado por no gravar las operaciones de intercambio de monedas digitales, es para evitar la problemática que puede surgir para determinar el valor de mercado correspondiente, el tipo de cambio a utilizar (toda vez que los Estados suelen exigir que la determinación de los hechos imponibles se realice en la divisa local), la asociación entre las pérdidas generadas por estas operaciones en determinados ejercicios y que susceptibles de compensarse con utilidades de otros ejercicios (en algunos Estados, el arrastre de pérdidas para la determinación de las rentas de personas naturales, suele tener ciertas limitaciones o, en todo caso, no se ha previsto un sistema como tal para este tipo de contribuyentes).

Por ejemplo, la administración tributaria de Singapur ha indicado –aunque únicamente para propósitos del Impuesto General a las Ventas (en adelante, IGV)– que, para efectos de la conversión a la divisa local, se podrá utilizar los tipos de cambios reportados por las casas de cambio de monedas digitales, cualquier proveedor que cuente con tipos de cambio sobre monedas digitales (se señala como ejemplos a Google Finance y Reuters), o, en caso no se pudiera obtener un tipo de cambio de dichas fuentes, se podrá utilizar el tipo de cambio acordado en cualquier acuerdo escrito entre el usuario y el proveedor de servicios o bienes (Inland Revenue Authority of Singapore, 2020).

El Internal Revenue Service de Estados Unidos (2014) ha seguido ese mismo razonamiento, al indicar que si una moneda digital se encuentra listada en un intercambio y el tipo de cambio se fija en función a la oferta y demanda del mercado, el valor de mercado de la moneda digital se determina mediante la conversión a dólares americanos a ese tipo de cambio, y que dicha metodología se emplee de una manera razonable a fin de que la misma sea consistente.

Por otro lado, en cuanto al costo computable de las monedas digitales que han sido adquiridas en diversas oportunidades también se tiene la posibilidad de adoptar distintas fórmulas legales para abordar el régimen aplicable. La administración tributaria de Finlandia ha extendido el tratamiento que corresponde a los activos tradicionales para abordar el caso de las monedas digitales (Veroskatt, 2020). Así, dicha legislación prevé, como regla general, un sistema de primeras entradas y primeras salidas (*first in, first out),* aunque a elección del contribuyente, quien podrá escoger, alternativamente, la posibilidad de acreditar el costo unitario. A su vez, dicha entidad ha indicado que, en los casos de transferencias de monedas digitales, las partes podrán utilizar el tipo de cambio de la fecha de transacción o el tipo de cambio acordado por las partes.

En este contexto, la alta volatilidad de las monedas digitales supone grandes retos para las administraciones tributarias a nivel global, ya que la determinación de la base imponible (tanto para el impuesto a la renta como para el IVA o general a los servicios, entre otros) dependerá de la posibilidad de cuantificar razonablemente el ingreso, precio y costo. Nótese que, todos los elementos antes mencionados resultan indispensables para identificar el aspecto cuantitativo de los tributos que resulten aplicables a las operaciones que involucran monedas digitales.

Por ello, resulta razonable que algunos Estados estén permitiendo que los inversionistas en monedas digitales utilicen valores de cotización reportados por las propias casas de cambio, y en caso dicho valor resulte complejo de identificar que se pueda utilizar alternativamente aquel que haya sido pactado por las partes (por ejemplo, existen monedas digitales que se entregan a inversionistas y a la fecha de dicho evento aún no cuentan con un valor de mercado porque se trata de un activo recién creado, por lo que, dicho valor recién se determinará cuando se permita transar con los mismos en el mercado).

IV. TRIBUTACIÓN DE LAS MONEDAS DIGITALES EN EL PERÚ[16]

En el Perú no existe una clasificación jurídica para abordar el tratamiento ni naturaleza de las monedas digitales. Tampoco existen pronunciamientos de las autoridades regulatorias ni tributarias con relación a dichos activos. Sin perjuicio de ello, tratándose de personas naturales, la Ley del Impuesto a la Renta (Decreto Legislativo 744, 1993) (en adelante, Ley del IR), ha previsto un régimen específico para determinar si la enajenación de un activo por parte de una persona natural puede originar una ganancia de capital gravada con dicho impuesto. Para tal efecto, dicho cuerpo normativo ha dispuesto una lista de activos específicos que pueden generar ganancias de capital gravadas, que incluye únicamente inmuebles y valores mobiliarios. Del mismo modo, se ha previsto un concepto abierto para los valores mobiliarios que podría resultar aplicable a algunas monedas digitales, como se describirá en los siguientes apartados.

Para efecto del presente análisis, resaltamos que la Ley del IR grava las ganancias obtenidas por personas naturales producto de la enajenación de valores mobiliarios. No obstante, la Ley no contiene una definición autónoma de 'valor mobiliario'. Debido a ello, existen quienes sostienen que correspondería realizar una remisión a la Ley de Títulos Valores (2000)[17] y la Ley de Mercado de Valores (1996)[18] para dotar de contenido al concepto de valores mobiliarios recogido en la Ley del IR, toda vez que esta norma carece de dicha tipificación.

No obstante, una remisión a dichos cuerpos normativos para brindarle contenido al concepto de valor mobiliario recogido en la Ley del IR, bajo una interpretación restrictiva, puede ocasionar una problemática toda vez que dichas normas se han diseñado tomando en consideración valores mobiliarios desde la óptica de emisores peruanos. Por ende, sostener una línea argumentativa en ese sentido, para efectos tributarios, podría conllevar a que se pretenda sostener que los valores mobiliarios emitidos por entidades extranjeras no se encontrarían comprendidos bajo dicha clasificación. A su vez, ello implicaría, vía interpretativa, una exclusión de los valores extranjeros del ámbito de aplicación de impuesto a la renta de personas naturales.

Si bien no hay un desarrollo jurisprudencial ni legislativo sobre la materia, y al menos hasta que se opte por alguna de dichas alternativas (abordar la clasificación a través de una modificación legislativa o mediante un análisis de cada moneda digital), la evaluación individual de cada moneda digital constituirá el proceso que deberá realizarse a fin de identificar si es que se trata o no de un valor mobiliario para propósitos tributarios.

Debemos destacar que, como resultado de las 8 257 monedas digitales que existen y cuyas cualidades y propósitos económicos pueden ser sustancialmente diversos, una extrapolación del concepto tradicional de valor mobiliario respecto de todas puede resultar inconsistente y conllevar a la atribución de efectos tributarios inadecuados.

Resulta interesante traer a colación la actual posición de la Securities and Exchange Commission toda vez que viene aplicando un criterio jurisprudencial de la Corte Suprema de los Estados Unidos del año 1946, para calificar algunas monedas digitales como *securities* sujetas al *Securities Act* de 1933. Cabe resaltar que, dicha legislación ha regulado una subcategoría de *security* denominada *investment contract* o contrato de inversión.

En el reconocido caso de 1946, *Securities and Exchange Commission c. W. J. Howey Co. et al.* se estableció como criterio jurisprudencial lo siguiente:

> […] an investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party, it being immaterial whether

[16] Se debe destacar que Perú no ha previsto en su legislación un impuesto a la herencia o a las donaciones, a diferencia de otros Estados.

[17] Según el artículo 255 de la Ley de Títulos Valores (2000):

> Son valores mobiliarios aquellos emitidos en forma masiva, con características homogéneas o no en cuanto a los derechos y obligaciones que representan. Las emisiones podrán estar agrupadas en clases y series. Los valores pertenecientes a una misma emisión o clase que no sean fungibles entre sí, deben estar agrupados en series. Los valores pertenecientes a una misma serie deben ser fungibles. Los valores sobre los cuales se hayan constituido derechos reales u otra clase de cargos o gravámenes dejan de ser fungibles, no pudiendo ser transados en los mecanismos centralizados de negociación, salvo que se trate de su venta forzosa.

[18] De acuerdo con el artículo 3 de la Ley de Mercado de Valores (1996):

> Son valores mobiliarios aquellos emitidos en forma masiva y libremente negociables que confieren a sus titulares derechos crediticios, dominiales o patrimoniales, o los de participación en el capital, el patrimonio o las utilidades del emisor. Para los efectos de esta ley, las negociaciones de derechos e índices referidos a valores mobiliarios se equiparán a tales valores.

> the shares in the enterprise are evidenced by formal certificates or by nominal interests in the physical as ets employed in the Enterprise (párr. 11)[19].

Sobre el particular, debemos indicar que el referido criterio jurisprudencial ha sido y viene siendo utilizado por la mencionada autoridad regulatoria a fin de someter algunas monedas digitales bajo su ámbito de regulación; es decir, dicho criterio clasificatorio no ha sido recogido por la autoridad tributaria de dicho país.

Nótese que, bajo este criterio, resulta indiferente la representación de los derechos económicos que le corresponden al inversionista y más bien lo que resulta relevante es la identificación del acuerdo entre dicho sujeto y el promotor, así como la asociación entre la actividad de un negocio individualizado y el reconocimiento del resultado a favor del inversionista. Dicho lo anterior, debemos indicar que este trabajo se limita a describir algunos criterios generales que podrían tomarse en cuenta para realizar clasificar determinadas monedas digitales bajo la categoría de valor mobiliario y solo para efectos tributarios.

Como se describirá a continuación, las monedas digitales que podrían ser consideradas como valores mobiliarios deberán extenderse solo sobre aquellas que otorguen a sus tenedores un derecho a participar sobre los resultados de un negocio individualizado, y cuyo valor de cada inversión dependa estrictamente en el desarrollo de las actividades de dicha empresa, mas no de la utilidad que pueda representar dicha moneda al permitir la adquisición de bienes y servicios en una red descentralizada o principalmente descentralizada.

Se deberá distinguir aquellas monedas digitales típicas de aquellas atípicas. Para estos propósitos, las monedas digitales típicas serán aquellas que operan como una divisa tradicional, su operatividad se basa sobre la tecnología de cadena de bloques y la criptografía, y en la medida de lo posible que se trate de una red descentralizada que permita la anotación de las transacciones realizadas entre sus usuarios. Adicionalmente, que el valor de la moneda digital sea independiente de la actividad económica de una entidad individualizada, es decir, que su valor derive principalmente del uso que le puedan dar sus usuarios, ya que con las mismas podrán adquirir otras monedas digitales, activos digitales, bienes regulares o incluso servicios.

De otro lado, las monedas digitales atípicas serán aquellas que se asemejen a los instrumentos representativos del capital o patrimonio de una entidad en particular, o incluso de aquellos instrumentos representativo de deuda, así como aquellos instrumentos híbridos que reúnan características de ambos. Cabe resaltar que, bajo este tipo de activos la asociación de los resultados de la actividad de un negocio individualizado y su repercusión en el valor de estas monedas digitales atípicas se encuentra entrelazado. En la siguiente sección, no se analizarán las implicancias de este tipo de monedas digitales toda vez que su tratamiento tributario debería equipararse al que ya le es aplicable a estos instrumentos tradicionales.

Cabe indicar que, las monedas digitales típicas, además de no calificar como un valor mobiliario, tampoco podrían ser consideradas como *commodity*[20], dinero de curso legal sea digital o físico[21], o representación de dicho dinero tradicional.

Ahora bien, con las disposiciones actualmente vigentes, las monedas digitales que deben encontrarse fuera de la categoría de valores mobiliarios, en términos generales, consistirán en todas aquellas que no representen un instrumento de participación en el capital de una entidad, ni que les reconozca a sus titulares un derecho crediticio

---

[19] Traducción libre:

> Un contrato de inversión para propósitos del *Securities Act* significa un contrato, transacción o esquema bajo el cual una persona invierte su dinero en un emprendimiento común y tiene la expectativa de obtener ganancias únicamente de los esfuerzos del promotor o de un tercero, resultando inmaterial si las acciones en una empresa se representan en un certificado formal o bajo un interés nominal en los activos físicos utilizados por la empresa.

[20] Según el Glosario de la Ley 26702 (1996) por *commodities* debe entenderse "[m]ercancías primarias o básicas consistentes en productos físicos, que pueden ser intercambiados en un mercado secundario, incluyendo metales preciosos, pero excluyendo oro, que es tratado como una divisa". Bajo dicha definición, las monedas digitales no podrían ser reconocidas como tales, toda vez que se tratarían de activos intangibles, cuya representación no es física, y que no reflejan mercancías primarias ni básicas consistentes en productos físicos.

[21] Debemos indicar que las monedas digitales no califican como monedas legales (o de curso legal), ello con excepción de las Central Bank Digital Currency (en adelante, CDBC) que en un futuro tendrán mayor acogida y diversos Estados podrían terminar proliferando una migración del dinero de curso legal físico a una representación parcial o totalmente digital. El caso más popular a la fecha consiste en el yuan digital emitido por el Banco Popular de China, es decir, el banco central de la República Popular China. Los CDBC al tratarse de monedas digitales emitidas por bancos centrales de Estados, claramente, deberán ser reconocidas como monedas de curso legal cuya representación será estricta y únicamente digital.

respecto del cual tengan un derecho sobre un capital aportado, ni algún derecho a un rendimiento o interés (por su mera tenencia), ni tampoco puede considerarse como tal a aquellos instrumentos híbridos que se representen en monedas digitales[22].

Como se ha venido describiendo, las monedas digitales típicas tienen como propósito actuar como una divisa tradicional que le permite a los tenedores intercambiar valor a través de una red descentralizada. En cambio, se evidenciaran indicios de una moneda digital atípica en aquellos modelos en donde los promotores o desarrolladores de una moneda digital en particular y valiéndose de la tecnología de cadena de bloques ofrezcan al público en general instrumentos de inversión tradicionales, en donde típicamente, el esquema ya no se valdría de una red descentralizada, sino que, la asociación entre el valor creado por las actividades económicas del vehículo emisor se entrelacen con en el valor de la moneda digital[23]. En ese escenario, podría resultar plausible sostener que dicha moneda digital atípica deba ser considerada como un valor mobiliario para efectos tributarios, y como tal, se sujete a las disposiciones que resultan aplicables a ese tipo de activos.

Por su parte, las monedas digitales típicas antes descritas se encontrarían comprendidas bajo la categoría general de bienes muebles recogida en el artículo 886 del Código Civil (1984); esto es, bajo la legislación general, pues estos activos aún no han sido recogidos en disposición jurídica alguna que le otorgue una naturaleza distinta.

Los principales tributos que serán analizados son el impuesto a la renta y el IGV y se describirán las implicancias tributarias que pueden verificarse como resultado de adquirir, mantener o enajenar monedas digitales típicas. Dicha aproximación tomará en cuenta las diferencias que consideramos podrían ser aplicables en caso el adquirente, tenedor o transferente de estos activos sea una persona natural o jurídica[24].

A. Ámbito de aplicación de la Ley del Impuesto a la Renta

La Ley del IR no ha previsto regulación alguna respecto de los ingresos que los contribuyentes domiciliados pudieran obtener como consecuencia de la adquisición y enajenación de monedas digitales típicas. Ello toma mayor relevancia en el caso de personas naturales, tal y como lo dispone la Ley del IR, el ámbito de aplicación sobre las rentas que generan determinados capitales se encuentra más limitada a diferencia de como se ha estructurado dicho ámbito para las rentas que obtienen personas jurídicas.

En ese contexto, el régimen tributario aplicable tiene que determinarse en función a la definición del concepto de renta, recogido por la Ley del IR, que –en resumen– considera como renta la que proviene de una fuente durable susceptible de generar ingresos periódicos (**teoría de la renta producto**), así como los beneficios derivados de la enajenación de bienes de capital (**ganancias de capital**). Además, para el caso específico de las empresas, la Ley grava "cualquier ganancia o ingreso derivado de operaciones con terceros" (Decreto Legislativo 744, 1993, art. 3) (**teoría del flujo de riqueza**).

Nótese que el ámbito de aplicación del impuesto a la renta, tratándose de personas naturales sin negocio, se circunscribe a que las rentas puedan encontrarse comprendidas bajo la teoría de la fuente o renta producto, mientras que, en el caso de personas jurídicas, el ámbito de aplicación es más amplio pues las rentas que obtengan deben observar la teoría del flujo de riqueza.

En síntesis, dichas teorías son definidas en la doctrina de la siguiente manera:

---

22 Se excluye de esta referencia a los *non-fungible tokens* (en adelante, NFT) o los *stock tokens* cuyo análisis podría requerir una investigación independiente. También, se debe señalar que este criterio debe tomarse con bastante precaución y valerse de otros elementos que permitan tipificar la existencia de un valor mobiliario.

Los NFT consisten en activos digitales que representan objetos reales tales como el arte, la música, ítems de videojuegos, vídeos, entre otros, cuya titularidad se anota en una plataforma de cadena de bloques, y se permite la transferencia de dicho activo intangible a terceros. En cambio, los *stock tokens* son representaciones digitales de acciones que son transadas en mercados centralizados tradicionales. El valor del *stock token* refleja el valor de la acción subyacente y suelen ser tratados como instrumentos derivados, ya que, el elemento subyacente no se transfiere con ocasión a la enajenación del instrumento.

23 Cabe destacar que, esta referencia no significa que toda oferta primara de monedas digitales o ICO deba ser considerada como la entrega de valores mobiliarios a favor de inversionistas; sino que, existen casos en donde un proyecto inició de manera centralizada y progresivamente el proceso de validación de los bloques se descentralizó al incorporar mayores mineros o validadores a la propia red, alejando la asociación entre el emisor y el valor intrínseco de cada moneda digital.

24 Para efectos prácticos, toda alusión a persona natural o jurídica debe entenderse referida a sujetos domiciliados en Perú conforme a la legislación tributaria peruana. Por su parte, al referirnos a persona natural lo realizamos partiendo de la premisa que se trata de un individuo que califica como 'persona natural sin negocio', puesto que, de calificar como persona natural con negocio, el tratamiento tributario aplicable sería el mismo al que se sujetan las personas jurídicas.

- **Teoría de la renta producto** (García Mullín, 1980): solo serían categorizados como renta según este criterio, aquellos ingresos que cumplan con los siguientes requisitos:

  a) La renta debe ser un producto, una riqueza nueva, distinta y separable de la fuente que la produce, y debe de tratarse de una nueva riqueza material.

  b) La renta debe provenir de una fuente productora durable. En cuanto a lo que debe entenderse como fuente productora se tiene como ejemplo al capital, sea corporal o incorporal, que, teniendo un precio en dinero, es capaz de suministrar una renta a su titular. Bajo ese concepto, se tiene a las cosas muebles o inmuebles, capitales monetarios, derechos y actividades. Por su parte, en cuanto a la exigencia que dicha fuente sea durable se debe entender dicho capital debe sobrevivir la producción de la renta (derivada), manteniendo su capacidad para repetir la generación de rentas en un futuro a favor de su titular.

  c) La renta debe ser periódica, es decir, que exista la posibilidad que se deriven nuevas rentas del capital explotado.

  d) La fuente (el capital colocado) se ha puesto en explotación para que pueda producir la nueva renta.

- **Teoría del flujo de riqueza:** calificará como renta cualquier beneficio o enriquecimiento proveniente de terceros, es decir, como recoge la Ley del IR, el total de riqueza que desde los terceros fluye hacia el contribuyente en un período determinado. Bajo este criterio, no importa si los ingresos provienen o no de una fuente durable, sino que basta que la ganancia o beneficio se derive de operaciones con terceros. Como bien indica la doctrina (Medrano, 2018), bajo este criterio se incluyen los ingresos provenientes de actividades accidentales y los ingresos eventuales cuya generación dependen de elementos aleatorios y ajenos a la voluntad de quien los recibe.

Asimismo, como bien indica el referido autor, bajo esta teoría:

> […] lo esencial es que exista una operación con terceros; se excluye del concepto de renta el aumento de valor que experimentan los bienes que no se han enajenado, así como los beneficios que el sujeto puede proporcionarse sin realizar intercambios, tales como el uso de bienes durables o la provisión de bienes y servicios de propia producción (Medrano, 2018, p. 24).

B. Ámbito de aplicación de la Ley del Impuesto General a las Ventas

El artículo 1 de la Ley de Impuesto General a las Ventas ha establecido que califican como operaciones gravadas con este impuesto, entre otras, la venta en el país de bienes muebles, la prestación o utilización de servicios en el país (Decreto Supremo 055-99-EF, 1999). Sobre el particular, el artículo 3 de la referida Ley define algunos de los aludidos conceptos, en los siguientes términos:

- Por **bienes muebles** debe entenderse a

> [l]os corporales que pueden llevarse de un lugar a otro, los derechos referentes a los mismos, los signos distintivos, invenciones, derechos de autor, derechos de llave y similares, las naves y aeronaves, así como los documentos y títulos cuya transferencia implique la de cualquiera de los mencionados bienes (Decreto Supremo 055-99-EF, 1999, art 3.b).

- Se consideran **servicios** a

> [t]oda prestación que una persona realiza para otra y por la cual percibe una retribución o ingreso que se considere renta de tercera categoría para los efectos del Impuesto a la Renta, aun cuando no esté afecto a este último impuesto; […]. También se considera retribución o ingreso los montos que se perciban por concepto de arras, depósito o garantía […] (Decreto Supremo 055-99-EF, 1999, art. 3.c.1).

A su vez, para propósitos de este análisis, resulta igual de relevante destacar que, según el artículo 9 de la Ley del IGV, califican como contribuyentes del impuesto, las personas naturales, las personas jurídicas, entre otros, que desarrollen actividad empresarial y realicen algunas de las operaciones gravadas con este impuesto (Decreto Supremo 055-99-EF, 1999). Por su parte, el referido artículo de la Ley dispone que las personas naturales que no realicen actividad empresarial calificarán como contribuyentes del impuesto únicamente cuando realicen habitualmente las operaciones gravadas con el impuesto (Decreto Supremo 055-99-EF, 1999, art. 9).

C. Personas naturales sin negocio[25]

1. Minería

La actividad de la minería realizada en menor escala por una persona natural solo requiere de la designación de uno o varios ordenadores en un espacio determinado, un uso intensivo de electricidad, internet, refrigeración y ventilación, a fin de que dichas computadoras puedan resolver los algoritmos, de manera automatizada y sin la intervención de un humano para llevar ello a cabo. Dicha labor computacional no debería quedar comprendida bajo el concepto de servicios prestados de manera independiente según la definición prevista por la Ley del IR. En otras palabras, la persona natural que destina un ordenador o varios para la minería de monedas digitales no debería generar una renta de trabajo para este último.

Como se ha indicado previamente, en este tipo de actividades, lo predominante es la asignación de determinados bienes de capital (el ordenador u ordenadores) para que estos, de manera automatizada, sin una intervención significativa de un humano, resuelvan dichos cálculos matemáticos (los algoritmos) que son necesarios para la elaboración de la red de bloques o el registro de las transacciones en dicha cadena de bloques[26].

Sin embargo, podría resultar plausible sostener que, la renta derivada del capital asignando (es decir, el ordenador u ordenadores), que automáticamente resuelve estos problemas matemáticos (sin intervención de humanos ni actividad realizada por estos), se encontraría comprendida bajo la teoría de renta producto y, como tal, conceptualmente, considerar a la referida renta como gravada, ya que se trataría de una operación que genera: (i) una renta nueva, distinta y separable, es decir, se trataría de una nueva riqueza material; (ii) proviene de una fuente durable, pues el ordenador u ordenadores subsisten el proceso de validación y continúan realizando dicha actividad de manera periódica, siendo posible que sigan produciendo nuevas monedas digitales; y (iii) el ordenador o los ordenadores se explotan de tal manera que se crea una nueva renta.

2. *Forging o Staking*

La asignación de monedas digitales como colateral para que personas naturales cuenten con el derecho para validar transacciones o crear nuevos bloques en una red, y como contraprestación por ello reciban monedas digitales o divisas tradicionales, en nuestra opinión, configuraría un evento que originaría un supuesto de renta gravada con el impuesto a la renta, bajo la teoría de renta producto, pues se trataría de un rendimiento periódico y durable, derivado del capital asignado, que permite la continua creación de nuevas riquezas (y que no supone la extinción o menoscabo del capital originario que ha sido colocado para su explotación).

3. *Airdrops*

Las monedas digitales que reciban las personas naturales a título gratuito como resultado de un *airdrop* ordinario, no constituye un supuesto que genere renta gravada sujeta al impuesto a la renta.

En cambio, en el caso de un *hardfork* que derive en un *airdrop*, podría sostenerse que el titular de monedas digitales originarias recibe monedas digitales recién creadas en ese contexto, y el motivo por el cual las ha recibido se debe al solo hecho de haber contado con un número determinado de monedas digitales previamente al *hardfork.*

En otras palabras, se podría sostener que se trata de una suerte de rendimiento del capital, susceptible de encontrarse comprendido bajo la teoría de renta producto, y como tal, conceptualmente, considerar dicha renta como gravada, ya que se trataría de una operación que genera rendimientos periódicos y cuya fuente es durable y distinta al capital que está siendo utilizado (que al explotarse el capital, la renta producida es distinta al mismo y la explotación no implica la reducción o el menoscabo de dicho capital).

---

[25] En esta subsección no se analizará implicancia alguna referida al IGV, puesto que, las personas naturales sin negocio no califican como contribuyentes de este impuesto, y como tales, no se verificarían los elementos de la hipótesis de incidencia previstos del cuerpo normativo que regula este impuesto.

[26] El criterio esbozado por el Tribunal Fiscal en la Resolución 09934-5-2017 (2017) resulta relevante para analizar cómo debe entenderse los alcances de la Ley del IR para definir si una persona natural está realizando la prestación de servicios, a fin de identificar si es que se está realizando o no una actividad empresarial, en la que se aprecie la presencia conjunta de trabajo y capital.

En ese caso en concreto, el Tribunal consideró que la persona natural había realizado actividades empresariales, puesto que se había comprometido al "[…] mantenimiento y funcionamiento, a subir contenidos y materiales, dentro de los parámetros permitidos, y a la implementación de las especificaciones de dicha empresa –su cliente– y del cumplimiento de los términos del contrato" (Resolución 09934-5-2017, 2017, p. 7).

Teniendo ello en consideración, si bien el caso planteado es distinto al analizado por el Tribunal Fiscal, es evidente que la participación de la persona natural fue lo que demostró la existencia del elemento trabajo que, de la mano del capital, generaban la existencia de una actividad empresarial.

4. ICO y posterior enajenación de monedas digitales

La adquisición de monedas digitales típicas por personas naturales provenientes de una oferta primaria no constituye un evento gravado con el impuesto a la renta, en cabeza del adquirente.

Por su parte, la renta que pueda obtenerse por la enajenación de monedas digitales –previamente adquiridas– por personas naturales, tampoco se encontrará gravada con el impuesto a la renta. Para efectos de la Ley del IR, solo pueden generar 'ganancias de capital' aquellos activos que se encuentran taxativamente enunciados en la Ley del IR[27]. En dicha lista, no existe referencia alguna a la eventual renta que podría generar la enajenación de una moneda digital típica y, en ese contexto, al no encontrarse referencia alguna a este tipo de activos, las rentas que pudieran obtener las personas naturales derivadas de su enajenación estarían fuera del ámbito de aplicación del impuesto a la renta.

A modo de ejemplo, las personas naturales que adquieren divisas tradicionales y las transfieren por otras, e incluso, si fueran a obtener una 'ganancia' asociada a dicha operación, dicha plusvalía no se encontraría gravada bajo la Ley del IR, toda vez que dicho cuerpo normativo no ha previsto, bajo las teorías de renta aplicables a personas naturales, que dicho tipo de operaciones sean susceptibles de generar ganancias gravadas, pese a que las mismas se originen en el intercambio de capitales.

5. Remuneraciones por la prestación de servicios

En el supuesto en que un empleador otorgue a su empleado una retribución en monedas digitales como consecuencia de una relación laboral existente, es decir, como contraprestación por los servicios prestados, dicho importe calificará como una renta proveniente de servicios prestados en una relación de dependencia y, como tal, las referidas sumas se encontrarán gravadas con el impuesto a la renta.

D. Personas jurídicas

1. Minería

a. *Impuesto a la renta*

Como se ha indicado, la minería de monedas digitales implica que el minero mantenga actualizado el registro descentralizado y, en algunas ocasiones, que valide transacciones que son anotadas en los bloques. A cambio de efectuar dichas actividades, el minero, en determinadas ocasiones, será receptor de una moneda digital, varias o fracciones de esta, como contraprestación y, en otras ocasiones, también podrá recibir una comisión por el registro de las transacciones.

Siendo ello así, el ingreso proveniente de la minería que la persona jurídica receptora de la moneda digital obtenga, claramente estaría comprendido dentro del ámbito de aplicación de la Ley del IR, puesto que se derivaría de las actividades propias del giro de negocio del referido minero, en sus operaciones con terceros, es decir, bajo la teoría de flujo riqueza.

Cabe destacar que la renta gravable que deba determinar el minero constituirá el costo computable de las monedas digitales, valor que deberá tener debidamente identificado para efectos de su reconocimiento ante una futura enajenación a terceros de dichas monedas digitales.

b. *IGV*

La empresa que realice la actividad de minería de monedas digitales, conceptualmente, podría estar comprendida dentro del ámbito de aplicación de la Ley del IGV. Sin embargo, existen argumentos para sostener que el referido impuesto puede resultar de difícil aplicación en la práctica, puesto que los validadores no tienen conocimiento ni forma de averiguar la identidad de las partes que se están viendo beneficiadas por la actividad (*i.e*. validación) llevada a cabo por aquellos. Dicha particularidad –asociada a este tipo de actividad– conlleva una evidente problemática puesto que el prestador del servicio no tiene como individualizar e identificar al usuario del servicio.

La doctrina ha advertido esta problemática señalando que, conceptualmente, la administración tributaria peruana podría pretender tratar a la minería como una operación de prestación de servicios gravada con el IGV (López Miranda, 2020). Dicha posición se basaría en el amplío concepto que ha recogido nuestra legislación respecto de qué debe entenderse como 'servicios', bastando identificar la existencia de cualquier prestación que una persona realiza para otra y por la cual percibe una

[27] El artículo 2 de la Ley del IR (1993) agrega que, entre las operaciones que generan ganancias de capital, se tiene:

> La enajenación, redención o rescate, según sea el caso, de acciones y participaciones representativas del capital, acciones de inversión, certificados, títulos, bonos y papeles comerciales, valores representativos de cédulas hipotecarias, certificados de participación en fondos mutuos de inversión en valores, obligaciones al portador u otros valores al portador y otros valores mobiliarios.

retribución o ingreso que se considere renta empresarial para efectos del impuesto a la renta.

Sin perjuicio de lo señalado, la observación formulada por la doctrina antes indicada parece acertada, en cuanto a que este tipo de operaciones podrían encontrarse comprendida dentro de la figura de 'exportación de servicios'[28], en cuyo caso, la operación no se encontraría sujeta al pago de IGV alguno. Ello, puesto que las actividades de validación que serían realizadas por las personas jurídicas en el Perú, típicamente se prestarían a favor de sujetos que domicilian en el extranjero, siendo que, en la actualidad, la participación de usuarios peruanos en el ecosistema de monedas digitales es bastante reducida (en comparación a la participación de usuarios domiciliados fuera del Perú).

No obstante, ello no significa que usuarios peruanos utilicen los servicios proporcionados por estas redes, y en dicho contexto, se trataría de una prestación de servicios efectuada por una persona jurídica domiciliada a favor de un usuario peruano, por lo que, dicha operación estaría gravada con el IGV.

2. *Forging o Staking*

a. *Impuesto a la renta*

El *forging o staking*, como se ha explicado antes, se asemejaría a la figura en que el validador deba asignar una cantidad determinada de monedas digitales como colateral, asemejándose a la figura de las cuentas de depósito en garantía (o *escrow*), para que, como contrapartida, cuente con el derecho de participar en el proceso de validación de transacciones. Así, como resultado de la validación y asumiendo un riesgo (sobre las monedas digitales asignadas como garantía), la red, aleatoriamente, podrá otorgar al validador monedas digitales recién creadas, o recibir una comisión por la anotación de una transferencia en la cadena de bloques.

Claramente, el producto entregado al validador se encontrará gravado con el impuesto a la renta. Ello, toda vez que dicha persona jurídica obtendría un rendimiento proveniente del capital que ha asignado a la red para tener expedito su derecho a crear nuevos bloques y validar transacciones (como una suerte de colocación de capital que produce rendimientos que son pagados a quien ha asumido el riesgo de, eventualmente, perder las monedas digitales colocadas como garantía).

Cabe destacar que, la renta gravable que deba determinar el validador constituirá el costo computable de las monedas digitales que le han sido reconocidas y otorgadas, importe que se deberá tener debidamente identificado para efectos de su reconocimiento ante una futura enajenación de dichos activos.

b. *IGV*

La asignación de monedas digitales para participar en la creación de nuevos bloques y la validación de transacciones podría configurar una 'prestación' en los términos de la definición de 'servicios' según la Ley del IGV y, sobre la base de ello, la administración tributaria podría sostener que se verificaría una operación sujeta a este impuesto con ocasión al *forging o staking.* Bajo dicha posición, la referida administración podría sostener que el ingreso que obtiene el validador proviene de una operación de garantía comprendida dentro de la definición de servicios prevista por la Ley del IGV.

Sin perjuicio de ello, esta operación también podría, conceptualmente, considerarse como 'exportaciones de servicios' no sujeta al pago del IGV, siempre que se cumplan los requisitos previstos por la legislación de dicho impuesto. Ello, toda vez que los usuarios beneficiados por la creación de la red, bloques y/o la validación de transacciones, en su gran mayoría domicilian en el extranjero.

3. *Airdrops*

En este tipo de operaciones, los emisores crean y otorgan monedas digitales a determinados usuarios a título gratuito. Asimismo, existen *airdrops* que se producen como resultado de *hard-forks*, es decir, de una división de la cadena de bloques, manteniendo la moneda digital original, y creando nuevas monedas digitales que son otorgadas a favor de los titulares de las monedas digitales originarias.

[28] Según el artículo 33 de la Ley del IGV (Decreto Supremo 055-99-EF, 1999):

Los servicios se considerarán exportados cuando cumplan concurrentemente con los siguientes requisitos:

a) Se presten a título oneroso desde el país hacia el exterior, lo que debe demostrarse con el comprobante de pago que corresponda, emitido de acuerdo con el reglamento de la materia y anotado en el Registro de Ventas e Ingresos.

b) El exportador sea una persona domiciliada en el país.

c) El usuario o beneficiario del servicio sea una persona no domiciliada en el país.

d) El uso, la explotación o el aprovechamiento de los servicios por parte del no domiciliado tengan lugar en el extranjero.

Claramente, el producto que recibiría el beneficiario –persona jurídica– se encontrará gravado con el impuesto a la renta, toda vez que obtendría una renta proveniente de sus operaciones con terceros, en el supuesto en que el *airdrop* realizado por el otorgante sea íntegramente a título gratuito o, incluso, en el supuesto en que se ha producido el *hard-fork,* y, como resultado de este, se entrega al titular originario de una moneda digital particular, una moneda digital recién creada.

Se debe indicar que, la renta gravable que deba determinar el beneficiario de los *airdrops* constituirá el costo computable de las monedas digitales que le fueron otorgadas, el que deberá ser considerado en caso de una futura enajenación de estas.

4. ICO

En los ICO, los emisores transfieren monedas digitales a terceros, las que son adquiridas a título oneroso por estos. Es decir, los terceros pagan un precio para adquirir estas monedas digitales vía la transferencia de otras monedas digitales o mediante el pago de divisas tradicionales.

Partiendo de la premisa que, el adquirente sería una persona jurídica, esta operación únicamente produciría para esta última el reconocimiento de un costo computable asociado al precio que ha pagado a favor del emisor (sea que dicho precio haya sido pagado vía la entrega de otra moneda digital u otra divisa tradicional). Por el lado del transferente[29], que típicamente se trataría de entidades domiciliadas en el exterior[30], no habría un hecho imponible gravado con el impuesto a la renta, toda vez que no existiría un criterio de vinculación jurisdiccional que califique dicha eventual renta como de fuente peruana para el sujeto no domiciliado.

5. Enajenación de monedas digitales

La renta que puede originarse por la enajenación de monedas digitales, razonablemente, tendría que encontrarse sujeta las disposiciones vinculadas a la determinación de 'ganancias de capital', siendo el impuesto a la renta de cargo de la enajenante persona jurídica domiciliada.

Al respecto, el artículo 2 de la Ley del IR (1993) establece el concepto de ganancia de capital, de la siguiente manera: "[…] cualquier ingreso que provenga de la enajenación de bienes de capital. Se entiende por bienes de capital a aquellos que no están destinados a ser comercializados en el ámbito de un giro de negocio o de empresa […]".

Bajo ese contexto, las personas jurídicas que enajenen monedas digitales deberán determinar la ganancia de capital correspondiente, constituida por la diferencia entre el precio de venta recibido (que no podrá ser inferior a su valor de mercado) y el costo computable que tuviere sobre los activos transferidos.

Nótese que, bajo la teoría de flujo riqueza que resulta aplicable a este tipo de contribuyentes, el ámbito de aplicación del impuesto a la renta es más amplio que aquel aplicable a las personas naturales, ya que, en el caso de personas jurídicas, se encontrará gravada la ganancia que se obtenga en el devenir de sus actividades en sus relaciones con otros particulares con los que participa en igualdad de condiciones.

6. Problemática

El hecho que las disposiciones generales de la Ley del IR y de la Ley del IGV puedan resultar aplicables a algunas de las rentas u operaciones antes descritas y, como resultado de ello, originen eventos gravados con dichos impuestos, no debe llevarnos a la conclusión de que la legislación tributaria peruana deba omitir esclarecer la incertidumbre que gira en torno a estos activos. En nuestra opinión, en un futuro estos aspectos van a tener que abordarse y regularse apropiadamente, pues este tipo de activos tal y como ha sido advertido en la legislación comparada, ocasionan una serie de problemas al momento en que se aborda su tratamiento con la legislación tributaria ordinaria que ha sido prevista y diseñada para tratar activos tradicionales.

Los principales retos que este tipo de activos presentará para propósitos de su calificación tributaria se evidencian en, al menos, los siguientes aspectos: (i) su calificación como una moneda digital típica o si se trata de una figura atípica para estos propósitos (es decir, que califique como valor mobiliario); (ii) la determinación del valor de mercado aplicable; (iii) el tipo de cambio aplicable, sea que se transfieran a cambio de otras monedas digitales o contra la entrega de divisas tradicionales; (iv) el régimen de determinación del costo computable aplicable a este tipo de activos; y (v) la inexistencia de un régimen de arrastre de pérdidas para las

[29] Actualmente, todas las emisiones de monedas digitales se han realizado por emisores que domicilian en el extranjero.

[30] Según la Ley del IR (Decreto Legislativo 774, 1993), los sujetos no domiciliados en el Perú solo tributan respecto de las rentas que obtienen que califiquen como de fuente peruana. De lo supuestos previstos por dicho cuerpo normativo, no habría supuesto alguno que abarque la renta asociada a una moneda digital emitida o creada en el exterior.

personas naturales que les permita compensar adecuadamente las pérdidas de capital asociadas a este tipo de activos contra las rentas positivas que pueda obtener en los siguientes ejercicios.

Asimismo, en caso incrementarán las actividades de minería, *forging o staking*, por parte de empresas en el Perú, consideramos que resultaría beneficioso establecer un régimen específico para considerar que estas operaciones no se encuentran afectas al IGV, en ningún caso, ello debido a la complejidad asociada a la identificación de los usuarios que se beneficiarían de las validaciones que efectuarían los validadores de personas jurídicas peruanas.

V. CONCLUSIONES

El surgimiento y creación de nuevas monedas digitales en el mundo ciertamente está y continuará revolucionando la forma en que opera la economía global. Al tratarse de una innovación relativamente incipiente que constantemente está siendo sometida a cambios tecnológicos drásticos, resulta complicado establecer disposiciones de carácter regulatorio y tributario, tomando como base para ello, las características de solo algunas de las monedas digitales. Nos parecen acertadas las indicaciones que ha efectuado la OCDE con relación a que aún estamos en una etapa temprana para establecer lineamientos claros que puedan replicarse en diversas legislaciones, incluso en un contexto en que hay diversos Estados interesados en abordar el tratamiento tributario y regulatorio de esta nueva clase de activos, pues la promulgación de un régimen inadecuado puede suponer una barrera o desincentivo para que nuevos usuarios comiencen a participar en este ecosistema.

Antes de promulgar normas tributarias asociadas a las monedas digitales, consideramos que Perú debiera esperar a los cambios que se implementarán en los siguientes años a la tecnología de bloques y a las monedas digitales que vienen cobrando mayor sostenibilidad y fiabilidad en los mercados globales. Como hemos indicado, una adopción temprana de normas tributarias puede generar serios desincentivos para los inversionistas peruanos que tengan intenciones de invertir en estos nuevos activos.

En nuestra opinión, en un futuro, el legislador peruano deberá explorar el régimen más adecuado y propicio para abordar los distintos eventos asociados al ciclo económico de las monedas digitales. Pero, dicha labor deberá realizarla con suma cautela, debiendo considerar, por ejemplo, que a la fecha el precio de estos activos es sumamente volátil y existen dificultades operativas para la determinación de los tipos de cambios –al no haber una fuente fiable que reporte este valor con relación a una divisa tradicional–. Actualmente, incluso para activos tradicionales, no existen en nuestro país disposiciones claramente definidas en cuanto al tipo de cambio que deben aplicar las personas naturales para efectos de la determinación del costo y/o del precio de venta en monedas extranjeras. Dicha carencia revelaría uno de los problemas más relevantes a ser evaluado respecto a esta materia.

Por su parte, otra gran problemática que debería evaluarse consiste en analizar la posibilidad de promulgar normas que le permitan a las personas naturales y jurídicas domiciliadas el arrastre de pérdidas de fuente extranjera, especialmente, teniendo en consideración que, con las monedas digitales, así como se pueden obtener ganancias sustanciales, también pueden generarse pérdidas considerables.

REFERENCIAS

Australian Taxation Office (30 de marzo de 2020). Transacting with Cryptocurrency. https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?anchor=Transactingwithcryptocurrency

Banco Mundial (2017). *Distributed Ledger Technology (DLT) and Blockchain* (FinTech Note 1). https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf?sequence=5

Bergman, A. (2 de marzo de 2018). Taxation Of Cryptocurrency Proof Of Stake Transaction Fees. *Forbes*. https://www.forbes.com/sites/greatspeculations/2018/03/02/taxation-of-cryptocurrency-proof-of-stake-transaction-fees/?sh=607f208416c9

Chandrasekera, S. (8 de diciembre de 2020). Spark Token Airdrop Comes with a Tax Bill. *Forbes*. https://www.forbes.com/sites/shehanchandrasekera/2020/12/08/spark-token-airdrop-comes-with-a-tax-bill/?sh=acd376a6cfe3

Chester, J. (12 de junio de 2017). A New Way To Raise Money: The Initial Coin Offering. *Forbes*. https://www.forbes.com/sites/jonathanchester/2017/06/12/a-new-way-to-raise-money-the-initial-coin-offering/?sh=42507da35fb5

Cipek, K. (27 de julio de 2020). Cryptocurrency Taxation: How to take a step forward. *Inter-*

American Center of Tax Administrations. https://www.ciat.org/cryptocurrency-taxation-how-to-take-a-step-forward/?lang=en

CoinMarketCap (13 de enero de 2021). Cuadros de criptomoneda mundial. https://coinmarketcap.com/es/charts/

García Mullín, R. (1980). *Impuesto sobre la Renta. Teoría y Técnica del Impuesto.* Instituto de Capacitación Tributaria – República Dominicana.

HM Revenue & Customs (2019). *Policy Paper - Cryptoassets: tax for individuals*. https://www.gov.uk/government/publications/tax-on-cryptoassets/cryptoassets-for-individuals

Houben, R., & Snyder, A. (2018). *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion* (Study). European Parliament. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

Inland Revenue Authority of Singapore (2020). *GST: Digital Payment Tokens.* https://www.iras.gov.sg/irashome/uploadedFiles/IRASHome/e-Tax_Guides/e-Tax%20Guide_GST_Digital%20Payment%20Tokens.pdf

Internal Revenue Service (2014). *Notice 2014-21*. https://www.irs.gov/pub/irs-drop/n-14-21.pdf

(2019). *Revenue Rule 2019-24*. https://www.irs.gov/pub/irs-drop/rr-19-24.pdf

López Miranda, L. (2020). Bitcoin: ¿Tenerla o ignorarla? Una aproximación hacia el tratamiento tributario peruano de la criptomoneda más famosa del mundo. *Ius et Veritas,* (58), 140-153. https://doi.org/10.18800/iusetveritas.201901.008

Massachusetts Institute of Technology (2018). Blockchain Basics & Transactions, UTXO and Script Code [Video]. Youtube. https://youtu.be/zGDTt9Q3vyM

Medrano, H. (2018). *Derecho Tributario - Impuesto a la renta: aspectos significativos*. Fondo Editorial de la Pontificia Universidad Católica del Perú.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Bitcoin Organization. https://bitcoin.org/bitcoin.pdf

Organización para la Cooperación y el Desarrollo Económicos [OCDE] (2020). *Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues.* https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.pdf .

Seibold, S., & Samman, G. (2016). *Consensus Immutable agreement for the Internet of value*. KPMG. https://assets.kpmg/content/dam/kpmg/pdf/2016/07/kpmg-blockchain-consensus-mechanism.pdf

Skatteetaten. (s/f). Tax and VAT relating to Bitcoin and other virtual currencies. Norwegian Tax Administration. https://www.skatteetaten.no/en/business-and-organisation/reporting-and-industries/industries-special-regulations/internet/tax-and-vat-on-virtual-currencies

Van Adrichem, B. (2019). Howey Should be Distributing New Cryptocurrencies: Applying the Howey Test to Mining, Airdropping, Forking, and Initial Coin Offerings. *Science and Technology Law Review*, *20*(2), 388-422. https://doi.org/10.7916/stlr.v20i2.4775

Veroskatt (22 de enero de 2020). Taxation of virtual currencies. https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48411/virtuaalivaluuttojen-verotus3/

(2020). Taxation of Virtual Currencies. https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48411/virtuaalivaluuttojenverotus3/#2.5-virtuaalivaluutan-louhintaan-osallistumisesta-saatu

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Agenzia delle Entrate, 2 de septiembre de 2016, Risoluzione 72/E (It.).

Código Civil [CC], Diario Oficial *El Peruano*, 25 de julio de 1984 (Perú).

Decreto Legislativo 774, Ley del Impuesto a la Renta, Diario Oficial *El Peruano*, 31 de diciembre de 1993 (Perú).

Decreto Legislativo 861, Ley del Mercado de Valores, Diario Oficial *El Peruano*, 22 de octubre de 1996 (Perú).

Decreto Supremo 055-99-EF, Texto Único Ordenado de la Ley del Impuesto General a las Ventas e Impuesto Selectivo al Consumo, Diario Oficial *El Peruano*, 15 de abril de 1999 (Perú).

Directiva 2006/112/CE del Consejo, de 28 de noviembre de 2006 , relativa al sistema común del impuesto sobre el valor añadido, 2006 O.J. (L 347) 1 (UE).

Informação Vinculativa 5717/2015, 27 de diciembre de 2016 (Bras.).

Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintencia de Banca y Seguros, Diario Oficial *El Peruano*, 9 de diciembre de 1996 (Perú).

Ley 27287, Ley de Títulos Valores, Diario Oficial *El Peruano*, 19 de junio de 2000 (Perú).

Securities and Exchange Commission c. W. J. Howey Co. et al., 328 U.S. 293 (1946).

Tribunal Fiscal, 10 de noviembre de 2017, Resolución 09934-5-2017 (Perú).

10.18800/themis.202101.012

INNOVANDO EN LA ARENERA: UNA APROXIMACIÓN A LAS *FINTECH* Y A LA IMPORTANCIA DE LA IMPLEMENTACIÓN DE UN *SANDBOX* REGULATORIO EN PERÚ

INNOVATING IN THE SANDBOX: AN APPROACH TO THE FINTECH AND THE IMPORTANCE OF THE IMPLEMENTATION OF A REGULATORY SANDBOX IN PERU

Tamara Rezqallah Arón*
Exmiembro de THĒMIS
Payet, Rey, Cauvi, Pérez

Currently, we are living through a technological revolution, which has reached the financial system. Companies that offer financial products and services that leverage technology to be more efficient and to offer users effective solutions related to finance, known as FinTech, have become more common. However, the novelty and innovation given by FinTech companies do not only offer advantages to users and the market, but also challenges for regulators, as they must balance protecting constitutional assets while ensuring a suitable legal ecosystem for the development of innovations in technological and financial matters.

In light of this, an alternative that seems to balance the aforementioned factors is the implementation of a regulatory sandbox: a controlled space where FinTech companies can live test their innovative financial products and services. Regulators from all over the world have been implementing sandboxes in their respective jurisdictions with encouraging results. In this sense, due to its flexibility and adaptability to different legal systems and contexts, the implementation of a regulatory sandbox is an attractive alternative for the development of the FinTech industry in Peru.

Keywords: FinTech; regulatory sandbox, Latin America; financial innovation; financial inclusion.

Actualmente, vivimos una época de revolución tecnológica que ha alcanzado al sistema financiero. Cada vez son más comunes las FinTech *o empresas que ofrecen productos y servicios financieros que se apalancan de la tecnología para ser más eficientes y ofrecer al usuario soluciones efectivas relacionadas con las finanzas. Ahora bien, la novedad e innovación aportadas por las* FinTech *no solo ofrecen ventajas a los usuarios y al mercado; sino que también representan desafíos para el regulador, pues este debe buscar el equilibrio entre la tutela de bienes constitucionales y el aseguramiento de un ecosistema legal idóneo para el desarrollo de las* FinTech*.*

Así las cosas, una alternativa que parece balancear todo ello es la implementación de un sandbox *regulatorio: es decir, un espacio controlado en el que las* FinTech *pueden probar sus productos y servicios en tiempo real. Reguladores de todo el mundo vienen implementado* sandboxes *en sus jurisdicciones con resultados alentadores. En tal sentido, debido a su flexibilidad y adaptabilidad a distintos ordenamientos jurídicos, la implementación de un* sandbox *regulatorio es una alternativa atractiva para el desarrollo de la industria* FinTech *en Perú.*

Palabras clave: FinTech*;* sandbox *regulatorio; América Latina; innovación financiera; inclusión financiera.*

* Abogada. Asistenta Legal en Payet, Rey, Cauvi, Pérez Abogados (Lima, Perú). Contacto: tamara.rez.ar@gmail.com

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 21 de enero de 2021, y aceptado por el mismo el 18 de junio de 2021.

I. INTRODUCCIÓN

Es un hecho que la industria *FinTech* está cambiando radicalmente la manera en la que las personas vivimos y trabajamos (Harcourt, 2019, p. 16). Especialmente, viene transformando los mercados financieros modernos y, en consecuencia, presenta desafíos sin precedentes a los reguladores de cada país (Tsang, 2019, p. 356).

En un esfuerzo por seguirle el ritmo a esta revolucionaria tendencia que parece haber llegado para quedarse, algunos de nuestros vecinos latinoamericanos han implementado marcos regulatorios bastante completos al respecto, lo que se ve reflejado en la cantidad significativa de empresas *FinTech* que han encontrado en ellos ecosistemas legales idóneos para su desarrollo. Es así como, en el año 2020, existían 771 *FinTech* en Brasil (Statista, 2020), 414 en México (Ernst & Young, 2020, p. 10) y 200 en Colombia (Finnovista, 2020).

El caso peruano, sin embargo, difiere de los ejemplos latinoamericanos antes indicados. Actualmente, no existe en Perú una disposición legal que regule las *FinTech* en general. Por el contrario, la estrategia de nuestros reguladores parece ser la implementación de desarrollos normativos selectivos y centrados en actividades que, a su criterio, requieren normas concretas y especializadas –sea por su grado de desarrollo o riesgos asociados, entre otros factores–; por lo que no se ha optado, por el momento, por emitir una 'Ley *FinTech*' como sí lo han hecho otros países (Vodanovic Legal, 2019, p. 48). Muestra de ello es que, en enero de 2020, el Poder Ejecutivo emitió el Decreto de Urgencia 13-2020 (en adelante, Decreto de Urgencia), que regula, entre otras materias, el financiamiento participativo financiero o *crowdfunding*. Dicho Decreto de Urgencia ha sido reglamentado mediante la Resolución de Superintendente 45-2021-SMV/02 (2021), que aprobó el Reglamento de la Actividad de Financiamiento Participativo Financiero y sus Sociedades Administradoras, publicado en mayo del presente año (en adelante, Reglamento FPF).

En línea con lo señalado, la ausencia de un marco regulatorio idóneo para el desarrollo de la industria *FinTech* en Perú también se evidencia en el número de empresas de este tipo a las que acoge. A diferencia de los países latinoamericanos indicados, a finales de 2020, se identificaron 148 emprendimientos *FinTech* en el Perú (Ernst & Young, 2020, p. 40). Es decir, al término del año pasado, existían en nuestro país poco más de un centenar de empresas –distintas a entidades financieras– dedicadas a brindar o facilitar servicios financieros empleando la tecnología (Vodanovic Legal, 2019, p. 4).

De lo anterior, se puede identificar que las cifras reflejan que empresarios con ideas innovadoras con potencial de continuar la transformación de los servicios financieros con base en la tecnología se ven desalentados a proseguir con sus proyectos debido a la ausencia de un ambiente legal que los propicie y facilite.

Dicho esto, y sin perjuicio de desarrollar con mayor detalle las ventajas de las *FinTech* en las secciones siguientes, se aprecia que nuestro ordenamiento jurídico presenta posibilidades de mejora en aras de promover el desarrollo de las *FinTech*. En el presente trabajo, se desarrollará una de dichas posibilidades: la implementación de un *sandbox* regulatorio.

II. MARCO METODOLÓGICO

A. El mundo *FinTech*

1. Concepto

El término *FinTech* suele ser utilizado de manera amplia para abarcar una diversidad de productos basados en la simbiosis de los servicios financieros y la tecnología (Avendaño Carbellido, 2018, p. 98). Sin embargo, cabe precisar que este concepto no puede ser utilizado con ligereza. Su relevancia y sus particularidades son tales que las instituciones financieras internacionales más importantes han optado por delimitarlo y definirlo.

De esta manera, el Comité de Supervisión Bancaria de Basilea ha decidido emplear la definición de *FinTech* desarrollada por el Consejo de Estabilidad Financiera. Estas instituciones entienden por *FinTech* a aquella "innovación habilitada tecnológicamente, que podría resultar en nuevos modelos de negocios, aplicativos, procesos o productos, asociados a un efecto significativo en los mercados e instituciones financieras y en la prestación de servicios financieros" (Comité de Supervisión Bancaria de Basilea, 2017, p. 8) [traducción libre][1].

A partir de la definición anterior, podemos concluir que *FinTech* no es cualquier prestación de servicios

[1] Texto original: "[…] technologically enabled financial innovation that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and the provision of financial services".

financieros a través de medios tecnológicos. La nota característica radicaría en que tal prestación ha de ser innovadora y capaz de producir efectos significativos en el sistema financiero.

Un equipo de trabajo del Fondo Monetario Internacional también ha hecho un esfuerzo por esclarecer el concepto de *FinTech*. He y otros explican que

> las *FinTech* aprovechan la explosión del *big data*, los avances en materia de inteligencia artificial, poder computacional, criptografía y el alcance del internet. Las fuertes complementariedades entre estas tecnologías están dando lugar a la impresionante formación de nuevos aplicativos relacionados con servicios que comprenden desde pagos hasta financiamiento, manejo de activos, seguros, y asesoría. Es así como surge la posibilidad de que las *FinTech* emerjan como alternativas competitivas frente a los intermediarios, mercados y estructuras financieras tradicionales (2017, p. 7) [traducción libre][2].

Siguiendo este orden de ideas, las *FinTech* se basan en los desarrollos tecnológicos más recientes, que no por ello dejan de ser variados. Consiguientemente, estos productos innovadores se apalancan de tecnología diversa para, asimismo, ofrecer productos vinculados con diferentes modalidades de servicios financieros.

En suma, se puede definir el concepto de *FinTech* como aquella innovación consistente en la aplicación de herramientas tecnológicas recientemente desarrolladas en la elaboración y prestación de productos y servicios financieros respectivamente, lo cual conlleva un impacto significativo en el funcionamiento, estructura y regulación de los mercados e instituciones financieras. Dichos productos y servicios innovadores pueden ser de diverso tipo –préstamos, gestión de finanzas empresariales y personales, pagos y remesas, financiamiento colectivo, banca digital, puntaje crediticio, identidad y fraude, negociación de activos y mercado de capitales, entre otros (Vodanovic Legal, 2019, p. 5)–, lo cual, sumado a la eficiencia aportada por las herramientas tecnológicas, permite a estos nuevos modelos de negocio competir con las entidades financieras tradicionales e, incluso, llegar a sectores relegados por estas.

2. Beneficios

Luego de delimitar el concepto de *FinTech*, resulta evidente que este nuevo modelo de negocios presenta múltiples beneficios para sus usuarios y el sistema financiero en general. Por un lado, Irene Peña y Fernando Rojas indican que "[l]as *FinTech* tienen la capacidad de aportar soluciones tendentes a optimizar el funcionamiento del sistema financiero en su conjunto, intensificando la competencia y reduciendo los costes para sus participantes" (2017, p. 9).

En efecto, al emplear la tecnología para ofrecer sus productos y servicios financieros, se logra mayor eficiencia en relación con aquellos ofrecidos por las empresas tradicionales del sistema financiero. De esta manera, la industria *FinTech* reduce sustancialmente el costo de transacciones en comparación con el dinero fiduciario (Harcourt, 2019, p. 18).

El caso de M-PESA demuestra cómo es que, en la realidad, las *FinTech* se presentan más eficientes en comparación con la banca tradicional y el manejo de dinero en efectivo. M-PESA es un servicio de transferencia de dinero vía móvil de origen keniano. En un país de baja bancarización, los usuarios de M-PESA destacan que dicho producto les permite enviar dinero a sus familias sin tener que viajar a diversas localidades; también es más seguro porque mitiga el riesgo de ser asaltado y, al poder llegar a cualquier lugar mientras se tenga un teléfono móvil, fomenta la inclusión financiera (Cairns & Thomas, 2010).

En línea con lo anterior, otra de las ventajas de las *FinTech* que resulta especialmente relevante en nuestro país es el acercamiento de tales servicios a sectores económicos emergentes cono lo son las micro, pequeñas y medianas empresas (en adelante, Mipymes), las cuales constituyen un sector relegado por la banca tradicional, contribuyendo también de esta forma a la bancarización de nuestra economía y a la inclusión financiera (Mendiola, 2020).

De acuerdo con la Superintendencia de Banca, Seguros y AFP (en adelante, SBS), a noviembre de 2020, existían en Perú 54 empresas de operaciones múltiples, de las cuales 16 pertenecen a la

[2] Texto original:

> FinTech leverages the explosion of big data on individuals and firms, advances in artificial intelligence, computing power, cryptography, and the reach of the internet. The strong complementarities among these technologies are giving rise to an impressive array of new applications touching on services from payments to financing, asset management, insurance, and advice. The possibility now looms that entities driven by FinTech may emerge as competitive alternatives to traditional financial intermediaries, markets, and infrastructures.

banca múltiple y representan el 90.08% del monto total de los activos de dichas empresas de operaciones múltiples (2020b). No obstante, solo una de dichas empresas de banca múltiple se encuentra especializada en microfinanzas: MiBanco, Banco de la Microempresa (Superintendencia de Banca, Seguros y AFP [SBS], 2020b).

Por el contrario, en el 9.92% restante, se tiene que 26 empresas de operaciones múltiples se especializan en microfinanzas. Estas son empresas financieras (5 de 10), cajas municipales (12 de 12), cajas rurales de ahorro y crédito (6 de 7) y entidades de desarrollo de la pequeña y mediana empresa, las Edpyme, (3 de 9) (SBS, 2020b).

Así las cosas, las *FinTech* constituyen una alternativa atractiva para el usuario microfinanciero. Este tipo de empresas contactan directamente a las Mipymes con nuevas posibilidades de crecimiento y fuentes de financiamiento. Al emplear la tecnología, ofrecen a estos usuarios préstamos más flexibles que los bancos tradicionales, con tasas de rendimiento atractivas (Da Re, 2015).

En la misma línea, Hoder, Wagner, Sguerra y Bertol señalan lo siguiente:

> Aunque muchas de las soluciones fintech hayan estado inicialmente enfocadas en la banca y los préstamos de consumidores, también hay muchas aplicaciones para las MiPyME. Las eficiencias obtenidas por medio del buen uso de las tecnologías modernas están creando opciones de financiamiento más atractivas para las MiPyME en todo el mundo. Las innovaciones en el financiamiento para las MiPyME profundizan nuestra comprensión de un mercado heterogéneo, reducen los costos de operación y aumentan los márgenes, fortalecen las capacidades de gestión de riesgos, y mejoran la capacidad empresarial y el potencial de crecimiento de las MiPyME (2016, p. 19).

En suma, la capacidad de adaptación a mercados heterogéneos y la reducción de costos que caracterizan a las *FinTech* las convierte en una alternativa idónea para el financiamiento de las Mipymes, sector que encuentra una reducida oferta especializada en el sistema financiero actualmente.

Lo anterior se ve reforzado con la última actualización del tope legal máximo de las tasas de interés aplicables a los préstamos ajenos al sistema financiero. De acuerdo con el artículo 1243 del Código Civil (1984)[3], la tasa máxima de interés convencional compensatorio o moratorio es fijada por el Banco Central de Reserva del Perú (en adelante, BCRP); limitación de la que se encuentran exoneradas las empresas del sistema financiero, pudiendo fijar libremente las tasas de interés para sus operaciones activas y pasivas en virtud del artículo 9 de la Ley General del Sistema Financiero (Ley 26702, 1996)[4].

Antes de agosto de 2019, el tope legal máximo de tasas de interés se establecía en función de la tasa promedio para créditos a microempresas. Ello, sumado a la exoneración otorgada a favor de las empresas del sistema financiero, colocaba a las *FinTech* –en su calidad de prestamistas exógenos al sistema financiero– en una situación de desventaja respecto de aquellas empresas financieras. Asimismo, al no poder cobrar tasas de interés superiores al límite comentado, se veían restringidas de poder atender a una demanda con mayor riesgo crediticio, pues no podían compensarlo con altas tasas de interés (Garvan, 2019).

Es en dicho contexto que, mediante la Circular 18-2019, el BCRP modificó el tope legal máximo para las tasas de interés ofrecidas por prestamistas fuera del sistema financiero, el cual ahora pasó a calcularse en virtud de la tasa promedio para créditos a microempresas o la tasa promedio del sistema financiero para créditos de consumo, la que sea mayor.

Dicho cambio fue gratamente acogido, particularmente, por las *FinTech*. En efecto, ello les permitirá aprovechar la nueva regulación para ingresar a mercados nuevos –por ejemplo, financiamiento a empresas exportadoras u otorgamiento de créditos vehiculares–, así como también dirigirse a segmentos no cubiertos por el sistema financiero,

---

[3] Artículo 1243.-

> La tasa máxima del interés convencional compensatorio o moratorio, es fijada por el Banco Central de Reserva del Perú. Cualquier exceso sobre la tasa máxima da lugar a la devolución o a la imputación al capital, a voluntad del deudor (Código Civil, 1984).

[4] Artículo 9.-

> Las empresas del sistema financiero pueden señalar libremente las tasas de interés, comisiones y gastos para sus operaciones activas y pasivas y servicios. Sin embargo, para el caso de la fijación de las tasas de interés deberán observar los límites que para el efecto señale el Banco Central, excepcionalmente, con arreglo a lo previsto en su Ley Orgánica. La disposición contenida en el primer párrafo del artículo 1243 del Código Civil no alcanza a la actividad de intermediación financiera […] (Código Civil, 1984).

tomando un mayor riesgo e incluyendo a más personas, como lo son aquellas sin historial crediticio (Fernández, 2019).

La industria *FinTech*, sin duda, resulta atractiva en la medida en que facilita el acceso a servicios financieros, promoviendo, especialmente, la inclusión financiera de sectores poco relacionados con la banca tradicional. En paralelo, este sector tradicional también ha empezado a adaptarse a los cambios propuestos por las *FinTech* para así poder competir ante la presencia de productos y servicios financieros disruptivos. A modo de ejemplo, en 2019, el holding Credicorp –al cual pertenece el Banco de Crédito del Perú (BCP)– efectuó una inversión de US$ 1 000 000.00 (Un millón y 00/100 dólares de los Estados Unidos de América) en Independencia, una *FinTech* local dedicada al otorgamiento de préstamos personales en línea (Rojas, 2019). Asimismo, en septiembre de 2020, la aplicación de compras a domicilio Rappi anunció una alianza estratégica con Interbank para impulsar la banca digital en Perú, integrando servicios financieros de una empresa bancaria en la plataforma de una *FinTech* a través de *Application Programming Interfaces* (APIs) (Ernst & Young, 2020, p. 52).

En conclusión, es indiscutible que las *FinTech* presentan diversas ventajas para los usuarios de estas y el mercado en general. Sin embargo, como se desarrollará a continuación, este tipo de compañías innovadoras también traen consigo ciertos desafíos para los reguladores.

3. Desafíos

Sin perjuicio de los beneficios descritos en la sección precedente, desde el punto de vista regulatorio, el fenómeno *FinTech* representa un conjunto de retos no menores que, inevitablemente, han de ser enfrentados por las entidades competentes en tanto la tendencia a migrar hacia servicios financieros tecnológicos no parece ir en retroceso, sino todo lo contrario.

Claudia Vásquez resalta como desafíos del regulador financiero **(i)** la protección del consumidor de los servicios proporcionados por las *FinTech* y **(ii)** el carácter internacional de estos nuevos servicios:

> El desafío es en encontrar el equilibrio entre la protección del consumidor y la innovación en el sector financiero por el surgimiento de competidores como FinTech e InsurTech. La desconfianza del consumidor frente al sector financiero tradicional se explica entre tantos factores porque siente que no se protegen sus derechos, lo que hace que busque nuevas alternativas en un contexto digital internacional y globalizado, por lo tanto, este consumidor deja de ser un consumidor financiero para convertirse en un consumidor internacional. Las FinTech e InsurTech no tienen una limitación geográfica para el ejercicio de su actividad, ellos están en Internet y todos los individuos del planeta tienen acceso a los servicios que ofrecen, la protección al consumidor internacional es una pieza clave para el desarrollo económico mundial en esta era digital (2018, p. 250).

En consecuencia, el regulador tendría como desafío fomentar la innovación del sector financiero, buscando el equilibrio con la protección del usuario de los productos y servicios *FinTech*; al igual que también debe tener en cuenta que, a pesar de encontrarse limitado por el alcance de su jurisdicción, estos productos y servicios se ofrecen en un contexto globalizado y, por ende, no es extraño que parte de sus procesos se lleve a cabo en el exterior, lo que limita su capacidad de regulación.

Por otro lado, los inversionistas perciben como uno de los principales obstáculos para el desarrollo de emprendimientos *FinTech* el hecho de que sus propuestas tecnológicas, por lo general, no pueden ser implementadas efectivamente por la presencia de barreras normativas y legales (Vodanovic Legal, 2019, p. 38). Adicionalmente, así como una excesiva regulación puede frenar el desarrollo de estas innovaciones, la ausencia de una regulación especializada también es considerada un obstáculo para la ejecución de las *FinTech*. Esta situación genera incertidumbre en los inversionistas, al no tener claridad respecto al panorama legal o las 'reglas de juego' que regirán la implementación de sus proyectos, lo que termina constituyendo un desincentivo para decidir ejecutarlos (Vodanovic Legal, 2019, p. 38).

De acuerdo con Alison Harcourt , existen otras barreras a la entrada de nuevos proveedores de servicios financieros:

> Por décadas, los servicios financieros han sido operados por agentes establecidos (bancos e intermediarios) con culturas que, por lo general, han ralentizado la adopción de tecnologías y constituyeron barreras de entrada a nuevos operadores. De manera similar, las soluciones tecnológicas desarrolladas por las compañías de tecnología más grandes a nivel mundial generan problemas de concentración de mercado, bloqueo de clientes y falta de interoperabilidad. Por último, la necesidad de autenticación del consumidor suele requerir tecnologías como lector de huella digital en los dispositivos, reconocimiento facial y de voz, así como data biométrica, la cual es cada

> vez más usada para validar identidades (2009, p.18) [traducción libre][5] .

Así, los inversionistas interesados en llevar a cabo un emprendimiento *FinTech* no solo deben enfrentar barreras legales para su ingreso al mercado. También encontramos otras de carácter estratégico, basadas en la conducta de los actuales competidores; al igual que barreras operativas, las que se refieren, básicamente, al empleo de tecnología que permita la adecuada validación de las identidades de los usuarios, protegiéndolos y, como consecuencia de ello, logrando que el público mantenga su confianza en las *FinTech*.

Finalmente, Irene Peña y Fernando Rojas sintetizan adecuadamente lo explicado en los párrafos precedentes en relación con los desafíos que trae consigo la industria *FinTech*:

> […] dado su carácter innovador, sus implicaciones para la economía real son, en muchos casos, difíciles de mesurar. Por ello, la respuesta desde el ámbito regulatorio debe ser equilibrada, evitando excesos normativos que penalicen su correcto desarrollo y contribución a la creación de un sistema financiero más robusto, pero, a su vez, ofreciendo las garantías necesarias a los consumidores de estos productos (2017, p. 9).

En suma, la industria *FinTech* tiene el potencial para generar un verdadero impacto positivo en el mercado financiero, lo que se traduciría en bienestar para sus usuarios. Sin embargo, para que ello pueda efectivamente materializarse, es necesario que estos emprendimientos encuentren un ambiente regulatorio idóneo destinado a alcanzar un equilibrio entre **(i)** la flexibilización de ciertos requisitos normativos que limitan el desarrollo de innovaciones tecnológicas y, por otro lado, **(ii)** la protección al consumidor financiero. Esto último es relevante, pues coadyuva a que los ciudadanos tengan confianza en el sistema financiero y se animen a participar en él, fomentando la dinámica de dicho sistema.

B. Regulación del fenómeno *FinTech* en el extranjero

Tal como se ha desarrollado en la sección precedente, las *FinTech* presentan retos no menores para el regulador financiero. Como se ha señalado en la introducción del presente trabajo, parece ser que la estrategia de nuestro regulador consiste en implementar desarrollos normativos selectivos y centrados en actividades que, a su criterio, requieren normas concretas y especializadas –sea por su grado de desarrollo o riesgos asociados, entre otros factores–; por lo que no se ha optado, por el momento, por emitir una 'Ley *FinTech*' como sí lo han hecho otros países (Vodanovic Legal, 2019, p. 48). A la fecha, solo contamos con el Decreto de Urgencia y el Reglamento FPF, los cuales regulan la actividad de *crowdfunding*.

Asimismo, se ha indicado que la experiencia en otros países ha sido distinta. En algunos casos, se ha optado por abordar el fenómeno *FinTech* a nivel regulatorio, generando así seguridad jurídica respecto al panorama legal para el desarrollo de tales emprendimientos. Ello, evidentemente, se ve reflejado en un mayor número de *FinTech* en comparación con el del caso peruano, que supera por poco el centenar. A continuación, se realizará una revisión de los modelos regulatorios implementados en el extranjero, para lo cual se observará específicamente a los países con mayor desarrollo de emprendimientos *FinTech* de la región –Brasil, México y Colombia–, así como también a España, que ha desarrollado en los últimos años un importante marco normativo al respecto y cuyo ordenamiento jurídico es un referente constante en el desarrollo de la regulación peruana; y al Reino Unido, el cual es el país líder en la materia a nivel mundial.

1. Brasil

En el año 2020, Brasil acogía –aproximadamente– a 771 *FinTech* (Statista, 2020). Ello no es fortuito. Por el contrario, el gobierno brasileño ha implementado una serie de medidas que favorecen el desarrollo de este tipo de empresas.

En el plano regulatorio, la Comisión de Valores Mobiliarios promulgó en 2017 el Instruçao CVM 588. En virtud de este, se reguló el *equity crowdfunding* u oferta de valores mobiliarios bajo plataformas digitales; dispensando de su registro ante la entidad a las micro y pequeñas empresas que sean emisoras en el marco de dicha modalidad de oferta (Vodanovic Legal, 2019, p. 14). Posteriormente, en 2018, el Consejo Nacional Monetario Nacional de

[5] Texto original:

> Financial services have for decades been operated by established incumbents (banks and intermediaries) with cultures that often slowed technological adoption and barred entry for new operators. Similarly, technological solutions are developed by the largest tech companies worldwide presenting problems of market concentration, customer lock in and lack of interoperability. Lastly, the need for customer authentication often requires technologies such as device fingerprinting, voice and facial recognition as well as biometric data which is increasingly used to authenticate identity.

Brasil emitió la Resolução 4.656, la cual estableció los requisitos y procedimientos aplicables a entidades financieras dedicadas a otorgar préstamos mediante plataformas digitales, a través de las modalidades de préstamo directo y *peer-to-peer* (Vodanovic Legal, 2019, p. 14).

Si bien las medidas regulatorias antes indicadas aclararon el panorama legal aplicable a las *FinTech*, lo que facilita su desarrollo, también se ha implementado iniciativas de promoción directa de las *FinTech*. Entre ellas, destaca la creación del Centro de Innovación de Tecnología Financiera –FinTech Hub– por parte de la Comisión de Valores Mobiliarios en 2016. El FinTech Hub brasileño tiene por objetivo investigar y analizar el desarrollo de la implementación de nuevas tecnologías en el mercado de valores de dicho país (Vodanovic Legal, 2019, p. 15).

En paralelo, la sociedad civil también se ha visto involucrada en el fomento de las *FinTech*. En 2018, se implementó el Laboratorio de Innovaciones Financieras y Tecnológicas (LIFT), el cual es un espacio colaborativo virtual impulsado por Fenasbac –sociedad civil sin fines de lucro–, en coordinación con el Banco Central de Brasil, empresas de tecnología y especialistas en la materia (Vodanovic Legal, 2019, p. 15).

Por último, también destacan el Laboratorio de Inovaçao Financiera –proyecto conjunto de la Asociación Brasileña de Desarrollo, el Banco Interamericano de Desarrollo y la Comisión de Valores Mobiliarios– y el Canal do Desenvolvedor MPME del Banco Nacional de Desarrollo Económico y Social de Brasil, el cual está destinado al financiamiento de las *FinTech* (Vodanovic Legal, 2019, p. 15).

Como se puede apreciar, en Brasil, las *FinTech* no solo cuentan con un ecosistema legal que, ante todo, les provee seguridad jurídica, sino que también –desde ya algunos años– se vienen implementando proyectos destinados a su desarrollo y financiamiento.

2. México

En Latinoamérica, México le sigue los pasos a Brasil en cuanto al desarrollo *FinTech* con un aproximado de 414 en el 2020 (Ernst & Young, 2020, p. 10). En este caso, aquel desarrollo tampoco es fortuito, pues hay un adecuado desarrollo normativo sobre la materia, así como también se han implementado diversas iniciativas para fomentar este tipo de emprendimientos tecnológicos.

A diferencia de los enfoques peruano y brasileño, que optan por una regulación especializada de las diversas manifestaciones de las *FinTech*, en México, se cuenta con una Ley *FinTech* (Ley para Regular las Instituciones de Tecnología Financiera, 2018). Promulgada en 2018, se basa en los principios de inclusión e innovación financiera, promoción de la competencia, protección al consumidor, preservación de la estabilidad financiera, prevención de operaciones ilícitas y neutralidad tecnológica; y establece el marco regulatorio aplicable a las denominadas Instituciones de Tecnología Financiera, los servicios prestados por estas, su organización, operación y funcionamiento.

La Ley *FinTech* regula de manera general los diversos tipos de emprendimientos *FinTech* como, por ejemplo, el *equity crowdfunding* y el *lending crowdfunding*, al igual que las criptomonedas o "activos virtuales" (Vodanovic Legal, 2019, p. 11). Expertos destacan que este cuerpo legal obliga a las entidades financieras a contar con interfaces de programación de aplicaciones informáticas (en adelante, API, por sus siglas en inglés), de modo tal que permitan compartir los datos de sus clientes con terceros proveedores, bajo ciertos requisitos (Vodanovic Legal, 2019, p. 11).

Entre las iniciativas de promoción de la industria *FinTech* en México, se encuentran concursos para el desarrollo de proyectos y grupos de discusión sobre la materia (Vodanovic Legal, 2019, p. 12). Sin embargo, destaca el recurso a los *sandboxes* regulatorios, introducidos por la Ley *FinTech* bajo la figura de 'Modelos Novedosos'.

Así las cosas, la Embajada del Reino Unido en México junto con las empresas DAI México y Distrito Emprendedor, vienen implementando el Sandbox Challenge. Se trata del primer concurso de innovación financiera destinado a probar nuevos modelos de negocio en el sistema financiero, mediante el esquema de Modelos Novedosos introducido por la Ley *FinTech*; es decir, aquellos emprendimientos dedicados desarrollar una actividad financiera que requiere autorización o registro por parte del regulador, utilizando tecnológicas innovadoras o en modalidades diferentes a las existentes actualmente en el mercado (Sandbox Challenge, 2020).

Dicho todo lo anterior, se puede concluir que, al igual que Brasil, México ofrece claridad legal a quienes deseen desarrollar modelos de negocios *FinTech*, así como también existen diversas iniciativas al amparo del propio marco regulatorio para su promoción.

3. Colombia

Un tercer ejemplo latinoamericano es el caso colombiano. Al cierre de 2020, existían en Colombia

200 *FinTech* (Finnovista, 2020). El regulador colombiano ha combinado el tratamiento normativo general de las *FinTech* con el especializado, aunque con mayor tendencia a este último.

Por un lado, el Decreto 661 de 2018 modificó el Decreto 2555 de 2010 –el cual regula el sector financiero, de seguros y el mercado de valores– para reconocer y regular la actividad de asesoría financiera a través de medios tecnológicos en el mercado de valores (Vodanovic Legal, 2019, p. 17).

Ahora bien, en relación con la regulación especializada según los diversos modelos de *FinTech*, la Ley 1735 de 2014 reconoce y regula a las Sociedades Especializadas en Depósitos y Pagos Electrónicos (SEDPE), las cuales se dedican a captar recursos a través de depósitos electrónicos, envío y recibo de giros financieros, entre otras actividades adicionales (Vodanovic Legal, 2019, p. 17). Finalmente, mediante Decreto 1357 de 2018, se emitió la regulación aplicable al *equity crowdfunding*, actividad sujeta a autorización de la Superintendencia Financiera de Colombia (en adelante, SFC) (Vodanovic Legal, 2019, p. 17).

En adición al desarrollo normativo descrito, la SFC creó en 2017 InnovaSFC, un grupo de trabajo de innovación financiera y tecnológica destinado a facilitar la innovación en el sector financiero. Sus objetivos son acompañar la innovación al servicio del consumidor financiero, apoyar los desarrollos innovadores que promueven la inclusión y la educación financiera, apoyar el desarrollo y la innovación financiera y tecnológica, y promover la innovación sostenible (Superintendencia Financiera de Colombia [SFC], 2020).

Consiguientemente, la SFC implementó tres mecanismos en el marco de Innova SFC para lograr los objetivos planteados: **(i)** elHub u oficina destinada al acompañamiento y asesoría en materia de innovación financiera y tecnológica; **(ii)** laArenera o el marco dispuesto para la realización de pruebas de negocios de innovación financiera y tecnológica en un espacio de control y supervisión; y **(iii)** *RegTech* o la herramienta por la cual se toman los desarrollos tecnológicos para apalancar la innovación dentro de la propia SFC (SFC, 2020). Cabe resaltar que, a la fecha, elHub cuenta con 182 iniciativas, ocho proyectos han sido aceptados para su prueba en laArenera y se han realizado cinco pilotos de *RegTech* (SFC, 2020).

En suma, Colombia presenta recientes esfuerzos legislativos e institucionales para el desarrollo de un marco regulatorio aplicable a ciertas *FinTech* y para fomentarlas. Resulta interesante el empleo de diversos mecanismos para lograr tales objetivos, lo que incluye procesos de innovación, incluso, al interior del supervisor. Todo ello hace que sea lógico concluir que, a pesar de contar con un número modesto de *FinTech*, el crecimiento de este sector despegará en Colombia, siguiendo el ritmo de Brasil y México.

4. España

También conviene revisar el caso de España en tanto ha presentado un importante desarrollo de la industria *FinTech* en los últimos años –existiendo, a septiembre de 2020, un total de 406 *FinTechs* en dicho país (Abanca Innova, 2021)–; así como también porque el ordenamiento jurídico español es un referente constante en el desarrollo regulatorio peruano. De hecho, España también ha optado por un enfoque especializado al regular las *FinTech*, pues el regulador ha ido desarrollando normativas especializadas para diversos tipos de tecnologías financieras, sin elaborar una ley marco general.

Por un lado, respecto al ordenamiento comunitario, resalta la Directiva 2015/2366 sobre servicios de pago, más conocida como PSD2, la cual incorporó los cambios tecnológicos en la regulación de dichos servicios, reforzó los requisitos de seguridad para los servicios de pago electrónicos y abrió dicho mercado a terceros sin licencia bancaria (pero autorizados y registrados) (Lema, 2018, pp. 51-52). Publicada en 2015 a nivel europeo, pero con efectos legales en España desde la promulgación del Real Decreto-Ley 19/2018 en 2018, sentó las bases "para la puesta en marcha de un nuevo escenario con mayores oportunidades al establecer objetivos más ambiciosos para el entorno competitivo del sector financiero, tanto para las entidades financieras tradicionales como para las fintech y empresas de otros sectores" (Lema, 2018, p. 51).

Adicionalmente, encontramos en el ordenamiento jurídico español la Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial, que regula el *crowdfunding*. De acuerdo con Zunzunegui dicha norma representa un marco regulatorio de máximos, que regula al detalle los estatutos de las plataformas de *crowdfunding*, por lo que es de carácter intervencionista, paternalista y protector del *statu quo* bancario (2015, p. 7).

Más recientemente, se ha promulgado la Ley 7/2020, de 13 de noviembre, para la transformación digital del sistema financiero, en virtud de la cual se regula un "entorno controlado de pruebas que permita llevar a la práctica proyectos tecnoló-

gicos de innovación en el sistema financiero con pleno acomodo en el marco legal y supervisor, respetando en todo caso el principio de no discriminación" (2020, art. 1). Como consecuencia de ello, en febrero de este año el *sandbox FinTech* español cerró su primera convocatoria para la postulación de proyectos, presentándose en total 67 iniciativas piloto a fin de ser evaluadas por la Comisión de Coordinación (Ministerio de Asuntos Económicos y Transformación Digital, 2021).

Así las cosas, España destaca por presentar un esfuerzo normativo por brindar reglas claras para el desarrollo de las *FinTech* –lo cual se plasma en la cantidad de dichas empresas en el país–, al mismo tiempo que cuenta iniciativas para fomentar el desarrollo de estas a través de programas como el *sandbox FinTech*.

5. Reino Unido

Por último, al estudiar las *FinTech*, no se puede dejar de mencionar al Reino Unido, país líder a nivel mundial en la innovación financiera y tecnológica. Resalta el rol de la Financial Conduct Authority (en adelante, FCA), quien, en los últimos años, se ha encargado de regular y promover la industria *FinTech* en el Reino Unido.

En el año 2014, la FCA creó Project Innovate, constituyendo un grupo de trabajo para el desarrollo de las siguientes iniciativas: **(i)** un *sandbox* regulatorio, permitiendo probar nuevos modelos de negocios, sus productos y servicios, en un espacio controlado y bajo la supervisión de la FCA; **(ii)** una unidad de asesoría destinada a brindar *feedback* a compañías que desarrollan modelos automatizados de asesoría regulatoria a bajo costo y guía al consumidor; y **(iii)** un *hub* de innovación que ofrece contacto directo y apoyo a empresarios que deseen solicitar una autorización o variación en los permisos del regulador (Global Legal Insights, 2020).

Definitivamente, la iniciativa del *sandbox* regulatorio ha sido la de mayor impacto. La profesora Alison Harcourt destaca que Londres se ha convertido en un *hub* internacional de la industria *FinTech* a partir de la implementación del primer *sandbox* a nivel mundial en el 2016 por parte de la FCA (2019, p. 16). Es así como la tasa de crecimiento anual de *FinTech* fue de 22% entre 2014 y 2016; mientras que, en 2018, se contaba con más de 1 600 *FinTech* que representaron un valor de 6.6 mil millones de libras esterlinas al Reino Unido (Harcourt, 2019, p. 16).

En dicho contexto, el primer *sandbox* impulsado por la FCA contó con la participación de 18 emprendimientos, seleccionados entre 69 solicitantes. A la fecha, la FCA cuenta desde 2019 con el quinto *sandbox* regulatorio en el que participan 29 *FinTech*, seleccionadas de un total de 99 postulantes (Financial Conduct Authority [FCA], 2020) y, en 2018, estableció el primer *sandbox* global: el Global Financial Innovation Network (en adelante, GFIN), que, de 44 solicitudes, cuenta con ocho participantes, que son acompañados por reguladores de 33 jurisdicciones (FCA, 2019; Global Financial Innovation Network [GFIN], 2019).

La exitosa experiencia del Reino Unido fue rápidamente replicada en diversos países como Dinamarca, Noruega, Alemania, Irlanda, Países Bajos, Suecia, Hong Kong, Australia, Singapur o Corea del Sur. Adicionalmente, como ya se ha desarrollado, México y Colombia, dos de los países latinoamericanos con mayor crecimiento de los emprendimientos *FinTech*, también vienen implementando *sandboxes*.

En conclusión, el modelo británico de regulación y promoción de las *FinTech* es, sin duda, un caso de éxito digno de ser observado y estudiado. Particularmente, el empleo de un *sandbox* regulatorio como herramienta para promover el desarrollo de negocios *FinTech* representa una oportunidad para que proyectos verdaderamente innovadores y con potencial de generar un impacto significativo en el mercado sean probados en la realidad, pero siempre bajo la regulación y cercana supervisión de la autoridad.

6. Balance sobre las experiencias extranjeras destacadas

A modo de resumen, se puede apreciar en el siguiente cuadro las medidas regulatorias y de fomento de las *FinTech* implementadas en Brasil, México, Colombia y el Reino Unido; así como el número aproximado de dichos negocios desarrollados en estos países (ver Cuadro 1).

Lo anterior evidencia que la fructífera experiencia del Reino Unido tras la implementación de los *sandboxes* regulatorios también ha sido replicada en algunos países latinoamericanos, lo que ha permitido un notable desarrollo de la industria *FinTech* en la región. A pesar de que países como México y Colombia cuentan con distintas culturas y ordenamientos jurídicos respecto al Reino Unido –pero más cercanos a la cultura y ordenamiento jurídico peruanos–, la flexibilidad de esta herramienta regulatoria la hace fácilmente adaptable a distintos contextos. De esta manera, resulta relevante analizar la importancia de la implementación de un *sandbox* regulatorio para el desarrollo de las *FinTech* en el Perú.

Cuadro 1

	Brasil	México	Colombia	España	Reino Unido
Medidas Regulatorias	▪ Instruçao CVM 588 (*equity crowdfunding*) ▪ Resolução 4.656 (préstamos directos y *peer-to-peer* bajo plataformas digitales)	▪ Ley *FinTech* (Ley para Regular las Instituciones de Tecnología Financiera, 2018)	▪ Decreto 661 de 2018 (asesoría financiera a través de medios tecnológicos) ▪ Ley 1735 de 2014 (Sociedades Especializadas en Depósitos y Pagos Electrónicos –SEDPE). ▪ Decreto 1357 de 2018 (*equity crowdfunding*)	▪ Real Decreto-Ley 19/2018 (servicios de pago). ▪ Ley 5/2015 (fomento de la financiación empresarial – *crowdfunding*)	—
Medidas de Promoción	▪ Centro de Innovación de Tecnología Financiera – FinTech Hub (Comisión de Valores Mobiliarios). ▪ Laboratorio de Innovaciones Financieras y Tecnológicas –LIFT (Fenasbac, Banco Central de Brasil, entre otros). ▪ Laboratorio de Inovaçao Financiera (Asociación Brasileña de Desarrollo, Banco Interamericano de Desarrollo y Comisión de Valores Mobiliarios). ▪ Canal do Desenvolvedor MPME (Banco Nacional de Desarrollo Económico y Social de Brasil).	▪ Concursos para el desarrollo de proyectos y grupos de discusión sobre la materia. ▪ **Sandbox Challenge**, para 'Modelos Novedosos'.	▪ InnovaSFC: (i) elHub. (ii) **laArenera.** (iii) *RegTech*.	▪ ***Sandbox FinTech***.	▪ Project Innovate: (i) ***sandbox*;** (ii) Unidad de Asesoría; (iii) *Hub* de Innovación.
Número de *FinTech* en 2020 (aprox.)	771	414	200	406	1 600[6]

Fuente: Elaboración propia a partir de las fuentes citadas en la presente sección II.

III. MARCO TEÓRICO-NORMATIVO

Para efectos del desarrollo del presente trabajo de investigación, se realizará un análisis cualitativo a partir de la consulta de –principalmente– fuentes extranjeras. Estas fuentes incluyen tanto doctrina como legislación, además de documentos oficiales de reguladores financieros de diversos países e internacionales. Cabe resaltar que se trata de información producida en los últimos años, debido a la novedad del fenómeno *FinTech* y, especialmente, de los *sandbox* regulatorios implementados para fomentar estos emprendimientos.

Sin perjuicio de ello, no se dejará de consultar doctrina y legislación nacional; ello con la finalidad de entender el problema concreto desde el que partimos, al igual que para evaluar la factibilidad de la propuesta de implementación de un *sandbox* regulatorio en Perú.

IV. DESARROLLO

A partir de lo señalado en la sección II, se puede observar que uno de los mecanismos más utilizados para la promoción y desarrollo de los modelos de negocios *FinTech* a nivel mundial es una herramienta conocida como *sandbox* regulatorio. En tal sentido, en el presente apartado, se analizará la importancia de la aplicación de dicha herramienta para promover la industria *FinTech* en Perú.

A. Concepto de *sandbox* regulatorio

Al igual que el concepto de *FinTech*, el de *sandbox* también ha sido considerado de tal relevancia entre los reguladores internacionales que el Comité de Supervisión Bancaria de Basilea lo define como "una prueba en tiempo real de nuevos productos o servicios en un ambiente controlado, en el que destaca una cooperación activa del supervisor y el

[6] Cifra correspondiente al año 2019 (Department for International Trade & HM Treasury, 2019, p. 12).

otorgamiento de dispensas en relación con la regulación aplicable por parte de dicha autoridad" (2017, p. 40) [traducción libre][7].

La definición propuesta por el Comité de Supervisión Bancaria de Basilea también ha sido acogida a nivel doctrinario. A modo de ejemplo, Aguilar y Lluesma señalan que el *sandbox* es "un espacio controlado por el regulador en el que las entidades pueden probar sus ideas innovadoras con exención del cumplimiento de determinados requisitos o con garantías en caso de que no haya marco regulatorio aplicable" (2019, p. 95).

Consiguientemente, el *sandbox* regulatorio implica la implementación de un espacio controlado de pruebas, en el que pueden operar productos y servicios innovadores en tiempo real dentro de un marco regulatorio reducido o flexibilizado, pero bajo una cercana supervisión de la autoridad competente. De esta manera, si bien se encuentran sujetas a ciertas limitaciones, las *FinTech* pueden probar sus negocios y realizar los ajustes pertinentes, sin frenar su innovación y desarrollo.

Por su parte, Ahn, Lee y Choi destacan que un *sandbox* regulatorio permite que las *FinTech* se incorporen con mayor facilidad al mercado, pero sin estar exentas de control y supervisión:

> Un *sandbox* regulatorio es un marco establecido por un regulador que permite a las *FinTech* y otros innovadores llevar a cabo experimentos en tiempo real en un espacio controlado bajo la supervisión del regulador y con menores restricciones. Ello ayuda a que la innovación tecnológica genere nuevos productos y servicios creativos, y a que estos ingresen más fácilmente al mercado (2019, p. 1) [traducción libre][8].

En efecto, los *sandboxes* regulatorios también representan para las *FinTech* una puerta de ingreso al mercado. Se trata de un ingreso bajo ciertas dispensas regulatorias, pero, asimismo, de manera ordenada y controlada. Ello permite prestar atención ante cualquier posible falla del producto o servicio, pudiendo realizarse ajustes inmediatamente y continuar con las pruebas en el mercado.

B. Características

A fin de dar mayor claridad al concepto de *sandbox* regulatorio y su funcionamiento, a continuación, se explicarán brevemente sus principales características. Según el Comité de Supervisión Bancaria de Basilea, estos rasgos característicos se encuentran referidos a (i) el ingreso al *sandbox*, (ii) el otorgamiento de dispensas o flexibilizaciones regulatorias temporales y (iii) la restricción a las condiciones en las que operan sus participantes (2017, p. 40).

1. Ingreso al *sandbox*

Una de las particularidades de los *sandboxes* regulatorios es que, quienes desean ingresar y someter a prueba sus modelos de negocio *FinTech*, deben pasar previamente por un concurso. Es decir, no cualquier interesado puede tocar la puerta del regulador y solicitar su ingreso al *sandbox*.

Son varios los criterios que suelen requerirse a los postulantes de los diversos *sandboxes*. Por ejemplo, que el producto o servicio a ser probado sea genuinamente innovador, que genere un beneficio al consumidor, que resulte difícil encuadrarlo dentro de las figuras preexistentes en el marco regulatorio vigente y que se encuentre listo para salir al mercado (Comité de Supervisión Bancaria de Basilea, 2017, p. 40).

En tal sentido, el estándar de admisión suele ser bastante elevado y es por tal motivo que la mayoría de los postulantes al *sandbox* no ingresan a este ambiente controlado de pruebas. Tal como se ha mencionado, cuando se implementó el primer *sandbox* impulsado por la FCA en el Reino Unido, se presentaron 69 solicitantes, de los cuales solo fueron admitidos 18 emprendimientos (FCA, 2020). Esta particularidad tampoco ha cambiado con el paso de los años: de los 99 postulantes al *sandbox* implementado más recientemente, se eligieron a 29 *FinTech*; mientras que se recibieron 44 solicitudes para acceder al nuevo GFIN, pero solo ocho proyectos fueron los elegidos para participar (FCA, 2020; GFIN, 2019).

[7] Texto original:

> A regulatory sandbox usually refers to live testing of new products or services in a controlled environment. Sandboxes may be considered to be more than just a dialogue or an informal exchange as they engage a supervisor's active cooperation during the test period. Sandboxes also imply the use of legally provided discretions by the supervisory agency.

[8] Texto original:

> A regulatory sandbox is a framework set up by a regulator that allows FinTech start-ups and other innovators to conduct live experiments in a controlled environment under a regulator's supervision and with fewer restrictions. It helps technological innovation lead to creative new products and services and helps bring these more easily into the market.

Lo anterior se vincula con lo señalado en la sección II sobre el concepto de *FinTech*: si bien este término puede ser utilizado cotidianamente para referirse a diversas manifestaciones de negocios que emplean la tecnología en las finanzas, lo cierto es que el concepto se ciñe a aquellos productos y servicios financieros basados en tecnología novedosa, con potencial de generar un verdadero impacto innovador en el mercado y al consumidor. Esta delimitación actuaría como filtro, lo que le permite al regulador centrar todos sus esfuerzos en aquellos productos o servicios respecto de los cuales sí valga la pena ajustar o flexibilizar la regulación aplicable en atención a su carácter innovador y disruptivo.

2. Otorgamiento de dispensas o flexibilizaciones regulatorias temporales

Como se ha reiterado a lo largo del presente trabajo, los productos y servicios financieros ofrecidos por los negocios *FinTech* suelen ser tan innovadores y novedosos que, por lo general, sus inversionistas advierten que sus propuestas tecnológicas no pueden ser implementadas efectivamente por la presencia de barreras normativas y legales que constriñen y limitan el desarrollo de dichos negocios (Vodanovic Legal, 2019, p. 38). Similarmente, la ausencia de una regulación especializada también es considerada un obstáculo para la ejecución de las *FinTech*, pues genera incertidumbre en los inversionistas, al no tener claridad respecto al panorama legal o la normativa que regirá la implementación de sus proyectos, lo que termina constituyendo un desincentivo para decidir ejecutarlos (Vodanovic Legal, 2019, p. 38).

En ese sentido, los *sandboxes* regulatorios permiten operar tales productos y servicios otorgando ciertas dispensas temporales respecto de la regulación aplicable, para así probar la viabilidad de los proyectos seleccionados. Ahora bien, debe resaltarse que las barreras legales no solo se encuentran en la regulación prudencial del sistema financiero; pues también se hallan en las normas relacionadas con la protección de datos personales, protección al consumidor o prevención del lavado de activos y financiamiento del terrorismo, por lo que es usual que se exija a los participantes del *sandbox* informar a sus consumidores y demás *stakeholders* que la compañía en cuestión se encuentra ofreciendo el producto o servicio innovador en el marco de un *sandbox* regulatorio (Comisión de Supervisión Bancaria de Basilea, 2017, p. 40).

Se puede apreciar, entonces, que la implementación de un *sandbox* regulatorio demanda un especial compromiso del regulador para otorgar temporalmente dispensas o flexibilizar ciertas exigencias regulatorias con el propósito de que los productos y servicios de sus participantes sean realmente puestos a prueba y puedan operar en el mercado. Al mismo tiempo y por tal motivo, el regulador también debe obligarse a supervisar de cerca a los participantes del *sandbox* y efectuar los ajustes regulatorios cuando corresponda, en caso de que el 'marco normativo a medida' no haya resultado completamente adecuado.

3. Restricción a las condiciones en las que operan los participantes

El hecho de que el *sandbox* regulatorio sea reconocido como un 'espacio controlado de pruebas' no viene únicamente de la constante supervisión de la autoridad responsable. En adición a ello, dicha autoridad suele imponer una serie de restricciones a la forma en la que se ofrecen los productos y se prestan los servicios de los participantes, de modo tal que se mitigue en la mayor medida posible el riesgo inherente a estas actividades.

En efecto, de por sí, cualquier forma de negocio que involucre el manejo de los ahorros del público representará un riesgo que debe ser observado por el regulador, máxime si consideramos que ello ha recibido tutela a nivel constitucional[9]. Siguiendo este orden de ideas, al no tener el regulador suficiente certeza sobre la magnitud de los riesgos de las *FinTech* debido a su novedad y –en ciertos casos– complejidad o incomprensión al respecto, así como la provisionalidad del marco regulatorio aplicable a los participantes del *sandbox*, es evidente que sus actividades conllevarán una serie de riesgos.

Por tal motivo, se pretende mitigar aquellos riesgos –en su mayoría, desconocidos o indeterminados– minimizando el alcance del ofrecimiento de los productos y servicios bajo prueba, dirigiéndolo hacia consumidores y transacciones que resulten cuantitativa y cualitativamente suficientes para obtener la data necesaria para analizar las pruebas de los proyectos de los participantes. Algunas de las restricciones o parámetros que tradicionalmente se imponen a los participantes de los *sandboxes* regulatorios se encuentran relacionados con el número máximo permitido de clientes con los que los participantes pueden contratar, especificación del consumidor permitido, niveles máximos de

[9] El artículo 87 de la Constitución Política del Perú establece lo siguiente: "El Estado fomenta y garantiza el ahorro. La ley establece las obligaciones y los límites de las empresas que reciben ahorros del público, así como el modo y los alcances de dicha garantía […]" (1993).

transacciones, entre otras (Comité de Supervisión Bancaria de Basilea, 2017, p. 40).

En conclusión, todas las características propias de los *sandboxes* regulatorios se orientan a lograr el equilibrio entre la promoción de las *FinTech*, el desarrollo de modelos innovadores y su ingreso al mercado de la mano con ciertas dispensas regulatorias, pero sin perder de vista la protección al consumidor y al sistema financiero en general.

C. ¿Por qué optar por la implementación de un *sandbox* regulatorio?

Como se desprende de lo explicado líneas arriba, la idea detrás de un *sandbox* regulatorio es otorgar flexibilidad a sus participantes para que puedan innovar y probar sus productos y servicios financieros mientras se encuentran en una etapa previa a la salida oficial al mercado. Ello implica la exención de diversos requisitos normativos, lo que nos lleva prácticamente a tener una 'regulación a la medida' de cada participante. Asimismo, cabe precisar que las 'reglas de juego' aplicables al *sandbox* varían dependiendo del país en el que se implemente: por ejemplo, dependiendo de la jurisdicción, existen criterios diversos respecto de su duración, tipo de participantes –combinación de agentes tradicionales y *amateurs* o solo estos últimos–, entre otros.

Evidentemente, se trata de una propuesta atractiva y de vanguardia, pero no es la única de la que puede echar mano el regulador. Otra alternativa igualmente válida –a la que se denominará, para efectos del presente trabajo, 'Autorización Simplificada'– sería que dicho regulador simplificara de modo general los requisitos normativos para otorgarle autorizaciones de funcionamiento a las *FinTech*, y que estas puedan operar en el mercado principal directamente con este tipo de Autorización Simplificada.

Entonces, ¿por qué el *sandbox* regulatorio es una mejor opción? Para dar respuesta a dicha interrogante, a continuación, se compararán sendas alternativas: la implementación de un *sandbox* regulatorio y el establecimiento de una Autorización Simplificada a las *FinTech*. Dada la diversidad y variabilidad de características regulatorias de los *sandboxes* a lo largo del mundo, se tomará como referencia el modelo implementado por la FCA en el Reino Unido, debido a su éxito y mayor desarrollo, por lo cual también ha sido la base para la importación de esta herramienta a otros países.

1. Incertidumbre y barreras legales

Como punto de partida, en el Reino Unido, los participantes del *sandbox* regulatorio pueden solicitar asesoría individual en la interpretación de las normas aplicables, y también dispensas o modificaciones a la normativa de la FCA (García Ocampo, 2017, p. 22). Al optar por una Autorización Simplificada, por el contrario, cada *FinTech* deberá contratar sus propios servicios de asesoría legal, lo que claramente eleva sus costos, y esta se materializará en la opinión de otro privado (a diferencia del *sandbox* británico, en el que es el personal del mismo regulador quien ayuda a comprender la regulación desde su punto de vista institucional). Además, bajo la Autorización Simplificada, las *FinTech* tendrían que cumplir con la regulación aplicable al resto del mercado principal, en donde no hay posibilidad de solicitar dispensas y/o modificaciones de aplicación individual.

En relación con lo último, se reitera lo mencionado en los párrafos precedentes: el *sandbox* regulatorio permite mitigar la incertidumbre regulatoria; es decir, verificar el alcance de la regulación aplicable a estos productos y servicios financieros complejos y novedosos (Vodanovic Legal, 2019, p. 65). Asimismo, la regulación aplicable al mercado principal resulta en la mayoría de los casos onerosa para las *FinTech*, siendo considerada por estas una barrera de entrada al mercado (Vodanovic Legal, 2019, p. 38). Al mismo tiempo, la ausencia de una regulación especializada también incide en la incertidumbre legal que pretende reducir el *sandbox* regulatorio (Vodanovic Legal, 2019, p. 38). Por ejemplo, para una *FinTech* dedicada a las criptomonedas, la alternativa de la Autorización Simplificada no resultará adecuada, en tanto la incertidumbre persiste incluso tras ingresar al mercado principal, ya que en nuestro país no se cuenta con una regulación especializada para ofrecer este producto.

En línea con lo mencionado, la flexibilidad del *sandbox* regulatorio se complementa con una 'reportería' semanal al regulador; de modo tal que puedan detectarse falencias y, consiguientemente, efectuar ajustes de manera temprana y oportuna. Dicha 'reportería' debe incluir los avances clave alcanzados, los resultados obtenidos y la gestión de riesgo, y la falta de entrega de esto se sanciona con la cancelación de la prueba (García Ocampo, 2017, p. 24).

2. Incertidumbre de mercado

La opción de un *sandbox* regulatorio –a diferencia de la Autorización Simplificada– también permite mitigar la incertidumbre de mercado. Con ello, se hace referencia a que "en circunstancias normales es casi imposible conocer el verdadero impacto de iniciativas comerciales en el mercado antes de su lanzamiento" (Vodanovic Legal, 2019,

p. 65). En otras palabras, un inversionista no conoce cuál va a ser la recepción de su producto o servicio por parte del público, hasta que ingresa al mercado a ofrecerlo.

Efectivamente, al contar con una Autorización Simplificada, un emprendedor recién empieza a probar su producto o servicio una vez que se encuentra en el mercado principal. Es por ello que, recién en ese momento, se puede dar cuenta de la acogida de dicho producto o servicio. En el caso de que los resultados no sean los esperados y decida retirarse del mercado, dicho conocimiento llegará muy tarde, pues para entonces ya habrá efectuado grandes esfuerzos organizativos, regulatorios y económicos.

El *sandbox* regulatorio, por el contrario, permite detectar en una fase prematura la posible respuesta del mercado. Si bien las pruebas se realizarán ante un grupo limitado de consumidores, la aceptación –o falta de ella– por parte de estos permitirá a los participantes del *sandbox* dar marcha atrás sin tener que haber implementado íntegramente su modelo de negocio, lo que se traduce en menores pérdidas; así como también, al no tener todavía una licencia o autorización administrativa estable, se ahorraría los costos de obtenerla y tener que cancelarla luego por no alcanzar el éxito esperado.

3. Mitigación de riesgos

Como se ha desarrollado precedentemente, al encontrarse en una fase de pruebas, las *FinTech* que participan en un *sandbox* regulatorio experimentan sus productos y servicios ante un número limitado de usuarios y niveles reducidos de transacciones, aunque lo suficiente para obtener datos estadísticos relevantes (Comité de Supervisión Bancaria de Basilea, 2017, p. 40; García Ocampo, 2017, p. 23).

Esta limitación al número de usuarios y transacciones permite contener los riesgos inherentes a las *FinTech*; los cuales son operacionales, de lavado de activos y/o financiamiento del terrorismo, solvencia, entre otros (Vodanovic Legal, 2019, pp. 58-62). Asimismo, estos usuarios son seleccionados sobre la base de su adecuación al tipo de innovación y mercado, así como también a los riesgos. Por ejemplo, bajo el esquema de la FCA, en el caso de productos especialmente riesgosos, estos se dirigen exclusivamente a clientes sofisticados —o 'inversionistas institucionales', para utilizar el concepto propio de nuestro ordenamiento—; mientras que se contará con clientes *retail* siempre que estos no asuman los riesgos, puedan presentar sus quejas ante la empresa y el *ombudsman* financiero y tener acceso al Esquema de Compensación de Servicios Financieros de la empresa (García Ocampo, 2017, pp. 23-24).

A diferencia de lo que sucede en el caso del *sandbox* regulatorio, al tener una Autorización Simplificada, las *FinTech* podrían operar en el mercado principal, llegando a cualquier tipo y cantidad de usuarios, y realizando las transacciones permitidas bajo dicha Autorización Simplificada (probablemente, sin limitación según su cantidad o nivel de riesgo). Así, no solo podrían contratar con clientes poco experimentados o ajenos al riesgo, sino que también se multiplicaría el riesgo inherente a esta clase de actividades al tener la posibilidad de llegar a una mayor cantidad de usuarios y de ejecutar tantas transacciones como les resulte factible.

4. Protección al consumidor financiero

Los participantes del *sandbox* regulatorio tienen la obligación de informar a sus clientes que se encuentran en dicho espacio controlado de pruebas, además de los términos y condiciones de estas (García Ocampo, 2017, pp. 23-24). Ante ello, los usuarios deben prestar su consentimiento informado (García Ocampo, 2017, p. 24), por lo que están advertidos de que, en el curso de dicha experimentación, la regulación aplicable al producto o servicio contratado puede variar constantemente. En cuanto a la Autorización Simplificada, los usuarios de las *FinTech* no recibirían necesariamente información tan detallada sobre cómo operan estas empresas, y corren el riesgo de que el producto o servicio contratado fracase por las barreras legales que ya se han explicado.

Adicionalmente, en caso de que los productos y servicios de los participantes de un *sandbox* regulatorio fallen, generando pérdidas en perjuicio de los usuarios, estos serán compensados por los propios participantes, sin perjuicio de que puedan presentarse salvaguardas adicionales, atendiendo a los riesgos particulares de alguno de estos emprendimientos (García Ocampo, 2017, pp. 23-24).

Respecto al supuesto de la Autorización Simplificada, al no existir una regulación especializada, las *FinTech* estarían sometidas al régimen general del Fondo de Seguro de Depósitos de la SBS (en adelante FSD). El artículo 145 de la Ley General del Sistema Financiero establece que las empresas que ingresen al FSD deberán efectuar aportaciones a este durante 24 (veinticuatro) meses para que sus operaciones se encuentren respaldadas (Ley 26702, 1996); por lo que los usuarios de *FinTech* que operen bajo una Autorización Simplificada no gozarían de la cobertura del FSD durante los dos primeros años de operaciones de la empresa, quedando desprotegidos.

5. Aspectos adicionales

Por último, el hecho de concentrar a las *FinTech* más innovadoras y con mayor potencial en un *sandbox* regulatorio centraliza la búsqueda de información sobre estas: ya sea por parte de inversionistas interesados en apoyarlas financieramente, así como también por el lado de otras entidades encargadas de su supervisión (por ejemplo, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [Indecopi] en materia de protección al consumidor y el Ministerio de Justicia y Derechos Humanos en lo relativo a la protección de datos personales).

A diferencia de la implementación del *sandbox*, el escenario de una Autorización Simplificada resulta menos eficiente para dichos efectos. En tanto las *FinTech* se encuentran desperdigadas por el mercado principal, junto a los demás agentes (tradicionales) de este, se requerirán esfuerzos adicionales para identificarlas y distinguirlas de dichos agentes.

Dicho todo lo anterior, se puede resumir de la siguiente manera:

Cuadro 2

	***Sandbox* Regulatorio**	**Autorización Simplificada**
Incertidumbre y barreras legales	Los participantes pueden solicitar asesoría individual sobre la regulación al propio regulador.	Cada *FinTech* debe conseguir y costear su propia asesoría legal, la cual será brindada por privados.
	Se pueden solicitar dispensas o modificaciones en la regulación aplicable, lo cual se encuentra sujeto a ajustes.	Cumplir con la regulación aplicable puede resultar oneroso; así como también hay actividades que carecen de regulación especializada.
Incertidumbre de mercado	Permite probar la respuesta de la demanda a los productos y servicios ofrecidos antes de salir al mercado principal.	Las *FinTech* advierten las falencias de sus productos y servicios y la respuesta de los usuarios recién al salir al mercado principal.
Mitigación de riesgos	Los participantes prueban sus productos y servicios ante un número limitado de usuarios, lo que minimiza riesgos.	Las *FinTech* pueden operar en el mercado principal en general, sin ninguna restricción respecto al número y tipo de clientes, lo cual potencia los riesgos inherentes.
Protección a los usuarios	Deben prestar su consentimiento informado, luego de conocer los términos y condiciones en que los productos y servicios contratados se experimentan.	Prestan su consentimiento para contratar con las *FinTech*, pero el estándar de información y detalle no es tan elevado.
	En caso de que fallas en el producto probado generen pérdidas en perjuicio de los usuarios, los participantes deben compensarlos.	Al no existir una regulación especializada, las *FinTech* no estarán cubiertas por el FSD durante los primeros dos años de operaciones.
Aspectos adicionales	Genera centralización de *FinTech* con mayor potencial y nivel de innovación, lo cual es eficiente para los inversionistas y otras autoridades supervisoras.	Las *FinTech* se encuentran desperdigadas en el mercado principal, junto con los demás agentes (tradicionales).

Fuente: Elaboración propia a partir de las fuentes citadas en la presente sección IV.

En conclusión, se aprecia que el *sandbox* regulatorio constituye una herramienta adecuada para el desarrollo de las *FinTech* en nuestro país, lo cual –como se ha explicado– conllevaría una serie de ventajas a los usuarios, en contraposición a la alternativa de que el regulador implemente una Autorización Simplificada de funcionamiento para dichos negocios innovadores.

D. Consideraciones sobre una posible regulación del *sandbox* en Perú

A modo de corolario, y sin ánimos de ser exhaustivos, se procederá a brindar algunas notas respecto de una eventual regulación del *sandbox* en Perú.

Como punto de partida, y dada la naturaleza de las *FinTechs* esbozada a lo largo del presente trabajo, una regulación del *sandbox* que pretenda perdurar por un tiempo razonable en nuestro ordenamiento jurídico debe ser flexible. Así, debido a que el sector *FinTech* está caracterizado por su innovación constante y su disrupción en relación con los productos y servicios financieros existentes, se debe hacer un esfuerzo por que el marco regulatorio no sea rígido, sino que, por el contrario, se base en principios a favor de la protección del usuario y el fomento de la innovación, más que en prescripciones estrictas que limiten el desarrollo del *sandbox* y la participación de proyectos en él. Lo anterior no significa, sin embargo, que no deban existir reglas claras. Por el contrario, ello es relevante en tanto brinda seguridad jurídica y fomenta la participación en el *sandbox*.

Uno de los aspectos donde es preciso tener claridad es el relativo al de los requisitos para participar del *sandbox* o 'criterios de entrada'. Sin duda alguna, los participantes de la arenera deben cumplir con el requisito fundamental de tener proyectos

innovadores. Ello significa que el proyecto que presenten debe ser novedoso, lo cual puede implicar lo siguiente: (i) que el producto o servicio ofrecido no existe anteriormente o no se encuentra licenciado; (ii) se propone la creación de un nuevo canal o plataforma para el ofrecimiento de productos y servicios financieros; (iii) se basa en la aplicación de una tecnología o innovación financiera que no se ha probado con anterioridad en la jurisdicción; y/o (iv) cualquier otra manifestación que, a juicio del regulador, puede considerarse como innovación (Herrera y Vadillo, 2018, p. 17).

Otros requisitos que igualmente deberían considerarse en una regulación del *sandbox* son los relativos al estado del producto o servicio propuesto, el cual debería encontrarse desarrollado a tal punto que, de ser elegido el proyecto, se encuentre listo para ser probado y ofrecido a potenciales consumidores. Asimismo, es relevante analizar cuál es el beneficio que los proyectos postulantes ofrecen al consumidor financiero y al mercado en general, a través de su capacidad de producción, envío, captura o generación de valor (Herrera y Vadillo, 2018, p. 17).

Por otro lado, es importante definir los requisitos a ser exigidos a las plataformas postulantes, a fin de que acrediten tener el respaldo humano, financiero y organizacional suficiente para poder ejecutar sus proyectos correspondientes. A dichos efectos, se debe definir el tipo societario mediante el cual deben operar las plataformas postulantes y el capital social mínimo de estas. Evidentemente, dicho capital social no debe ser igual al de las entidades tradicionales del sistema financiero, pero sí debe ser suficiente para operar el negocio y cubrir cualquier contingencia. También es recomendable exigir la presentación de las hojas de vida de los principales accionistas y de los directores y gerentes de la plataforma, para así constatar la capacidad técnica y profesional de quienes operarían la plataforma.

Asimismo, la regulación del *sandbox* debe delimitar aspectos operativos adicionales como la duración del periodo de pruebas de los proyectos, el tipo y la cantidad de clientes que podrán contratar los productos y servicios ofrecidos, el estándar de revelación de información a estos usuarios y la remisión de reportes de seguimiento y demás información relevante al supervisor; además de las competencias y facultades de supervisión y sanción de dicha autoridad (Herrera y Vadillo, 2018, pp. 17-18).

Finalmente, es de especial relevancia la definición de un sistema de eventual compensación de daños. Como se ha mencionado en la sección precedente, en caso se dé alguna falla de los productos o servicios ofrecidos en el *sandbox* regulatorio, generando pérdidas en perjuicio de los usuarios, el regulador debe exigir a los propios participantes mantener una cantidad de dinero determinada en reserva, a fin de cubrir dichas reparaciones, sin perjuicio de que puedan presentarse salvaguardas adicionales, atendiendo a los riesgos particulares de alguno de estos emprendimientos (García Ocampo, 2017, pp. 23-24).

V. CONCLUSIONES

La expansión de la tecnología a diversos ámbitos de nuestras vidas es un hecho y el sistema financiero no es ajeno a ello. En ese sentido, las *FinTech* proveen una serie de ventajas a los usuarios de productos y servicios financieros –y al mercado en general– al apalancarse de las eficiencias ofrecidas por las nuevas tecnologías.

Resulta evidente, entonces, que es positivo y beneficioso para la sociedad fomentar el desarrollo de las innovaciones financieras y tecnológicas. Sin embargo, como toda actividad basada en el manejo del ahorro público, las *FinTech* conllevan riesgos, a los cuales se suma la incertidumbre respecto a cómo definir y regular las diversas innovaciones tecnológicas que vienen surgiendo.

Así las cosas, la implementación de *sandboxes* regulatorios es una herramienta que –en la medida de lo posible– permite compatibilizar las ventajas y desafíos que rodean a la industria *FinTech*, buscando un equilibrio entre la promoción y el desarrollo de las innovaciones financieras y tecnológicas de un lado y, por otro, la protección del consumidor, de sus datos personales, la prevención del lavado de activos y el financiamiento del terrorismo, y el aseguramiento de la estabilidad y la confianza en el sistema financiero en general. En efecto, contar con un espacio controlado de pruebas en el que las *FinTech* puedan operar en tiempo real les permite corroborar la viabilidad de sus productos y servicios, y también –de la mano con el regulador– ir ajustando la regulación aplicable y las dispensas o flexibilizaciones que correspondan. Todo ello, bajo la cercana supervisión de la autoridad, ante un reducido grupo de consumidores y con limitaciones al nivel de riesgo de las transacciones permitidas.

Debido a su particular adaptabilidad, la implementación de *sandboxes* regulatorios ha dado resultados fructíferos en países tan diversos entre sí como el Reino Unido, Noruega, Singapur, Hong Kong, Corea del Sur o México. En consecuencia, dichos países han experimentado un gran desarrollo de las *FinTech*, lo que se ve reflejado en la cantidad

de compañías de este tipo presentes en ellos, así como los ingresos generados por estos negocios.

En suma, la implementación de un *sandbox* regulatorio en Perú conllevaría muchas ventajas. Como se ha visto, esta herramienta fácil de adaptar en diversos contextos y ordenamientos jurídicos coadyuvaría al desarrollo de la industria *FinTech* en el país y, por ende, se intensificarían los beneficios aportados por este tipo de modelos de negocio, en beneficio de los usuarios de sus productos y servicios, pero también del sistema y mercado financiero en general.

REFERENCIAS

Abanca Innova. (2020). Mapa del ecosistema FinTech en España. https://elreferente.es/scouting/en-espana-operan-ya-mas-de-400-startups-del-sector-FinTech/

Aguilar Alonso, I., & Lluesma Rodrigo, P. (2019). Una introducción al *sandbox* regulatorio. *Actualidad Jurídica Uría Menéndez*, (52), 95-100.

Ahn, C. S., Lee, D., & Choi, S. (18 de abril de 2019). South Korea: unpacking the sandbox. *International Financial Law Review*. https://www.iflr.com/Article/3869810/South-Korea-unpacking-the-sandbox.html.

Avendaño Carbellido, O. (2019). Los retos de la banca digital en México. *Revista del Instituto de Ciencias Jurídicas de Puebla, 12*(41), 87-108.

Cairns, P., & Thomas, J. (realizadores) (28 de julio de 2010). M-PESA Mobile Money [video]. You Tube. Consultative Group to Assist the Poor (CGAP). https://www.youtube.com/watch?v=ewJ-lpvWDEU

Comité de Supervisión Bancaria de Basilea (2017). *Sound Practices: Implications of FinTech developments for Banks and bank supervisors*. https://www.bis.org/bcbs/publ/d431_es.pdf

Da Re, G. (16 de septiembre de 2015). Cinco razones por las que las empresas FinTech son una oportunidad para instituciones financieras y pymes. *Gestión*. https://gestion.pe/blog/bid/2015/09/cinco-razones-por-las-que-las-empresas-FinTech-son-una-oportunidad-para-instituciones-financieras-y-pymes.html/?ref=gesr

Department for International Trade & HM Treasury. (2019) *UK FinTech. State of the Nation*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801277/UK-FinTech-state-of-the-nation.pdf

Ernst & Young (2020). *Guía FinTech Perú 2020/2021. Panorama legal y regulatorio para la inclusión financiera*. https://www.ey.com/es_do/law/el-futuro-del-sistema-financiero-en-america-latina

Fernández, J. (2 de septiembre de 2019). Nuevos límites de tasa de interés aumentarán la competencia entre entidades financieras. *Semana Económica*. https://semanaeconomica.com/economia-finanzas/mercado-de-valores/371329-nuevos-limites-de-tasa-de-interes-aumentaran-la-competencia-entre-entidades-financieras

Financial Conduct Authority [FCA] (2020). Regulatory Sandbox. https://www.fca.org.uk/firms/innovation/regulatory-sandbox

Finnovating (2019). FinTech Peru Map. https://www.finnovating.com/news/wp-content/uploads/2020/01/FINTECH_PERU_NOV_2019_V1.4.jpg

Finnovista (2020). El número de startups FinTech creció un 26% en un año en Colombia, hasta las 200. https://www.finnovista.com/radar/el-numero-de-startups-FinTech-crecio-un-26-en-un-ano-en-colombia-hasta-las-200/

García Ocampo, M. D. (2017). *Esquemas regulatorios que facilitan la innovación en tecnología financiera: Caso de "Regulatory Sandboxes" (Análisis descriptivo internacional)* (Documento de trabajo No. 156). Comisión Nacional de Seguros y Fianzas. https://www.gob.mx/cms/uploads/attachment/file/233021/156.-Esquemas_Regulatorios_que_Facilitan_la_Innovaci_n_en_Tecnolog_a_Financiera.pdf

Garvan, M. (25 de septiembre de 2019). Nuevos límites de la tasa de interés para entidades no financieras, ¿qué implica esto? *El Comercio*. https://elcomercio.pe/economia/mercados/nuevos-limites-de-la-tasa-de-interes-para-entidades-no-financieras-que-implica-esto-noticia/?ref=ecr

Global Finance Innovation Network [GFIN] (2019). Our Members. https://www.thegfin.com/members

Global Legal Insights (2019). FinTech 2019. United Kingdom. https://www.globallegalinsights.com/practice-areas/FinTech-laws-and-regulations/united-kingdom#:~:text=In%20the%20UK%2C%20there%20is,and%20delivery%20of%20financial%20services

Harcourt, A. (2019). Regulating Financial Technology. *Risk & Regulation*, (37), 16-19.

He, D., Leckow, R., Haksar, V., Mancini-Griffoli, T., Jenkinson, N., Kashima, M., Khiaonarong, T., Rochon, C., & Tourpe, H. (2017). *FinTech and Financial Services: Initial Considerations*. https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2017/06/16/FinTech-and-Financial-Services-Initial-Considerations-44985

Herrera, D., & Vadillo, S. (2018). *Sandbox Regulatorio en América Latina y el Caribe para el ecosistema FinTech y el sistema financiero* (Documento para discusión IDB-DP-573 del Banco Interamaricano de Desarrollo). http://www.fundacionmicrofinanzasbbva.org/revistaprogreso/wp-content/uploads/2018/06/Publicaciones-MF-Sandbox-Regulatorio-en-America-Latina-y-el-Caribe-para-el-ecosistema-FinTech-y-el-sistema-financiero-vf-1.pdf

Hoder, F., Wagner, M., Sguerra, J., & Bertol, G. (2016). *La revolución FinTech. Cómo las innovaciones digitales están impulsando el financiamiento para las MIPYME en América Latina y el Caribe. https://www.oliverwyman.com/content/dam/oliver-wyman/v2/publications/2016/dec/REVOLUCION-FINTECH-SPANISH.pdf*

Lema, M. (2018). *Las FinTech en España: situación actual y perspectivas de futuro* [Trabajo de fin de máster para la obtención del Máster en Banca y Finanzas]. Universidade Da Coruña. Facultade de Economía e Empresa, Coruña, España. https://core.ac.uk/download/pdf/154757522.pdf

Mendiola, A. (4 de marzo de 2020). El fenómeno *FinTech* y sus desafíos. *Diario Oficial El Peruano*. https://elperuano.pe/noticia/90586-el-fenomeno-FinTech-y-sus-desafios

Ministerio de Asuntos Económicos y Transformación Digital (2021). *El Sandbox financiero recibe en su primera convocatoria un total de 67 proyectos.* https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2021/210224_np_%20Sandbox.pdf

Peña, I., & Rojas, F. (2017). "Sandboxes": regulación y consumidores. *Revista Empresa Global*, (176), 9-12.

Rojas, I. (25 de septiembre 2019). FinTech peruana Independencia recibe inversión de Credicorp. *Lex Latin*. https://lexlatin.com/noticias/FinTech-peruana-independencia-recibe-inversion-de-credicorp

Sandbox Challenge (2020). Sandbox Challenge. https://www.sandboxchallenge.com/

Statista (2020). Number of FinTech startups in Brazil from 2017 to 2020. https://www.statista.com/statistics/892680/brazil-number-FinTech-startups/

Superintendencia de Banca, Seguros y AFP [SBS] (2020a). *Perú: Reporte de Indicadores de Inclusión Financiera de los Sistemas Financiero, de Seguros y de Pensiones.* https://intranet2.sbs.gob.pe/estadistica/financiera/2020/Junio/CIIF-0001-jn2020.PDF

(2020b). *Sistema Financiero Peruano. Noviembre 2020.* https://intranet2.sbs.gob.pe/estadistica/financiera/2020/Noviembre/SF-0003-no2020.PDF

Superintendencia Financiera de Colombia [SFC] (2020). *Acerca de innovaSFC*. https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/10097165/dPrint/1/c/0

Truby, J. (2018). FinTech and the city: Sandbox 2.0 policy and regulatory reform proposals. *International Review of Law, Computers & Technology*, (32), 1-33.

Tsang, C. (2019). From industry sandbox to supervisory control box: Rethinking the role of regulators in the era of FinTech. *Journal of Law, Technology & Policy, 2019*(2), 355-404.

Vásquez Rodríguez, C. P. (2018). *FinTech* e *Insurtech* en América Latina. Desafíos en la protección del consumidor, la regulación y la supervisión. En G.M. Acosta Álvarez de Hoyle (ed.), *Temas de protección al consumidor y regulación financiera* (pp. 236-258). Círculo de Derecho Administrativo.

Vodanovic Legal (2019). *El panorama de la industria FinTech en el Perú. Hacia un nuevo ecosistema colaborativo*. https://www.siicex.gob.pe/siicex/documentosportal/alertas/documento/doc/79431536radE2E60.pdf

Zunzunegui, F. (2015). *Régimen jurídico de las plataformas de financiación participativa (crowdfunding)* (Revista de Derecho del Mercado Financiero Working Paper 3/2015). http://www.rdmf.es/wp-content/uploads/2015/07/zunzunegui-wp-3_2015-regimen-juridico-de-las-plataformas-de-financiacion-participativa.pdf

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Circular 0018-2019-BCRP, Diario Oficial *El Peruano*, 19 de agosto de 2019 (Perú).

Código Civil [C.C.], Diario Oficial *El Peruano*, 25 de julio de 1984 (Perú).

Constitución Política del Perú [Const.] (1993) (Perú).

Decreto de Urgencia 13-2020, Decreto de urgencia que promueve el financiamiento de la MIPYME, emprendimientos y *startups*, Diario Oficial *El Peruano*, 23 de enero de 2020 (Perú).

Decreto 661, Decreto por el cual se modifica el Decreto 2555 de 2010 en lo relacionado con la actividad de asesoría y se dictan otras disposiciones, 17 de abril de 2018, Diario Oficial [D.O.] (Colom.).

Directiva 2015/2366, del Parlamento Europeo y del Consejo del 25 de noviembre de 2015 relativa a servicios de pago en el mercado interior y por la que se modifican las Directivas 2002/65/CE, 2009/110/CE y 2013/36/UE y el Reglamento (UE) Nº 1093/2010 y se deroga la Directiva 2007/64/CE, 2015 O.J. (L 337) 25.

Instruçao CVM 588, que regula las plataformas de inversión participativa, de 13 de julho de 2017, Diário Oficial da União [D.O.U.] de 14.07.2017 (Bras.).

L. 1735, Ley por la cual se dictan medidas tendientes a promover el acceso a los servicios financieros transaccionales y se dictan otras disposiciones, 21 de octubre de 2014, Diario Oficial [D.O.], (Colom.).

Ley para Regular las Instituciones de Tecnología Financiera, Diario Oficial de la Federación [D.O.F.] 09-03-2018 (Méx).

Ley 26702, Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca, Seguros y AFP, Diario Oficial *El Peruano*, 9 de diciembre de 1996 (Perú).

Ley de fomento de la financiación empresarial (B.O.E. 2015, 5) (Esp.).

Ley para la transformación digital del sistema financiero (B.O.E. 2020, 7) (Esp.).

Real Decreto-Ley 19/2018, Ley de servicios de pago y otras medidas urgentes en materia financiera, (B.O.E. 2018, 19) (Esp.).

Resolução 4.656 del Banco Central do Brasil, de 26 de abril de 2018, Diário Oficial da União [D.O.U.] 30.04.2018 (Bras.).

Resolución de Superintendente 45-2021-SMV/02, Resolución que aprobó el Reglamento de la Actividad de Financiamiento Participativo Financiero y sus Sociedades Administradoras, Diario Oficial *El Peruano,* 20 de mayo de 2021 (Perú).

Philippi
Prietocarrizosa
&Uría

El estudio Iberoamericano

Av. Santa Cruz 888, Miraflores, Lima, Perú
Teléfono: +511 5137200
ppulegal.com

10.18800/themis.202101.013

¿PODEMOS REGULAR A LAS *FINTECH*? DESAFÍOS Y PROPUESTAS

CAN WE REGULATE FINTECH? CHALLENGES AND APPROACHES

José Villafuerte Mendoza*
Universidad de Chicago

Faced with the undoubted proliferation of FinTech companies in Peru and in the world, this article describes the current situation of the market in this field in order to explore the legal implications of this new type of company.

In that order, it first analyze how the digital market has evolved in financial and insurance matters. In the same way, it warns of the specific risks of the growing FinTech industry. All of that, to be able to point out the challenges that governments face in order to regulate this matter. In addition, it exhibits various proposals from sectors of the academia for the regulation of the FinTech market. With all this, the author concludes by giving his opinion on the mentioned proposals and presents his own for the regulation of FinTech companies, developing three main stages of implementation.

Keywords: FinTech; regulation; SBS; RegTech; extraterritoriality; enforceability of laws.

Ante la indudable proliferación de las empresas FinTech *en el Perú y en el mundo, el presente artículo expone la situación actual del mercado de tal rubro para, a partir de ello, explorar las implicaciones legales que suponen este nuevo tipo de compañías.*

Con tal fin, el autor analiza cómo ha ido evolucionando el mercado digital en materia financiera y de seguros. De la misma manera, advierte los riesgos específicos de la creciente industria FinTech *para poder señalar los desafíos que los gobiernos tienen por delante para regular esta materia. Asimismo, el artículo exhibe variadas propuestas de sectores de la doctrina para la regulación del mercado* FinTech*. Con todo esto, el autor concluye dando su opinión sobre las propuestas antes mencionadas y presenta una propia para regulación de las compañías* FinTech *desarrollando tres etapas principales de implementación.*

Palabras clave: FinTech*; regulación; SBS;* RegTech*; extraterritorialidad; exigibilidad de las normas.*

* Abogado. Candidato a Master of Law (LL.M.) por la Universidad de Chicago (Chicago, Estados Unidos de América). Exasociado de Miranda & Amado (Lima, Perú). Contacto: jvillafuertem@uchicago.edu

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 5 de enero de 2021, y aceptado por el mismo el 1 de abril de 2021.

I. INTRODUCCIÓN

Como ha señalado el Banco de Desarrollo de América Latina (2016), la industria bancaria siempre ha utilizado las innovaciones tecnológicas para mejorar sus servicios y proveerlos de una forma más eficiente. Desde esa perspectiva, el actual uso del internet y de la industria digital para el desarrollo del sector financiero –concepto amplio bajo el cual podemos agrupar a todas las compañías *FinTech*– no sería una novedad, sino únicamente por las "características competitivas y propuesta de valor, superiores a la de los bancos tradicionales" tales como "una interfaz simple, amigable y conveniente, accesible a cualquier hora y lugar" (Banco de Desarrollo de América Latina, 2016, p. 7).

Sin embargo, la reciente evolución tecnológica en el mercado financiero tiene dos características fundamentales que revolucionan completamente el sector y que tienen el potencial de transformar nuestras concepciones sobre el mismo. Me refiero, a la ausencia de una presencia física del proveedor y a la ubicuidad de los servicios financieros.

Estas características han comenzado a poner en duda la efectividad de las regulaciones del mercado financiero, que históricamente estuvieron enmarcadas a una aplicación dentro de un territorio determinado por el espacio geográfico (aplicación territorial). En esa medida, la ausencia de un local físico, e incluso las limitaciones para crear fronteras infranqueables dentro del internet, son características disruptivas también en el terreno legal. Las nuevas tecnologías han comenzado a llevar al límite las interpretaciones legales y a poner en peligro la eficacia de los esfuerzos de los organismos reguladores.

Como veremos en el presente artículo, esta forma de proveer servicios financieros está cambiando el paradigma de la regulación en el mundo y revolucionando el concepto de supervisión del mercado financiero.

En ese contexto, el propósito del presente artículo es presentar un marco general sobre la situación actual del mercado *FinTech*, los problemas que tienen que enfrentar –y que vienen enfrentando– los reguladores, algunas alternativas a la regulación que ya han sido planteadas por algunos investigadores, y la opinión del autor sobre estas alternativas y la posibilidad de su aplicación.

II. ¿CÓMO ESTÁ EVOLUCIONANDO EL MERCADO DIGITAL EN MATERIA FINANCIERA Y DE SEGUROS?

La publicación Global FinTech Index 2020, elaborada por Findexable, analiza miles de ubicaciones geográficas otorgando una calificación basada en los datos recopilados de empresas *FinTech*, métricas sobre la infraestructura empresarial local, la calidad del ecosistema *FinTech,* el número de aceleradoras, incubadoras y asociaciones, y la existencia regulaciones amigables con el sector. Por esta razón, este índice resulta bastante útil a la hora de conocer el potencial de los mercados que son parte del estudio.

A nivel internacional, los países con mejores calificaciones son los Estados Unidos, el Reino Unido, Singapur, Lituania, Suiza y los Países Bajos. Los países sudamericanos en una mejor posición en el ranking global son Brasil (19), Chile (35) y Argentina (38), mientras que Perú se encuentra en el puesto 55 de 65 países analizados (Findexable, 2019).

La publicación resalta que los tipos de *FinTech* con mayor fortaleza en el Perú son aquellos dedicados a pagos, financiamiento alternativo, cambio de moneda y operaciones de *factoring* (Findexable, 2019, p. 55).

Este ranking nos pone en contexto sobre los grandes esfuerzos que debemos hacer para desarrollar el mercado *FinTech* en el Perú, el largo camino que nos queda por delante y los ejes temáticos que debemos abordar para crear un ecosistema amigable con el sector, incluyendo regulaciones que permitan su crecimiento.

Asimismo, el Global FinTech Adoption Index 2019, elaborado por la consultora Ernst & Young (EY) y trabajado sobre la base de entrevistas a más de 27 000 consumidores en 27 mercados (incluyendo Perú), contiene información bastante útil para entender la evolución del mercado financiero y de seguros en medios digitales. Gracias a esta fuente, sabemos que tres de cada cuatro consumidores en el mundo utilizan servicios electrónicos de transferencia de dinero y pagos, que uno de cada dos consumidores utiliza algún servicio de seguros, que el 33% de los consumidores buscan fuentes de financiamiento en plataformas distintas a los bancos tradicionales y que el 93% de pequeñas y medianas empresas prefieren encontrar soluciones tecnológicas donde sea posible (Ernst & Young, 2019).

Sin embargo, el dato más importante que nos proporciona este reporte es, en efecto, el **índice de adopción**. Se trata de un porcentaje que mide la utilización de estas tecnologías respecto de la población digitalmente activa. Como se puede ver en el cuadro siguiente, el Perú cuenta con un índice de adopción de 75%, por encima incluso de los Países Bajos, Estados Unidos, México o el Reino Unido. Esto nos permite concluir que el potencial de nuestro país para el desarrollo de esta industria

es más grande del que podríamos imaginar y por eso resulta tan urgente crear un ecosistema que permita su crecimiento.

Cuadro 1

País	Índice de Adopción
China	87%
India	87%
Rusia	82%
Sudáfrica	82%
Colombia	76%
Perú	75%
Países Bajos	73%
México	72%
Irlanda	71%
Reino Unido	71%
Argentina	67%
Hong Kong	67%
Singapur	67%
Chile	66%
Brasil	64%
Alemania	64%
Canadá	50%
Estados Unidos	46%
Francia	35%
Japón	34%

Fuente: Elaboración propia a partir del Global FinTech Adoption Index 2019 (Ernst & Young, 2019).

Asimismo, comparando el nivel de adopción por cada tipo de servicio *FinTech*, los seguros han subido del cuarto al segundo puesto (desde 2015 a 2019), mientras que los servicios de transferencia de dinero y pagos se han mantenido consistentemente en el primer lugar (ver Cuadro 2).

A nivel global, el índice de adopción de los servicios *FinTech* ha crecido sostenidamente desde un 16% en el 2015 hasta un 64% en el 2019 (Ernst & Young, 2019). Esta es, sin lugar a duda, una tecnología disruptiva y es el presente y futuro del mercado financiero y de seguros.

En cuanto a las inversiones en este sector, la Asociación para las Inversiones de Capital Privado en Latinoamérica (en adelante, LAVCA, por sus siglas en inglés) ha emitido el Annual Review of Tech Investment in Latin America, documento en el que se señala que las inversiones en Latinoamérica en compañías de tecnología se han incrementado en más del 100% cada año durante el periodo comprendido entre 2016 y 2019. El monto de las inversiones en la región ha llegado hasta los USD 4,603 millones en unas 440 transacciones de inversión (Latin American Private Equity & Venture Capital Association [LAVCA], 2020).

De la inversión total en tecnología en la región durante el 2019, el 31% representa a la industria *FinTech*, destacándose operaciones principalmente en Brasil, México y Argentina (LAVCA, 2020, p. 5).

En Perú, de acuerdo al siguiente cuadro, se han efectuado el 1.4% de todas las transacciones de inversión en tecnología en el año 2019, generando una inversión de USD 3 millones en seis transacciones. Lo que representa una reducción en comparación con el año 2019 en el que se invirtieron USD 16 millones. Cabe señalar que Perú es el único de los mercados principales de la región en el que se habían reducido las inversiones en compañías tecnológicas, tal como se aprecia en el cuadro 3.

A pesar de esta reducción en el monto global de inversiones en empresas de tecnología, el Centro de Emprendimiento e Innovación de la Universidad del Pacífico (Emprende UP) ha señalado que el número de compañías que ofrecen servicios *FinTech* en el Perú creció de 130 durante el año 2019 a 151 durante el 2020, representando un incremento del 16% (Andina/Difusión, 2020).

Este crecimiento es significativo teniendo en cuenta la ralentización de la economía durante el año 2020 originada, entre otros factores, por la crisis sanitaria ocasionada por la pandemia del COVID-19. Asimismo, dicho crecimiento traduce, en gran medida, el futuro de esta industria que a pesar de las dificultades logra abrirse paso, quizás motivada por superar dichas dificultades y cambiar

Cuadro 2

Categorías	2015	2017	2019	Ranking
Transferencia de dinero y pagos	18%	50%	75%	1
Seguros	8%	24%	48%	2
Depósitos e inversiones	17%	20%	34%	3
Presupuesto y planificación financiera	8%	10%	29%	4
Préstamos	6%	10%	27%	5

Fuente: Elaboración propia a partir del Global FinTech Adoption Index 2019 (Ernst & Young, 2019)

Cuadro 3

País	2018	2019
México	US$175 millones	US$649 millones
Colombia	US$334 millones	US$1,090 millones
Brasil	US$1,300 millones	US$2,490 millones
Chile	US$46 millones	US$63 millones
Perú	US$16 millones	US$3 millones
Argentina	US$84 millones	US$290 millones

Fuente: Elaboración propia a partir del Annual Review of Tech Investment in Latin America de LAVCA (2020)

el mercado tradicional que puede perder eficiencia bajo el nuevo contexto global.

En ese contexto, la Asociación FinTech Perú realizó un sondeo de opinión entre los fundadores de empresas *FinTech* para tener mayor claridad sobre el ecosistema en el Perú, especialmente en tiempos de crisis sanitaria y económica. Del sondeo podemos extraer algunos datos que nos dan una mejor perspectiva sobre el potencial de crecimiento del sector en nuestro país.

El primer dato relevante que encontramos es el referido al tipo de actividades desarrolladas por estas compañías dentro del Perú:

Cuadro 4

Tipo de servicio	Porcentaje de compañías dedicadas a la actividad
Financiamiento a PYMES	90%
Operaciones con monedas	80%
Financiamiento de personas	60%
Pagos	40%
Factoring	30%
Administración de activos	20%
Administración	10%
Infraestructura	10%

Fuente: Elaboración propia a partir del Reporte FinTech Perú durante Pandemia 2020 (Asociación FinTech Perú, 2021)

Se puede apreciar que en el mercado peruano hay una prevalencia de compañías dedicadas al financiamiento. Este fenómeno podría entenderse como una consecuencia de un mercado financiero tradicional con pocas alternativas de productos y de ofertantes.

Por otro lado, como se puede apreciar en el siguiente cuadro, la gran mayoría de proveedores *FinTech* peruanos se encuentran concentrados en Lima (ver Gráfico 1).

Esta distribución geográfica se puede entender también como una consecuencia de factores transversales a toda la economía del país como son una mayor presencia en Lima de recursos tecnológicos

Gráfico 1

Fuente: Elaboración propia a partir del Reporte FinTech Perú durante Pandemia 2020 (Asociación FinTech Perú, 2021)

y humanos especializados para el desarrollo de la industria, el acceso a internet deficiente en provincias y la ausencia de oportunidades educativas vinculadas al sector. En todo caso, tal como sucede en otro tipo de industrias, estamos ante un desarrollo desigual, cuya solución va más allá de los esfuerzos del sector privado y requiere de un análisis más profundo sobre las razones que generan esta desigualdad, análisis que debería generar la implementación de políticas públicas desde el Estado.

Finalmente, otro aspecto relevante que me gustaría resaltar del sondeo efectuado por la Asociación FinTech Perú es la expectativa que tiene el mercado sobre el desarrollo del sector *FinTech* (ver Gráfico 2).

Esta estadística nos demuestra un optimismo dentro del propio sector sobre su crecimiento, a pesar de los efectos de la pandemia en la economía. Ello podría deberse a varios factores, entre los que podríamos destacar el gran espacio de crecimiento en un país con un bajo índice de bancarización, al incremento de la demanda interna por capital de trabajo (en un escenario de ausencia de liquidez) y al incremento en la demanda de servicios no presenciales.

Gráfico 2

Fuente: Elaboración propia a partir del Reporte FinTech Perú durante Pandemia 2020 (Asociación FinTech Perú, 2021)

Como vemos, hay espacio para el crecimiento del sector *FinTech* en el Perú, los agentes de este mercado reconocen las oportunidades que se presentan y el desarrollo de la industria depende no solamente del sector privado, sino también del desarrollo de políticas públicas (fundamentalmente en infraestructura y en educación) que generen un ecosistema favorable para el desarrollo tecnológico.

III. ¿CUÁLES SON LOS RIESGOS ESPECÍFICOS DE LA INDUSTRIA *FINTECH*?

Un grupo de investigadores del Fondo Monetario Internacional (en adelante, FMI) destaca, como principales ventajas de la industria *FinTech*: la reducción de costos de transacción, el incremento de la competencia en el mercado financiero, la mejora de los servicios de intermediación y el fortalecimiento de la inclusión financiera (Berkmen *et al.*, 2019).

Sin embargo, como han apuntado diversas fuentes de consulta[1], existen riesgos asociados a esta tecnología producidos por las limitaciones en la supervisión y control de estas empresas, y vinculados también a la naturaleza propia del mercado *FinTech*. A continuación, se explorará brevemente cada uno.

A. Estabilidad financiera

Se pueden identificar tres características del mercado *FinTech* que podrían poner en riesgo la estabilidad financiera de un país.

La primera característica está referida al tamaño de las compañías, que en su mayoría no cuentan con los recursos y la capacidad suficientes para manejar y mitigar sus riesgos. Recordemos que décadas de análisis, intentos de regulación, crisis y resiliencia en el mercado financiero han moldeado las características de la regulación financiera en el mundo. En ese sentido, como consecuencia del desarrollo histórico del mercado financiero, la regulación que tenemos hoy es intrincada y costosa. Por lo tanto, la gran mayoría de empresas que brindan servicios *FinTech* no tienen la posibilidad operativa y económica de cumplir con el estándar regulatorio que se le exige a la banca tradicional, así pues, este estándar se ha convertido en un costo de entrada infranqueable para una empresa emergente (*startup*).

La segunda característica es la concentración. Como apunta Lehmann (2019), una de las peculiaridades de este sector es el alto nivel de concentración en sus operaciones. Esto es, que sus servicios pueden ser provistos desde un solo punto en el planeta sin necesidad de operar físicamente en otras locaciones (Lehmann pone de ejemplo a PayPal que opera en 200 países desde un solo punto en San Jose, California). Esta alta concentración debilita la capacidad de continuidad de las operaciones ante un evento de interrupción; por ejemplo, un desastre natural o una crisis sanitaria.

Finalmente, una tercera característica potencialmente problemática es la existencia de un solo canal de operaciones. A diferencia de la banca tradicional, que hoy en día opera tanto en el mercado digital como en oficinas físicas, la industria *FinTech* solo opera electrónicamente a través de sistemas operativos complejos totalmente computarizados. Esto convierte a las compañías *FinTech* en un blanco vulnerable a ataques o fraude cibernético, pues la totalidad de la información, procesos y recursos se encuentran digitalizados.

Sumadas estas tres características, se puede apreciar una debilidad estructural en la fortaleza patrimonial y capacidad operativa para afrontar eventos que afecten sus operaciones (a nivel económico o de procesos). La afectación de este sector en una situación de estrés generalizado podría causar, a su vez, un grave daño para otros sectores que dependan de la continuidad de las operaciones de las compañías *FinTech*, por ejemplo, si se trata de una pasarela de pagos o una compañía que recauda depósitos del público.

[1] Véase Lehman (2019) y Berkmen *et al*. (2019).

Por otro lado, las compañías *FinTech* que si presentan un tamaño considerable de operaciones y/o activos también constituyen un riesgo para la estabilidad financiera de los países. Este riesgo es similar a las externalidades ocasionadas por empresas bancarias tradicionales que cuentan con operaciones transfronterizas y cuya materialización se vio reflejada en la crisis financiera del 2008. Al respecto, es preciso recordar lo mencionado por Cecchetti, Domanski y von Peter quienes concluyeron en su momento que

> […] la crisis financiera tuvo un carácter claramente internacional, con pérdidas transfronterizas asociadas con activos de países extranjeros, brechas de financiamiento transfronterizas asociadas con pasivos en moneda extranjera y contagio transfronterizo derivado de la importancia sistémica de ciertas instituciones. Estos fenómenos apuntan a una capitalización inadecuada, liquidez insuficiente, regímenes de resolución insatisfactorios y una incapacidad para abordar las externalidades creadas por los grandes bancos globales (2011, p. R38).

Queda claro que estos riesgos se presentan tanto para entidades financieras tradicionales como aquellas que operan a través de medios digitales.

B. Integridad financiera

También nos enfrentamos a una potencial afectación a la integridad de los sistemas financieros. Los investigadores del FMI antes citados reconocen que, aunque las nuevas tecnologías puedan ayudar al cumplimiento de la regulación sobre prevención de lavado de activos y financiamiento del terrorismo, muchos de estos avances pueden ser utilizados para actividades criminales (Berkmen *et al.*, 2019). Este es el caso, por ejemplo, del uso de criptomonedas para operaciones de lavado de activos, aprovechando que una de las cualidades de esta tecnología es la anonimidad de las partes que participan en una transacción.

C. Ciberseguridad

Como señalamos anteriormente, sin perjuicio de que la vulnerabilidad de la tecnología *FinTech* a ciberataques es una característica que contribuye con generar riesgos específicos para la estabilidad financiera, esta problemática representa un riesgo en sí misma para los consumidores a nivel individual.

A pesar de que se ha desarrollado tecnología para prevenir los fraudes y luchar contra los ataques cibernéticos (tecnología biométrica, reconocimiento facial y *blockchain*), no todas las compañías han implementado estos avances en sus servicios.

D. Protección del consumidor (asimetría informativa)

Debido a la distancia entre el proveedor del servicio y el consumidor, la asimetría informativa se hace aún más evidente en la industria *FinTech*. Los riesgos que afrontan los consumidores, sobre todo en servicios transfronterizos, son difícilmente superables por una autoridad nacional de protección al consumidor.

Además, la asimetría informativa se presenta de forma particular en esta industria. Lenz pone como ejemplo a un proyecto de *crowdfunding* cuyo promotor tiene toda la información, mientras que el inversionista solo tiene posibilidades limitadas de verificar la veracidad y relevancia de la información ingresada en la plataforma (2015, p. 1). En ese caso, los inversionistas deben asumir un elevado riesgo y deberán confiar en la información proporcionada sin posibilidades de efectuar un análisis más profundo o un proceso de debida diligencia.

E. Protección de datos personales

Existe una preocupación generalizada en el mundo –que es transversal a toda la industria digital– sobre el correcto uso de los datos personales y el destino de estos. Los servicios *FinTech* no son la excepción.

Con una cantidad sin precedentes de compañías que ofrecen estos servicios, desde países tan diversos como lejanos, los consumidores y las agencias regulatorias no tienen claridad sobre el destino de los datos personales que compartimos, el uso que se les da y la posible transferencia de estos datos a compañías especializadas en manejar cantidades considerables de información *(big data)* y ofrecer, además, servicios utilizando esta información sin autorización expresa del titular de los datos (por ejemplo, marketing corporativo o político).

Tal como explican Arner, Barberis y Buckley (2016), el mercado *FinTech* se está moviendo de la digitalización de la moneda hacia la 'monetización' de la información. Los datos personales de los usuarios de estas plataformas se están convirtiendo en un activo bastante requerido en el mercado. La problemática que enfrentan los reguladores es buscar mecanismos adecuados para proteger al titular de los datos personales de usos no autorizados de dicha información.

F. Protección ante riesgos de insolvencia

Los bancos y las empresas de seguro tradicionales están sujetos a regulaciones específicas sobre si-

tuaciones de insolvencia patrimonial. En el Perú, por ejemplo, existe un régimen especial de vigilancia, intervención, disolución y liquidación de las empresas del sistema financiero y del sistema de seguros. Bajo este régimen especial, todas las etapas de un proceso de disolución y liquidación de una entidad regulada están sujetos al estricto control de la Superintendencia de Banca, Seguros y AFP (en adelante, SBS).

El objetivo de estos regímenes especiales es que cualquier situación que ocasione un riesgo de insolvencia para la empresa sea adecuadamente manejado y supervisado por el regulador correspondiente, con el fin de proteger los intereses de los ahorristas y la estabilidad financiera.

Sin embargo, considerando que las empresas *FinTech* realizan operaciones, en muchos casos, fuera del ámbito regular de supervisión de los organismos reguladores, el riesgo de insolvencia es manejado por cada compañía y asumido directamente por los consumidores.

IV. ¿CUÁLES SON LOS DESAFÍOS QUE TIENEN QUE ENFRENTAR LOS REGULADORES?

Así como existe una problemática particular de la industria *FinTech*, que hemos desarrollado en la sección III anterior, los organismos reguladores también enfrentan desafíos específicos generados por la evolución digital de la industria financiera y de seguros. En ese sentido, a continuación se detallan aquellos desafíos que parecen ser más relevantes.

A. Extraterritorialidad y exigibilidad de las normas

Como señala Dy (2016), la interconectividad entre los mercados actuales requiere de una aplicación extraterritorial de la ley. Nos referimos a situaciones cada vez más comunes en las que los servicios financieros son provistos por compañías sin ningún tipo de presencia en el territorio peruano, esto es, sin oficinas ni servidores ubicados en el territorio nacional.

Como podría esperarse, la reacción natural de un organismo regulador o de un legislador sería proponer que las normas que regulan el mercado financiero y de seguros evolucionen hacia una aplicación extraterritorial; es decir, a regular transacciones con efectos en el Perú, sin que sea relevante dónde han ocurrido las mismas o dónde se encuentra ubicado el proveedor del servicio.

Sin embargo, este primer impulso de regulación encuentra una limitación en la realidad. Si tenemos una norma que regula operaciones de una compañía ubicada en la India o Singapur –porque nos interesa supervisar sus operaciones efectuadas con residentes en el Perú– es probable que esta compañía no vaya a cumplir la costosa regulación peruana por un análisis de eficiencia económica. La compañía podrá seguir realizando operaciones porque no tiene ningún tipo de presencia física en el Perú y el regulador peruano no tiene la posibilidad de hacer cumplir las sanciones que imponga a una entidad que se encuentra en otra jurisdicción. En consecuencia, el problema de la territorialidad de la norma se convierte en un problema de exigibilidad.

Un ejemplo concreto lo podemos ver en la evolución del artículo 2 de la Ley 30050, la Ley de Promoción del Mercado de Valores (2013), que regula la publicidad de activos y servicios financieros no supervisados. En virtud de esta norma, toda publicidad o aviso sobre activos financieros que se encuentre bajo competencia de la Superintendencia del Mercado de Valores (en adelante, SMV) o de la SBS, respectivamente, solo puede realizarse por sujetos autorizados o supervisados por la SMV o por la SBS, respectivamente. En ese sentido, mediante Decreto de Urgencia 013-2020, emitido recientemente, se ha modificado este artículo para precisar que se encuentra dentro de esta limitación todo aviso y publicidad que se realice a través de servidores de Internet ubicados en el territorio extranjero (2020).

Como podemos apreciar, esta norma refleja un avance hacia una aplicación extraterritorial de la norma peruana; sin embargo, no soluciona el problema de su exigibilidad. Quizás esa sea la razón por la que el único efecto práctico que haya tenido esta regulación sea la emisión de diversos avisos y alertas publicados por la SMV en su portal web referidos a operaciones de *crowdfunding*, Forex o la adquisición de monedas virtuales y criptomonedas, publicitadas por entidades no supervisadas que se encuentran ubicadas en el exterior.

Por otro lado, algunos legisladores, actuando de una forma más agresiva, podrían plantear medidas más estrictas de control; por ejemplo, bloqueando servidores o páginas web vinculadas a servicios financieros o de seguros que no cumplan con la regulación peruana (en el caso de que esta evolucione completamente a una aplicación extraterritorial). Sin embargo, estas medidas colisionan con la narrativa de libertades individuales de los países que, en su mayoría, evitan limitar el acceso de sus ciudadanos a los contenidos de internet.

En efecto, como han señalado organizaciones afines al libre uso del internet[2], la aplicación extraterritorial de una norma que restrinja operaciones realizadas a través de internet, seguida de controles estrictos sobre el acceso a internet, podría acarrear efectos negativos para los ciudadanos y los Estados; entre ellos: (i) la falta de predictibilidad en la aplicación de las normas; (ii) la fragmentación del internet, creando un trato desigual entre los individuos respecto al acceso a las fuentes y servicios provistos a través de este; (iii) una serie de inconsistencias en la aplicación de la regulación entre entidades cuyo tamaño les permitiría cumplir con las normas y las *startup,* creando un nuevo tipo de desigualdad digital; (iv) los siempre usuales intentos de los estados por tomar o reafirmar el poder en el escenario internacional intensificando conflictos jurisdiccionales; y (v) la aparición de acciones no coordinadas entre los Estados para regular una situación en concreto (por ejemplo, las *FinTech*) en desmedro de las formas colaborativas de examinar los mercados para tomar mejores decisiones.

B. Dificultades para el control

Los organismos reguladores en el mundo enfrentan otro problema también importante. La velocidad con la que evoluciona la tecnología.

Mientras los servicios financieros continúan evolucionando, parece que la capacidad de los organismos reguladores para seguirles el paso es cada vez menos confiable. Esto se debe a la gran cantidad de información que manejan las compañías tecnológicas, el número creciente de operaciones que realizan y los medios no tradicionales para celebrarlas.

Existe una tendencia a nivel global, promovida originalmente por las instituciones financieras, orientada a la aplicación de tecnología en la regulación y en el cumplimiento de las normas que regulan el mercado financiero, denominada *RegTech*[3]. Sin embargo, estas tecnologías están lejos de ser aplicadas por todos los organismos reguladores en el mundo y de ser útiles para todos los aspectos que requieren control o vigilancia de una entidad gubernamental especializada.

C. Productos de distinta naturaleza

Asimismo, existe otra característica del mercado *FinTech* que se constituye como un problema para los esfuerzos de los organismos reguladores. Nos referimos a la diversidad de productos y servicios que ofrecen estas compañías y que, en circunstancias normales, corresponderían ser supervisados por dos o más organismos reguladores.

Como ejemplo concreto tenemos a las plataformas de negociación de valores (*trading*) que no solamente ofrecen un servicio de intermediación en el mercado de valores sujeto a la supervisión de la SMV, sino también productos financieros que deberían ser regulados –por un criterio de especialidad– por la SBS, tales como la emisión de dinero electrónico o la captación de recursos del público para colocarlos en forma de créditos (intermediación financiera).

Esta diversificación de productos y servicios se convierte en un problema cuando dos reguladores locales deben colaborar para analizar y supervisar el servicio. El problema se debe a que, usualmente, cada regulador tiene autonomía funcional y operativa, y maneja su propia dinámica interna, con reglas y estándares propios, y cada uno de ellos está en un nivel distinto de evolución tecnológica.

Es cierto que, eventualmente, la cooperación de los organismos reguladores puede dar frutos. Sin embargo, notemos que esa cooperación puede no ser oportuna ni eficiente por las demoras producidas por trabas burocráticas, o la creación de un marco regulatorio excesivamente costoso, o ineficiencias operativas como la no implementación de una 'ventanilla única' para la empresa sujeta a control.

V. ¿CUÁLES SON LAS PROPUESTAS PARA REGULAR EL MERCADO *FINTECH*?

Como adelantamos, muchos investigadores y especialistas han propuesto algunas alternativas para enfrentar los desafíos a nivel regulatorio que genera la industria *FinTech*. A continuación, explicamos las principales.

A. Cero regulaciones

Existe una tendencia –con orientación principalmente política e ideológica– que sostiene la necesidad de aplicar una estructura de libre mercado a la tecnología *FinTech*. Los defensores de esta coinciden en los beneficios para los consumidores de estos servicios, sobre todo en países en desarrollo con bajos niveles de bancarización o posibilidades limitadas de acceso al crédito.

Como explica Lehmann (2019), los promotores de esta estructura 'libertaria' consideran que la propia tecnología ha ideado maneras de reducir o incluso

[2] Véase Internet Society (2018).

[3] Véase Arner *et al*. (2016).

eliminar la asimetría informativa entre los proveedores de los servicios y los consumidores. Como los consumidores saben que estarán desprotegidos, estos recurrirán a fuentes que les permitan conocer la reputación de los servicios que están contratando. Estos son los servicios de calificación (*rating*) que ofrecen las redes sociales o incluso plataformas especializadas (Lehmann, 2019, p. 9).

El internet también permitiría solucionar otros problemas, como la capacidad que tendrán los inversionistas de un proyecto de *crowdfunding* de monitorear el proceso de forma remota, la posibilidad de organizar a los consumidores en plataformas determinadas para defender sus derechos o iniciar acciones colectivas en contra de los proveedores de los servicios.

No obstante lo anterior, esta propuesta parece ser sustentada en la ideología, pero no en la evidencia. Como señala Lehmann, muchos consumidores no buscarán información relevante sobre el servicio, sino que considerarán intuitivamente que están –en alguna medida– bajo el ámbito de protección del Estado (2019, pp. 9-10). Asimismo, los servicios de calificación no son siempre confiables, dado que no todos los consumidores finales califican los servicios, no todos los que califican son consumidores finales, algunos proveedores con comportamientos éticos cuestionables pueden modificar los resultados y las calificaciones otorgadas pueden estar plagadas de sesgos cognitivos de los consumidores (Lehmann, 2019, p. 10).

Finalmente, una estructura de libre mercado podría ser potencialmente peligrosa en cuanto al riesgo que generaría para la integridad del mercado financiero. Los servicios *FinTech* no necesariamente se encuentran incentivados a limitar la participación de la criminalidad organizada como usuarios o consumidores.

En suma, dejar el mercado *FinTech* al libre ejercicio de la oferta y la demanda –sin que medie una mínima intervención de una agencia gubernamental– no parece una respuesta adecuada ni proporcional a los potenciales riesgos que enfrentamos. Sin embargo, considero importante el llamado de atención que hacen los defensores de esta propuesta respecto a que la regulación no debería afectar el crecimiento del mercado *FinTech*, pues los beneficiarios serán –en última instancia– los consumidores, quienes podrán gozar de servicios más baratos y eficientes en un ambiente de libre competencia.

B. Autorregulación

También bajo la perspectiva de quienes piden 'menos regulación y más reputación', encontramos la propuesta de autorregulación del mercado *FinTech*.

Los defensores de esta alternativa sostienen que la autorregulación, es decir, la creación de códigos de conducta, mejores prácticas, principios generales, asociaciones de compañías del rubro y tribunales de ética, es una manera eficaz de conseguir una regulación para esta nueva forma de proveer servicios financieros y de seguros. Se basan en el conocimiento completo que tienen sobre el mercado sus propios agentes (los proveedores de los servicios), el alto índice de cumplimiento de estas regulaciones (dado que son los propios obligados los que fijan el estándar) y la importancia de la reputación en el mercado financiero, que para los proveedores sería el activo más importante.

Tal como señala Lehmann, otra ventaja de esta propuesta es que estos estándares regulatorios pueden ser aplicados o exigibles a nivel global, sin necesidad de adoptar una regulación propia para cada país (2019, p. 11). Se trataría de una exigencia de cumplimiento de un estándar fijado por los propios obligados en beneficio de la creación de una buena reputación.

Lamentablemente, esta propuesta ha sido desmentida por la realidad. A pesar de que se reconoce la utilidad de la autorregulación combinada con regulaciones estatales (como es el caso de Suiza o Estados Unidos), no es correcto señalar que la autorregulación por sí misma sea una solución a los riesgos existentes en el mercado financiero. Para dar un ejemplo concreto de esto debemos referirnos a la labor de la Financial Crisis Inquiry Commission (en adelante, FCIC) de los Estados Unidos de Norteamérica, una comisión creada por el Congreso de dicho país para examinar las causas de la crisis financiera y económica durante el 2008. El reporte final de la FCIC (2011) concluyó que los supervisores bancarios no identificaron y controlaron de manera adecuada y proactiva las debilidades de los bancos y su mal gobierno corporativo y gestión de riesgos, y a menudo mantuvieron calificaciones satisfactorias de las instituciones hasta justo antes de su colapso. Esta falla, señaló la comisión, fue causada por muchos factores, incluyendo la creencia de que la regulación era excesivamente onerosa, que las instituciones financieras eran capaces de autorregularse y que los reguladores no deberían interferir con las actividades reportadas como rentables.

Como podemos apreciar, la autorregulación no parece ser una solución en sí misma o como única respuesta al creciente mercado de servicios *FinTech*. No obstante, no se puede soslayar la im-

portancia de la creación de estándares propios de la industria y cómo estos pueden contribuir para generar un conjunto de reglas mínimas en las que no sea necesaria la intervención estatal.

C. *Sandbox* regulatorio

Esta propuesta regulatoria, usada esporádicamente en algunas jurisdicciones, permite crear un espacio de crecimiento para los emprendimientos tecnológicos y que la regulación evolucione de forma conjunta con cada emprendimiento.

El objetivo principal de crear un *sandbox* es permitir que los organismos reguladores otorguen excepciones al cumplimiento de la regulación local para efectos de permitir el desarrollo de innovaciones tecnológicas o productos financieros o de seguros que sean novedosos.

Usualmente, y tal como ocurre en el Reino Unido, Brasil o México, los *sandbox* están condicionados a que el emprendimiento *FinTech* se encuentre por debajo de algunos límites (en número o monto de operaciones y/o cantidad de consumidores). Una vez superados estos límites, la regulación financiera o de seguros sería inmediatamente aplicable a la actividad de la compañía.

Como se explica en un reporte del FMI, algunos países en la región han introducido mecanismos de facilitación que podrían considerarse *sandbox* regulatorios con el fin de no limitar la innovación y el desarrollo del mercado (Berkmen *et al.*, 2019, p. 24). Por ejemplo, México permite a las empresas *FinTech* y a las entidades del sistema financiero experimentar con nuevos modelos de negocio bajo una autorización especial otorgada por el Banco de México y los reguladores del mercado financiero, mercado de valores y de seguros.

En esa misma línea, mediante Decreto de Urgencia 013-2020 de 23 de enero de 2020, se modificó la Ley General del Sistema Financiero para incorporar una Trigésima Cuarta Disposición Final en la que se establece que la SBS puede autorizar la realización temporal de cualquier operación o actividad a través de modelos novedosos, pudiendo otorgar excepciones a la regulación aplicable a las personas naturales o jurídicas que realicen tales operaciones o actividades. Esta modificación normativa sería el primer paso del Perú hacia el establecimiento de un *sandbox* regulatorio para emprendimientos en el mercado financiero y de seguros.

Nótese que esta norma no establece otras limitaciones para solicitar excepciones a la regulación local más que la exigencia de que se traten de operaciones o actividades a través de modelos novedosos. En ese sentido, estas actividades potencialmente excluidas del ámbito de regulación general podrían ser desarrolladas tanto por nuevos emprendimientos como por las empresas del sistema financiero y de seguros ya constituidas. Nos parece razonable considerando que el impacto del costo regulatorio de los nuevos modelos de negocio no solamente depende del tamaño de la entidad que los pueda desarrollar, sino también de que cada tipo de negocio en sí mismo sea escalable y autosostenible.

Lamentablemente el modelo de *sandbox* regulatorio no soluciona el problema de la extraterritorialidad de la norma. Como hemos explicado anteriormente, la mayoría de los servicios *FinTech* tienen como objetivo una aplicación a escala global. Por lo tanto, el desarrollo de una regulación local (a través del modelo *sandbox* o cualquier otro modelo) no podría solucionar los sobrecostos que afronten las compañías cuando quieran ingresar a nuevas jurisdicciones, ni soluciona la problemática de compañías ya existentes –y de escala considerable– que quieran ingresar al mercado local.

Esta idea también es compartida por Dy, quien considera que no son recomendables las propuestas de un *sandbox* regulatorio o la neutralidad tecnológica[4], ya que no resuelven el problema de qué ley se aplica, ni abordan la necesidad de un regulador competente (2016, p. 11).

En mi opinión, la creación de un *sandbox* regulatorio soluciona un problema coyuntural de los emprendimientos en un mercado local y a una escala reducida. Sin embargo, esta propuesta está lejos de ser la regla general para un futuro en el que las *FinTech* dominen el mercado y tengan operaciones a nivel global.

D. *RegTech* o aplicación de tecnología para la supervisión

Otros expertos en materia regulatoria ven en el desarrollo tecnológico una oportunidad para la modernización de la labor de supervisión de las actividades en el mercado financiero y de seguros.

De hecho, Arner, Barberis y Buckley (2016) desarrollan extensamente esta posición y nos explican que

[4] Entiéndase por 'neutralidad tecnológica' el criterio a partir del cual muchos estados consideran ilegítimo hacer una distinción a nivel legal entre las compañías tradicionales y los emprendimientos tecnológicos.

el *RegTech* nació como una respuesta de la banca tradicional al incremento exponencial del número de sus operaciones y al posible riesgo que esto implicaba de cara al cumplimiento de la regulación. Estas compañías impulsaron la creación de diversos sistemas y tecnologías informáticas con la finalidad de automatizar determinados aspectos del cumplimiento de las normas que les son aplicables. En ese sentido, los avances tecnológicos en materia de cumplimiento normativo estarían vinculados a procedimientos de conocimiento del cliente, prevención de lavado de activos y financiamiento del terrorismo, generación de reportes regulatorios automatizados, análisis de requerimientos patrimoniales y pruebas de estrés, cumplimiento de límites operacionales, y márgenes obligatorios en la negociación de valores.

Los mismos especialistas ilustran el crecimiento acelerado del *RegTech* recordando que muchos bancos importantes (tales como Goldman Sachs, JP Morgan, Citibank, Morgan Stanley, Barclays, Deutsche Bank, HSBC y Standard Chartered) abrieron oficinas en Asia con el único propósito de dedicarlas al desarrollo tecnológico y la administración de las operaciones a nivel global (Arner *et al.*, 2016, p. 31).

A pesar de que el desarrollo tecnológico orientado al cumplimiento de las regulaciones ha sido promovido por las propias entidades reguladas, también es una oportunidad para que los organismos reguladores implementen estos avances con los siguientes objetivos:

i. Reducir los costos que afrontan los reguladores, quienes tienen el rol de supervisar un mercado dinámico y creciente con presupuestos limitados;

ii. Obtener resultados más confiables en su labor de supervisión, considerando que el alcance de la automatización de procesos podría incrementar el número de transacciones que son materia de revisión, algo que no se lograría con el análisis aleatorio de muestras reducidas de transacciones, tal como viene ocurriendo a la fecha;

iii. Dar un paso adelante en la búsqueda de regulaciones cuyo cumplimiento sea posible por los emprendedores en el mercado *FinTech*, permitiendo que la supervisión de estos no sea intrusiva y que los emprendimientos puedan generar reportes automáticos de sus operaciones, reduciendo los costos asociados al cumplimiento de la regulación; y,

iv. Mejorar los estándares de supervisión y prepararnos para un mercado completamente digital dominado por las compañías *FinTech*.

No obstante, la importancia de la modernización de la labor de supervisión, tenemos que reconocer que esto no soluciona el problema de la extraterritorialidad de la aplicación de la norma y las limitaciones que tiene un estado para regular operaciones transfronterizas. Por lo tanto, si bien estos avances son un paso adelante en la dirección correcta, de ninguna manera serán suficientes para abordar la regulación del mercado *FinTech* y los desafíos que esta nos presenta.

E. Un marco regulatorio global

Una de las corrientes más aceptadas es aquella que propone solucionar el problema de la extraterritorialidad a través de un marco regulatorio aplicable a nivel global, utilizando mecanismos de derecho internacional.

Como es lógico, dentro de este marco general, se encuentran consideradas diversas posturas, desde las más flexibles, que proponen un conjunto de regulaciones mínimas supervisadas por organismos independientes y privados, hasta aquellas más agresivas y rígidas, que proponen tratados internacionales y una supervisión efectuada por organismos de derecho internacional público.

En ese sentido, el análisis más adecuado de esta propuesta regulatoria debería comenzar por las posiciones más rígidas (y aparentemente menos factibles).

En palabras de Lehmann, un defensor de la propuesta de la regulación global, un tratado sobre la materia no sería posible por dos razones fundamentales: la primera es que la industria *FinTech* se caracteriza por su evolución constante y sería imposible cubrir en un solo instrumento legal la totalidad de situaciones que pudieran ser objeto de regulación; la segunda razón tiene que ver con una lectura política de la situación global, es muy complicado que los gobiernos renuncien a su labor de regular una industria que consideran tan importante (2019, pp. 21-22).

Agregaría que la renuncia de los Estados a regular el mercado financiero y someterse a una jurisdicción internacional es más complicada aún si consideramos algunos ejemplos que la realidad nos provee. Me refiero al tratamiento de los derechos humanos a nivel global. Aunque existe un consenso general en casi todos los países de la importancia del respeto por los derechos humanos, no todos han adoptado los instrumentos internacionales o se han sometido a tribunales supranacionales en la misma medida. Hay estados que se niegan a sujetarse a la jurisdicción internacional sobre el tema. ¿Qué nos hace pensar que la industria

FinTech tendría un mejor futuro en el ámbito internacional?

Parece más sensata entonces la propuesta de Lehmann vinculada a la adopción de normas menos rígidas preparadas por entidades con capacidad técnica suficiente, para lo cual propone al Financial Stability Board (2019, p. 22). El cumplimiento de estas normas –que evolucionarían conjuntamente con la industria– sería un requisito que los estados exigirían para el ingreso de tecnología *FinTech* a sus países. A pesar de ello, Lehmann acepta que la necesidad de normas locales no está descartada del todo, pues las diferencias idiosincráticas y económicas entre los países podrían requerir regulaciones diferenciadas (por ejemplo, en el caso de límites operativos) (2019, p. 23).

Nótese, sin embargo, que la exigibilidad de estas normas aún no soluciona el problema de la extraterritorialidad. Esto bajo la premisa de que existirán países con interés de convertirse en ejes del desarrollo del mercado *FinTech* reduciendo el estándar de sus exigencias. La idea de crear regulaciones menos rígidas es ciertamente más sensata que la utopía de tratados internacionales con aplicación global. No obstante, seguimos con el mismo problema ¿cómo aseguramos que todos los servicios *FinTech* que se ofrecen en un país –desde el exterior– cumplan con estas exigencias mínimas?

Por otro lado, cuando nos ponemos a analizar la propuesta de la regulación global surge inmediatamente la discusión sobre el organismo encargado de la supervisión. Esta discusión ha sido analizada a profundidad por diversos organismos e investigadores. De hecho, en la Agenda *FinTech* de Bali[5] (una iniciativa del FMI y el Banco Mundial para recomendar un conjunto de políticas para aprovechar los beneficios y oportunidades del mercado *FinTech*), tanto el FMI como el Banco Mundial han ofrecido su ayuda para mejorar la supervisión colectiva y ayudar a los países miembros en la tarea de supervisión, en colaboración con otros organismos internacionales.

Sin embargo, sabemos que en la actualidad no existe un organismo internacional que supervise a las entidades privadas con relación a temas financieros o de seguros, por lo que lograr la creación de un organismo con esa capacidad parece tan poco factible como un tratado que regule el mercado *FinTech* sustituyendo a las regulaciones locales. Esto se debe tanto a la imposibilidad a nivel político de que un gobierno renuncie a la supervisión local del mercado financiero como a la heterogeneidad del mercado global.

Al respecto, debemos mencionar la conclusión del estudio realizado por Beck y Wagner, en el que se sugiere que se deben usar dos factores para juzgar si un conjunto de países debe delegar la supervisión al nivel supranacional: el grado de existencia de externalidades entre países generadas por la insolvencia de las entidades financieras y el grado de heterogeneidad de los países (2016, p. 259). En ese sentido, los países que enfrentan bajas externalidades y son bastante heterogéneos solo deberían mostrar un nivel modesto de coordinación entre entidades supervisoras. Por otro lado, los países financieramente bien integrados que no sean particularmente heterogéneos deberían tener un fuerte enfoque supranacional de supervisión.

Dada la necesidad de que el mercado *FinTech* sea objeto de regulación a nivel global (y no solamente comunitario), la alta heterogeneidad entre los países nos conduciría a una supervisión supranacional ineficiente.

En cambio, bajo una estructura de supervisión descentralizada, tendremos no solamente diferencias en cuanto a la interpretación y aplicación de las regulaciones internacionales, sino a países compitiendo entre sí para convertirse en ejes de desarrollo *FinTech*. Esta competencia podría generar incentivos para que los gobiernos reduzcan el nivel de exigencia del cumplimiento de las normas internacionales.

Para abordar esta problemática, Lehmann (2019) propone construir un modelo de regulación competitiva pero que la base de la competencia entre los distintos países sea el grado de confianza en el cumplimiento de la regulación internacional y el profesionalismo de los organismos reguladores. Se propone trasladar al consumidor la información suficiente sobre el organismo regulador de cada empresa del rubro, para que este decida si contrata con la misma o no sobre la base de la confianza que le genere el país de origen de cada compañía.

Esta propuesta es interesante; sin embargo, probablemente sea insuficiente si tenemos en cuenta que el origen del país y el profesionalismo del regulador competente no es toda la información que un consumidor requiere para adoptar una decisión con conocimiento razonable de los riesgos que afronta al contratar los servicios de una compañía *FinTech*. Asimismo, no todos los riesgos derivados de la industria *FinTech* están referidos a costos que

[5] Véase Fondo Monetario Internacional (2018).

deba asumir el consumidor, también hay riesgos sistémicos que no se solucionan con la reducción de la asimetría informativa entre proveedores y consumidores.

VI. ¿CUÁL ES LA ESTRATEGIA DE REGULACIÓN MÁS ADECUADA?

Al margen de discusiones ideológicas, la evidencia y los argumentos planteados por diversos investigadores nos permiten concluir que es necesario que aquellas compañías que operan en el mercado *FinTech* tengan algún nivel de regulación mínimo que mitigue los riesgos propios de la industria y los riesgos asociados a las operaciones financieras transfronterizas.

También podemos concluir que esta regulación no debería afectar el crecimiento de esta industria que, desde todos los ángulos, resulta beneficiosa para los consumidores y para el desarrollo económico y la inclusión financiera.

Sin embargo, también nos queda claro que ninguna de las alternativas planteadas para la regulación y supervisión soluciona el problema de la aplicación extraterritorial de la norma y de su exigibilidad a sujetos y entidades sin presencia física en el territorio nacional, salvo por dos posiciones contrapuestas. La primera consiste en que la exigibilidad de la legislación local debería sustentarse en la capacidad del gobierno para bloquear servidores o páginas web a través de las cuales las compañías *FinTech* brindan servicios transfronterizos. La segunda posición es la adopción de una legislación supranacional que regule al mercado *FinTech*.

Con relación a la primera posición, debo reiterar mi rechazo a la posibilidad de que un país limite el acceso de sus ciudadanos a los contenidos de internet. Tal como se expone en el presente artículo, estas limitaciones son creadoras de desigualdades, potenciales conflictos políticos y fragmentación de la regulación a nivel global, convirtiendo en insostenibles los emprendimientos *FinTech* que dependen de contar con un negocio a escala mundial.

Sobre la segunda posición, si bien la alternativa es razonable, y algunas de las propuestas resultan lo suficientemente flexibles para no afectar el crecimiento del sector, debo dudar de la capacidad de coordinación internacional para conseguir tal objetivo. Como hemos visto, existen incentivos para que los países no solamente se alejen de la coordinación (incentivos políticos), sino también para que compitan entre sí para convertirse en el mercado principal o el promotor de la industria, reduciendo el nivel de sus exigencias regulatorias. Por lo tanto, considero que los esfuerzos de los países deben concentrarse primero en buscar soluciones de corto plazo, sin abandonar el ideal de una regulación global que, eventualmente, pueda reducir los incentivos de que los países compitan entre sí por quien tiene la regulación menos costosa, sino por quien tiene organismos reguladores más profesionales (tal como propone Lehmann).

Las soluciones de corto plazo que, en mi opinión, deberían explorarse corresponden a mecanismos de transparencia de la información e inteligencia financiera. Es evidente que el mercado *FinTech* está creciendo a un ritmo más acelerado que la capacidad de los Estados para coordinar acciones internacionales y, considerando que cerrar las fronteras no es una opción, debemos notar que quien asumirá en primer término cualquier riesgo será el consumidor (sufriendo los efectos de la asimetría informativa, el uso de sus datos personales y potenciales ciberataques a sus cuentas o activos).

En consecuencia, mi propuesta para el acercamiento de los organismos reguladores a la problemática del mercado *FinTech* comprende un trabajo desarrollado en tres etapas principales:

a) Una primera etapa consitiría en que los organismos reguladores proporcionen información a los consumidores para reducir la asimetría informativa. Esta información debería versar sobre el origen de las empresas *FinTech*, su grado de supervisión, si se encuentran sujetas a algún régimen de control, si han sido objeto de sanciones, si cuentan con denuncias públicas o acciones tomadas en su contra por consumidores y si revelan con transparencia la forma en que serán utilizados los datos de cada usuario.

   Esta labor permitiría cambiar el paradigma de lo que entendemos por un organismo regulador y dotarlo de facultades usualmente atribuibles a una agencia de transparencia de información y calificación de proveedores. Esta es una labor fundamental y que, en mi opinión, debería ser el primer paso para reducir los riesgos que afrontarán los consumidores en el corto plazo, a través de un mecanismo público de información que evitaría los riesgos ya señalados de plataformas de calificación privadas (ver sección V.A).

b) Una segunda etapa consistiría en tres labores paralelas. La primera es la necesaria modernización de la supervisión a través de todas las tecnologías *RegTech* desarrolladas hasta el momento. Esto permitiría la

reducción de los costos regulatorios y una supervisión más eficaz de las entidades financieras ya reguladas.

La segunda labor consistiría en la promoción de la autorregulación en el mercado *FinTech*. En ese sentido, ya existen diversas asociaciones privadas del sector conformadas por los proveedores. La creación de estándares mínimos autoimpuestos puede ser una forma bastante eficaz de lograr el cumplimiento de la regulación más importante (por ejemplo, de prevención de lavado de activos y financiamiento del terrorismo), lo que eventualmente se traduciría en una mayor reputación en el mercado de los proveedores que se adecúen a dichos estándares.

La última labor en esta segunda etapa corresponde a la creación de *sandboxes* regulatorios. Una buena forma de reducir los riesgos de la industria es contar con más compañías que ofrezcan servicios a nivel local. El crecimiento del mercado nacional requiere de organismos reguladores que abran las puertas a productos novedosos y que no destruyan un servicio antes de que este pueda despegar y ser sostenible. Sobre la materia, ya hay bastante desarrollo internacional y ejemplos de sobra de lo útiles que son estos espacios.

c) Finalmente, la última etapa, cuyo objetivo es casi utópico, es la creación de una regulación global (basada en normas mínimas y flexibles) y de una supervisión coordinada entre los países.

Si bien eso no va a ser factible en el corto plazo, no veo ninguna razón para que no continúen los esfuerzos para lograr la tan ansiada supervisión supranacional. Recordemos que, a pesar de que esta posibilidad resulta un tanto lejana por razones políticas y de heterogeneidad de los países, Beck y Wagner reconocen que esta situación sufrirá variaciones en el tiempo, dado que los países pueden superar las limitaciones políticas para una cooperación internacional, reduciendo efectivamente la heterogeneidad (2016, p. 259).

En términos generales, la situación actual de la industria *FinTech* requiere de respuestas eficaces y proporcionales de los organismos reguladores y de los legisladores. Es entendible que algunos países quieran aplicar a este sector las normas que ya regulan a la banca tradicional (bajo la premisa de que realizan operaciones similares por medios no tradicionales). Sin embargo, el análisis debe ir más allá y los gobiernos deberán preguntarse hasta qué punto pueden aplicar sus regulaciones efectivamente sin destruir el mercado local y cuáles son las medidas que deberán adoptar para reducir los riesgos de la industria en el corto plazo. Es una situación sin precedentes que requiere de respuestas creativas.

REFERENCIAS

Andina/Difusión (11 de setiembre de 2020). Sector fintech se muestra dinámico y crece 16% este año en el Perú. *Andina*. https://andina.pe/agencia/noticia-sector-fintech-se-muestra-dinamico-y-crece-16-este-ano-el-peru-813408.aspx

Arner, D., Barberis, J., & Buckley, R. (2016). *FinTech, RegTech and the Reconceptualization of Financial Regulation* (University of Hong Kong Faculty of Law Research Paper No. 2016/035). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847806

Asociación FinTech Perú (2021). *Reporte Fintech Perú durante Pandemia 2020*. https://drive.google.com/file/d/1uxSHWj-CJj7W2IcuJ49fF0KuqDSH-UYl/view?usp=sharing

Banco de Desarrollo de América Latina (2016). *La revolución de las empresas Fintech y el futuro de la banca. Disrupción tecnológica en el sector financiero* (Informe 24). https://scioteca.caf.com/bitstream/handle/123456789/976/FOLLETO%20N24%20VFINAL.pdf?sequence=1&isAllowed=y

Beck, T., & Wagner, W. (2016). Supranational Supervision: How Much and for Whom?. *International Journal of Central Banking*, *12*(2), 221-268.

Berkmen, P., Beaton, K., Gershenson, D., Arze, J., Ishi, K., Kim, M., Kopp, E., & Rousset, M. (2019). *Fintech in Latin America and the Caribbean: Stocktaking* (IMF Working Paper No. 19/71). https://www.imf.org/en/Publications/WP/Issues/2019/03/26/Fintech-in-Latin-America-and-the-Caribbean-Stocktaking-46677

Cencchetti, S., Domanski, D. & Von Peter, G. (2011). New Regulation and the New World Global Banking. *National Institute Economic Review,* 216, R29-240. https://doi.org/10.1177/0027950111411378

Dy, M. (2016). *The Challenges to Cross-Border Financial Regulation* (No. CBFL-Rep-MD1). Centre for Banking & Finance Law, Facultad de Derecho, Universidad de Singapur. https://law.

nus.edu.sg/publications/the-challenges-to-cross-border-financial-regulation-in-the-post-financial-crisis-era/

Ernst & Young (2019). *Global FinTech Adoption Index 2019*. https://www.ey.com/en_gl/ey-global-fintech-adoption-index

Financial Crisis Inquiry Commission (2011). *The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States*. https://www.govinfo.gov/app/details/GPO-FCIC/summary

Findexable (2019). *The Global Fintech Index 2020: The Global Fintech Index City Rankings Report*. https://findexable.com/wp-content/uploads/2019/12/Findexable_Global-Fintech-Rankings-2020exSFA.pdf

Fondo Monetario Internacional [FMI] (11 de octubre de 2018). *The Bali Fintech Agenda: A Blueprint for Successfully Harnessing Fintech's Opportunities* [Nota de prensa no. 18/388]. https://www.imf.org/en/News/Articles/2018/10/11/pr18388-the-bali-FinTech-agenda.

Internet Society (18 de octubre de 2018). The Internet and Extra-Territorial Effects of Laws. https://www.internetsociety.org/resources/doc/2018/the-internet-and-extra-territorial-effects-of-laws/

Latin American Private Equity & Venture Capital Association (2020). *LAVCA'S Annual Review of Tech Investment in Latam*. https://lavca.org/industry-data/inside-the-4th-consecutive-peak-year-lavcas-annual-review-of-tech-investment-in-latam/

Lehmann, M. (2019). *Global Rules for a Global Market Place? - The Regulation and Supervision of FinTech Providers* (European Banking Institute Working Paper Series 2019 - no. 45). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421963

Lenz, R. (2015). *"Take Care of Crowd!" - Legal Protection of Retail Investors in Crowdfunding is Long Overdue*. https://dx.doi.org/10.2139/ssrn.2702243

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Decreto de Urgencia 013-2020, Decreto de Urgencia que promueve el financiamiento de la mipyme, emprendimientos y startups, Diario Oficial *El Peruano*, 26 de junio de 2013 (Perú).

Ley 30050, Ley de Promoción del Mercado de Valores, Diario Oficial *El Peruano*, 26 de junio de 2013 (Perú).

10.18800/themis.202101.014

FUNDAMENTOS DE LA REGULACIÓN DEL *CROWDFUNDING*: A PROPÓSITO DEL DECRETO DE URGENCIA 013-2020 QUE ESTABLECE EL RÉGIMEN JURÍDICO DEL FINANCIAMIENTO PARTICIPATIVO FINANCIERO

THE REGULATION OF CROWDFUNDING: REGARDING EMERGENCY DECREE 013-2020 WHICH ESTABLISHES THE LEGAL REGIME FOR FINANCIAL CROWDFUNDING

José Alonzo Jiménez Alemán*
Banco Central de Reserva del Perú

The financing market is one of the cornerstones for the promotion of entrepreneurship, innovation and job creation. In this regard, participatory financing (also known as crowdfunding) is positioned as an important credit tool that, among other characteristics, through technological innovation, creates a flexible ecosystem of direct intermediation that allows investors and promoters to connect on a massive scale. At the same time, it ensures an effective competition of financing sources in the credit market.

In this article, the author presents a general framework on crowdfunding and critically analyzes its regulation in the Peruvian legal system. Along the same lines, taking into consideration comparative experience, he proposes some regulatory recommendations in order to promote the growth of crowdfunding and ensure its proper functioning in the market.

Keywords: Crowdfunding; Superintendencia del Mercado de Valores*; financial participative financing; investors; management companies; promoters.*

El mercado de financiamiento es uno de los ejes de la promoción del emprendimiento, innovación y la creación de empleo. En ese orden de ideas, el financiamiento participativo (o también denominado crowdfunding*) se posiciona como una herramienta de crédito importante que, entre otras características, a través de la innovación tecnológica, crea un ecosistema flexible de intermediación directa que permite conectar de forma masiva a inversores y promotores. A su vez, asegura una competencia efectiva de fuentes de financiamiento en el mercado de créditos.*

En el presente artículo, el autor expone un marco general sobre el crowdfunding *y analiza críticamente su regulación en el régimen jurídico peruano. En esa misma línea, tomando en consideración la experiencia comparada, propone algunas recomendaciones normativas, a fin de potenciar el crecimiento de la figura y garantizar su adecuado funcionamiento en el mercado.*

Palabras clave: Crowdfunding*; Superintendencia del Mercado de Valores; financiamiento participativo financiero; inversionistas; sociedades administradoras; promotores.*

* Abogado. Máster en Derecho de los Sectores Regulados por la Universidad Carlos III de Madrid. Especialista Legal Senior de la Subgerencia de Asesoría Legal en Asuntos Financieros de la Gerencia Jurídica del Banco Central de Reserva del Perú (Lima, Perú). Contacto: alonzo.jimenez@pucp.pe

Nota del Editor: Este artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 7 de enero de 2021, y aceptado por el mismo el 15 de junio de 2021.

I. INTRODUCCIÓN: IMPORTANCIA DEL *CROWDFUNDING* EN EL CONTEXTO ACTUAL

El funcionamiento del mercado de financiación es uno de los ejes de la promoción del emprendimiento, innovación y la creación de empleo, cuyo principal proveedor suele ser la banca tradicional. No obstante, ¿qué ocurre cuando este sector no cubre las necesidades de pequeños y medianos emprendimientos? En este contexto nacen iniciativas que pretenden cubrir los vacíos generados, a través de mecanismos de intermediación que permitan conectar (de forma masiva) a inversores con agentes demandantes de financiamiento. Esta idea es potenciada con el uso de tecnologías de la información, a fin de ampliar los canales de captación de inversores.

Nos referimos al 'financiamiento participativo' o *crowdfunding*[1]. Con esta herramienta se crea un escenario de intermediación directa, el cual consiste en un ambiente tecnológico (plataforma) en el que pueden contactarse 'directamente' promotores e inversores. El *crowdfunding*, a través de la innovación tecnológica, crea un ecosistema flexible, de compromiso colectivo, que tiene como meta convertirse en una alternativa en el mercado. En ese orden de ideas, el *crowdfunding* es concebido como un mecanismo alternativo al de la banca tradicional, por lo cual su promoción impulsa una competencia efectiva en beneficio de los consumidores (Kirby & Worner, 2014).

Sumado al valor intrínseco del *crowdfunding,* existe un factor que mejora su posición como servicio sustituto al financiamiento tradicional y es que no solo se trata de un espacio de interacción con los potenciales inversores, sino también representa un mecanismo de validación de la idea de negocio a partir de los puntos de vista e información de terceros, y funciona también como una herramienta publicitaria[2].

El crecimiento del *crowdfunding* como herramienta de financiación alternativa viene generando el interés de los países por ordenar la actividad y mitigar los fallos de mercado que vienen presentándose desde hace un tiempo. Por ejemplo, el legislador español decidió regular esta actividad económica, a través de la Ley 5/2015 de 27 de abril, de fomento a la financiación empresarial (en adelante, Ley 5/2015). También mereció la atención de la Unión Europea (en adelante, UE) que aprobó el Reglamento 2020/1503, del 07 de octubre de 2020, relativo a los proveedores europeos de servicios de financiación participativa para empresas (en adelante, Reglamento 2020/1503)[3].

En el Perú se aprobó una regulación en materia de financiamiento participativo, mediante Decreto de Urgencia 013-2020 del 23 de enero de 2020, cuyo proyecto de reglamento[4] fue publicado para comentarios por parte del Superintendencia de Mercado de Valores (en adelante, SMV), organismo encargado de asumir la competencia regulatoria y de gestión de la industria. Finalmente, se aprobó el Reglamento de la actividad de financiamiento participativo financiero y sus sociedades administradoras, a través de la Resolución de Superintendente 045-2021-SMV/02 del 20 de mayo de 2021[5].

En este contexto, el presente artículo tiene por objeto brindar un panorama general del *crowdfunding* y los fundamentos de su regulación, a fin de realizar algunas críticas constructivas al régimen jurídico peruano, y plantear algunas recomendaciones para continuar motivando su desarrollo. La experiencia comparada es valiosa para entender el norte de la industria y la postura del regulador en este nuevo escenario de interacción financiera.

II. ASPECTOS GENERALES: DEFINICIÓN, TIPOS Y FUNCIONALIDAD DEL *CROWDFUNDING*

A. Avances conceptuales del *crowdfunding*

De acuerdo a Kirby y Worner (2014), el *crowdfunding* es una herramienta de financiación utilizada para la captación de pequeñas sumas de dinero cuya fuente es un largo número de individuos u organizaciones, que financian un proyecto empresarial o un préstamo personal. Se ha dicho también que el *crowdfunding* o financiación participativa

[1] En el presente artículo se hará referencia a *crowdfunding*, servicios de financiación participativa (referencia de a la normativa europea) o financiamiento participativo (referencia a la norma peruana) como sinónimos. La entidad intermediaria se identificará como 'sociedad administradora', 'plataforma' o 'proveedor de servicios de financiación participativa' (referencia a la normativa europea).

[2] Así lo establece el artículo 4 del Reglamento 2020/1503 del Parlamento Europeo y del Consejo del 07 de octubre de 2020 relativo a los proveedores europeos de servicios de financiación participativa para empresas.

[3] Entrará en vigencia el 10 de noviembre de 2021 y es una referencia imprescindible.

[4] Aprobado mediante Resolución SMV 012-2020-SMV/01, del 26 de noviembre de 2020.

[5] Cabe indicar que las referencias al Reglamento se han realizado en la última revisión del artículo entre el 10 y 13 de junio de 2021, pues el presente artículo fue inicialmente redactado cuando el proyecto de Reglamento se encontraba sujeto a comentarios.

surge como una derivación del *crowdsourcing* que consiste en la puesta en común de recursos de cualquier tipo (ideas, bienes materiales e inmateriales, dinero) por una pluralidad indeterminada de personas interesadas en el éxito de un determinado proyecto, a través de internet y las redes sociales (López Ortega, 2016).

A través de las noticias se conoce que el origen del *crowdfunding* estuvo vinculado a proyectos de ayudas al desarrollo o de la cultura, instrumentados a través de donaciones o de pequeñas recompensas, pero que al incorporar una promesa de remuneración (retribución o reconocimiento) se han convertido en un nuevo modelo de financiación desarrollado sobre la base de las nuevas tecnologías. Este es el caso de la industria musical, en el que bandas como Radiohead han optado por este modelo de financiamiento para sus proyectos artísticos.

Su principal característica es el llamamiento multitudinario al ahorro público a través de una plataforma digital de acceso público, que establece las reglas para la interacción entre inversores y promotores (Alonso Espinosa, 2018; Moreno Serrano, 2016). Precisamente la nota característica del *crowdfunding* (y que llama la atención del regulador) es la naturaleza del llamado al ahorro del público en general. En atención a ello, nos parece adecuada la definición que propone Vieira Dos Santos (2017, cap. I): "[i]n our understanding, Crowdfunding is a form of financing projects and activities, with resource at online platforms, through an open call for investment of the public (crowd)".

B. Característica básica de este mercado: *Two side market*

El *crowdfunding* genera un mercado multilateral o de dos lados (*two-sided* o *multi-sided markets*), el cual se caracteriza por facilitar la presencia de dos o más grupos de usuarios cuyo beneficio deriva de la interacción entre los mismos. En efecto, se trata de mercados que operan sobre segmentos interdependientes de usuarios, que se benefician mutuamente de un efecto de red, en definitiva, del efecto que para que uno de los lados del mercado reciba valor, debe existir otro (Rodríguez Martínez, 2018).

En el caso en particular, nos referimos a los dos mercados a los que está expuesta la plataforma. Por un lado, al mercado de intermediación directa que está conformado por agentes superavitarios que buscan alternativas de inversión; y, por otro, el mercado de financiación, en el que interactúan agentes en busca de fondos para emprender actividades económicas. En este contexto, la plataforma cumple el rol de conectar ambos mercados. Este tipo de interrelación puede ser leída de la siguiente forma: mientras mayor número de agentes superavitarios utilicen la plataforma, más atractivo será el ecosistema para los agentes demandantes de financiamiento.

Considerando que el fenómeno se encuentra en una etapa inicial, se puede indicar que a la fecha no se ha advertido que los efectos de red (propios de este tipo de mercados) constituya un problema en el funcionamiento del mercado como sí lo representa en el mercado de los sistemas de pago encabezado por Visa y Mastercard[6] (Delgado & Pérez Asenjo, 2009).

C. Tipos de *crowdfunding*

El *crowdfunding* puede ser clasificado en dos grandes grupos: (i) no remunerativo y (ii) remunerativo. En el primer grupo, encontramos al *crowdfunding* basado en donaciones y recompensas. En ambos casos los financistas no persiguen un ánimo de lucro en su participación, sino más bien la motivación es de orden filantrópico o simplemente altruista. Se ha dicho que este tipo de campañas fueron las primeras en aparecer, principalmente para proyectos musicales como los de Radiohead o Estopa.

La diferencia entre estas categorías es que, en el no remunerativo, la recompensa a los financistas consiste en una prestación no financiera, como un 'reconocimiento' o 'gesto de agradecimiento' del promotor, tales como la invitación al estreno de la obra, un reconocimiento expreso, descuentos en las producciones, entre otros. No puede negarse que el elemento de la recompensa es clave para muchos financistas o entidades, motivo por el cual también se le denomina prepago, pues se ha utilizado para prepagar servicios o productos, o recibir una contraprestación no financiera con un valor económico cercano a la financiación facilitada (Ló-

[6] En el mercado de servicios de pago físico se ha podido advertir los efectos de red, propios de infraestructuras de procesamiento y compensación de pagos, encabezadas por Visa y Mastercard. En el caso peruano, se pudo advertir la interrelación entre el mercado de emisión de tarjetas (usualmente encabezado por las entidades bancarias) y el mercado de adquirencia (en el caso de Visa, a cargo de una empresa denominada Visanet), en el que los comercios se cometieron a los efectos de red que generó la posición de Visa en el mercado. Ello se traduce en la siguiente situación: en la medida de que la mayoría de las tarjetas de débito y crédito fueron emitidas con la marca Visa (y por ende procesadas con su infraestructura tecnológica), los comercios se vieron obligados a contratar los servicios de adquirencia de Visanet.

pez Ortega, 2016). Es posible afirmar que es uno de los más exitosos, tal como lo ha descrito Vieira Dos Santos (2017):

> If the reward has a low value, that can be considered symbolic, we are facing a mixed donation. «In these situations, there is place for a strong commitment to a steady growth, instead of giving priority to quick profits normally imposed by shareholders».
>
> In the other hand, the contribution of the funder may correspond to the value of the reward. Therefore, the contractual link here can be a purchase contract or a service agreement, in which the funder anticipates paying the price so the beneficiary can have the necessary funds to develop the project or activity. This model of pre-sale has a major success. In fact, the Crowdfunding campaign which had more funds in the world used this pre-sale model, being about a computer game called Star Citizen that raised 105 million dollars in Kickstarter, a reward-based Crowdfunding platform from the United States of America (cap. III.5.2).

En el segundo grupo (de base remunerativa*)*, encontramos el *crowdfunding* de valores y al *crowdlending* (préstamos). En el primer caso, los inversionistas participan en el capital social de la empresa beneficiaria o comprando deuda emitida por el promotor del proyecto. Los inversores reciben acciones, participaciones o títulos de deuda en proporción a su aporte. Estamos frente a una emisión primaria de valores que usualmente no son comercializados en mercados secundarios (Kirby & Worner, 2014), por lo cual la expectativa del inversionista se concentra en el proyecto (como en el caso del *project finance*). Asimismo, el emisor de este tipo de valores tampoco tiene la obligación de registrarlos.

El *crowdlending* es un préstamo que puede realizarse en cualquiera de las formas conocidas en el mercado: persona-persona (en inglés, *peer to peer* o P2P), persona-negocio (en inglés, *person to business* o P2B), negocio-persona (en inglés, *business to person* o B2P) o negocio-negocio (en inglés, *business to business* o B2B). Lógicamente, la contraprestación por el servicio es el interés que la partes pactarán y –seguramente– se encuentra previamente establecido en los términos del proyecto.

Respecto de su **potencial**, se ha señalado que sería un estímulo a la competencia en el mercado de créditos, principalmente en los sectores desatendidos por la banca tradicional (como es el caso de los pequeños y medianos emprendimientos). No obstante, consideramos que su participación también puede extenderse a los sectores rentables (población económicamente activa, consumidores financieros con récord crediticios favorables, grandes empresas, etc.).

D. Descripción básica del funcionamiento de las plataformas

La estructura básica del *crowdfunding* considera tres partes: (i) promotores, (i) inversionistas; y (iii) las plataformas que funcionan como intermediarias entre los dos primeros. Como puede suponerse, el promotor (denominado 'receptor' en la normativa peruana) es una persona natural o jurídica que busca financiamiento para desarrollar e implementar un proyecto de naturaleza cultural, artística, científica o de cualquier actividad económica. Los inversores son las personas naturales o jurídicas que financian los proyectos planteados por el promotor. Como indicamos, un aspecto clave del *crowdfunding* es el *open call* o llamamiento a los ahorros del público en general; por ende, el número de inversores suele ser indeterminado.

El último actor es la plataforma digital, la cual es dirigida por una sociedad administradora[7], cuya labor principal es la selección de proyectos y facilitación de una herramienta de interacción entre promotores e inversores, bajo determinadas directrices para el acceso (principalmente para los promotores). Como se verá, la complejidad de su labor se concentra en el equilibrio de intereses al que debe aspirar en un contexto de multifuncionalidad, pues no solo tiene la labor de poner en contacto inversores con receptores, sino también es frecuente que preste servicios como el asesoramiento empresarial, consultoría en tecnología de información, entre otros[8].

Gállego Lanau (2020) y Cuena Casas (2019) han señalado que el papel de los proveedores de servicios

[7] Para efectos del presente trabajo, los términos 'plataforma' y 'sociedad administradora' serán usados de forma indistinta para referirse a la persona jurídica o entidad que gestiona la plataforma de financiación participativa. Cabe indicar que la legislación peruana la denomina 'sociedad administradora'.

[8] Por ejemplo, en el caso de México, se permite que las instituciones de financiamiento colectiva puedan actuar como mandatarias o comisionistas de sus clientes, en atención al artículo 17 de la Ley para regular las Instituciones de Tecnología Financiera, en función de los parámetros que determine el ente regulador, la Comisión Nacional Bancaria y de Valores (2018). En el ámbito comunitario, el Reglamento 2020/1503 permite que las plataformas puedan cuantificar el precio de las ofertas de financiación participativa (art. 4.4, 2020) y presten el servicio de gestión individual de carteras (art. 6, 2020).

de financiación participativa no es de carácter técnico, automático y pasivo, es decir, no se limitan a transmitir neutralmente en la red una información producida por otros. Los proveedores tienen un papel activo en el control de la información transmitida y almacenada; así como en la realización de servicios subyacentes que inclinan el interés hacia una de las partes, como analizaremos. Considerando esta característica, podemos adelantar que no estamos frente a un agente que actúe de forma estrictamente neutral (como parecería exigirse en el caso peruano y se explicará más adelante).

Respecto del modelo, las plataformas pueden elegir entre dos: (i) *the all or nothing model*, en el que el financiamiento se otorga a los promotores siempre que se consiga el financiamiento mínimo para emprender el proyecto; y (ii) *the all for all model* en el que, independientemente de si se consigue o no el mínimo requerido, se otorga los fondos recaudados al promotor. Por lo general, el esquema elegido en la experiencia de otros países es el primero, a fin de mitigar el riesgo de fraude, como lo ha propuesto la SMV en su proyecto de reglamento[9].

III. FUNDAMENTO DE LA REGULACIÓN: FALLOS DE MERCADO

La intervención del Estado en el ámbito del *crowdfunding* puede enfocarse en dos aspectos: (i) la promoción de su desarrollo por el impacto en la promoción de fuentes alternativas de financiamiento y, por ende, en la competencia en el mercado de créditos; y (ii) los fallos de mercado y el establecimiento de las reglas de conducta de mercado para la protección del inversor.

Respecto del primer punto, la promoción de la industria del *crowdfunding* obedece a razones muy vinculadas al desarrollo económico del país, como es el respaldo financiero a las pequeñas y medianas empresas (en adelante, pymes), pero también está vinculado a factores como la promoción del espíritu emprendedor de la sociedad, la creación de trabajo y, sobre todo, la innovación e investigación (Vieira Dos Santos, 2017). Bajo esta premisa, no es raro que muchos países hayan optado por otorgar beneficios tributarios para su promoción y algunas entidades públicas hayan decidido abrir su propia plataforma (como es el caso de Crowdfunding Bizkaia).

El segundo enfoque de la intervención del Estado en el *crowdfunding* (fallos de mercado y determinadas reglas de conducta) es el que ocupará nuestra atención, pues en este ámbito encontramos multiplicidad de factores que ameritarían regulación. Los fallos de mercado más comunes están vinculados a la asimetría informativa (selección adversa y riesgo moral), aunque también se ha podido verificar la existencia de poder de mercado y barreras de entrada. Se han resaltado otros fallos de mercado como los 'problemas de coordinación y corridas'[10], los cuales no consideramos de una magnitud importante en una realidad como la peruana, sin perjuicio de lo cual deben ser evaluadas en función de la evolución del mercado de *crowdfunding*.

No obstante el enfoque con que se trabaje, no debe olvidarse que la razón más fuerte que justifica la intervención es la captación del ahorro público a través de mecanismos de comunicación masiva[11], pues de otra forma un préstamo o compra de acciones entre particulares no tendría que estar sujeta a la regulación del Estado. Como señala Moreno (2016, pp. 36-38), el valor del *crowdfunding* no radica en la financiación de un proyecto por un grupo de personas, sino más bien el uso de internet como forma de publicitar los proyectos y conseguir la financiación. Podemos resumirlo en la importancia del efecto multiplicador del internet (Rodríguez de las Heras Balell, 2016, pp. 373-374). En la misma lí-

[9] La referencia más importante es el numeral 3 del artículo 40 del proyecto de reglamento, el cual establece que todos los proyectos deben tener un plazo máximo de recaudación. Precisando ello, el artículo 45 del proyecto establece que los proyectos deben tener un plazo máximo de captación de fondos de nueve meses. Finalmente, el artículo 47 del proyecto establece los temas operativos sobre el cierre del financiamiento, entre otros, indicando un aviso previo antes de que finalice el plazo, la forma y plazo para la transferencia de fondos.

[10] Este tipo de problemas surgen cuando se necesitan inversiones simultáneas para que ambas partes de un mercado sean rentables. Se trata de que las inversiones complementen la industria y la hagan crecer. Por ejemplo, para que el mercado de valores sea rentable se necesitan que exista inversión, es decir, compra y venta de valores. En el caso de *crowdfunding*, se descartan (en esta etapa) problemas de coordinación, pues la sostenibilidad y el crecimiento de la industria no depende de la comercialización de los valores o préstamos colocados por el proveedor de servicios de financiación participativa en un mercado secundario (que en muy pocos países ha desarrollado o está permitido), sino en la solvencia del promotor del proyecto. La falta de liquidez de los valores y préstamos colocados, así como la ausencia de un mercado secundario elimina la posibilidad de problemas de coordinación y corridas, que pueden generar –por ejemplo– que, producto de información 'no confirmada', el precio de un valor pueda descender, con el consecuente daño a los titulares.

[11] En esa misma línea, el preámbulo de la Ley 5/2015 señala que una de las características que sobresale en las plataformas de financiación participativa es la participación masiva de inversores que financian con cantidades reducidas pequeños proyectos de alto potencial.

nea de pensamiento, Alonso Espinosa sostiene que la circunstancia esencial que determina la activación de los sistemas de protección de la inversión propios del mercado primario de valores reside en la "apelación pública al mercado de capitales" (2018, p. 347), es decir, al llamamiento público a invertir, en especial a inversores inexpertos.

A continuación, se analizarán los principales fallos de mercado con sus respectivas medidas de mitigación.

A. Selección adversa y transparencia[12]

Este es el fallo de mercado más común en el ámbito del *crowdfunding* pues los inversionistas deben afrontar serios problemas de asimetría informativa respecto de los proyectos publicados en la plataforma, en tanto no tienen la garantía de que el promotor publique toda la información relevante del proyecto, pues el incentivo del promotor es 'vender' un producto, por ende, procurará omitir información poco favorable del proyecto.

Este problema se potencia en el *crowdfunding*, pues el ecosistema suele ser el nicho de financiamiento de aquellos promotores o proyectos que no cumplan con las condiciones exigidas por las entidades bancarias tradicionales, por ende, suelen requerir financiamiento los proyectos más riesgosos y opacos. La clave para mitigar esta falla de mercado es la **transparencia.** Sobre el particular, Cox, Hillman, Langevoort, Lipton y Sjostrom (1991, p. 1) afirman que decidir comprar o vender un valor mobiliario requiere información confiable sobre asuntos tales como la condición financiera del emisor, sus productos y mercados, su administración, y el ambiente regulatorio y de la competencia. Con esta información, los inversionistas pueden intentar hacer un estimado razonable del valor presente del paquete de derechos que la propiedad de un valor confiere.

En este contexto no cabe duda de que existe una gran diferencia entre el nivel de información que el propio emisor o promotor tiene respecto de su situación económica y financiera, que la que tienen los potenciales inversores. Por su parte, Gilson y Kraakman (1984) aportan un fundamento clave en la promoción de la transparencia y es que advirtieron que los niveles de eficiencia de un mercado están estrechamente vinculados con los sistemas de difusión y análisis de información, en el sentido de que menores costos de acceso y procesamiento de la información vinculada al emisor están asociados a mayores niveles de eficiencia del mercado.

Atendiendo a lo expuesto, la transparencia debería ser uno de los pilares de la intervención de la autoridad, pues como ya se ha dicho, los proyectos de *crowdfunding* suelen ser proyectos muy riesgosos y, por ende, la información que debe suministrar debe ser proporcional a ello. Se ha explicado que especialmente, en el caso del *crowdlending*, existe evidencia sobre la falta de transparencia y los riesgos de la operación. Esto significa que los inversores no tienen conocimiento de todos los riesgos, y, por ende, el riesgo es mayor. Se ha demostrado adicionalmente que el retorno de la inversión depende del seguimiento de la inversión, por lo cual algunos países han elevado los requerimientos de transparencia (Kirby & Worner, 2014).

En este contexto, se vienen implementando algunas medidas que equilibran la posición de los inversionistas, tales como:

a) Realizar un *due diligence* sobre la información del proyecto y el riesgo de crédito. Muchas plataformas vienen implementando nuevos métodos de *credit scoring* a través de herramientas como el *big data* (Cuena Casas, 2019).

b) Implementación del mecanismo de 'crédito responsable' (versus la evaluación del riesgo de crédito), lo cual involucra no solo analizar el patrimonio del promotor, sino el grado de esfuerzo que puede suponer el pago del crédito, que puede involucrar un análisis sobre la viabilidad del proyecto o la valoración de los recursos a su disposición. En esa línea, una buena práctica sería que las plataformas hagan públicos los datos de morosidad de los promotores (Cuena, 2019).

c) Que la plataforma invierta en todos los proyectos que selecciona bajo la directriz *skin in the game*, con lo cual se asegura la existencia de un *due diligence* propio de un inversionista (crítica que se exige en las administradoras de fondos de pensiones, incluso). En algunas jurisdicciones, como en Perú o España (con algunos matices), se limita la participación de la plataforma como inversionista, lo cual debería repensarse en atención a este tipo de medidas, como analizaremos.

d) Que los promotores también sean responsables en el plano administrativo por la integridad, completitud, exactitud de la información que proporcionan.

[12] Para el desarrollo de este título, hemos tomado como referencia a Havrylchyk (2018).

B. Riesgo moral e incentivos adecuados en la contratación[13]

Nos referimos al riesgo moral del promotor, es decir, el riesgo de que pueda utilizar de forma indebida el financiamiento. El riesgo de utilizar los fondos captados para otros fines, cometer un fraude, o simplemente incumplir el pago de los intereses o las utilidades que genere el negocio (alegando un retraso, asumiendo la penalidad o simplemente señalando que el proyecto falló). Todo esto es grave en un contexto en el que usualmente no es exigible un colateral o garantía del préstamo o inversión; y cuando el seguimiento del proceso de avance del proyecto lo debe realizar el propio inversionista.

Una estrategia para paliar los efectos de esta falla de mercado es condicionar los pagos al promotor. El esquema *all or nothing* es apropiado para que únicamente sea transferido el financiamiento que alcance el tope exigido por el promotor. Con ello, se evita que el promotor se vea tentado de utilizar el dinero para otros fines o adecuar las características del proyecto al monto recaudado. Una medida adicional es condicionar los desembolsos a determinados hitos, para lo cual es importante el seguimiento del desarrollo del proyecto.

Finalmente, es oportuno indicar que también es aplicable un mecanismo de alineación de intereses del tipo *skin in the game*, a fin de obligar a que la plataforma invierta en todos los proyectos que selecciona, para de esa forma tener cierto grado de certeza sobre la diligencia con que trabajaría. También podría exigirse una inversión mínima del promotor a fin de generar un incentivo positivo para mejorar la diligencia. El hecho de arriesgar su propio capital es un elemento que puede equilibrar los intereses de las partes. Como se ha visto en países como el Reino Unido, si bien esta situación puede generar conflictos de intereses que deben ser gestionados, es un gran dinamizador de la industria.

C. Poder de mercado y barreras de entrada[14]

Queremos hacer una breve referencia a este tema, pues es importante transmitir la experiencia de otros países. Como se sabe, el *crowdfunding* quiere ingresar a un mercado dominado por grandes entidades bancarias, quienes usualmente captan a los mejores proyectos o los promotores con mejor antecedente crediticio, mientras que las plataformas suelen tener como objetivo el mercado desatendido por la banca tradicional (lo cual, como dijimos, involucra más riesgo en la actividad de financiamiento del *crowdfunding*).

En este contexto, se ha advertido un problema en la penetración del *crowdfunding* a los mejores proyectos y sujetos con mejor capacidad de pago, y es la ausencia de una herramienta que permita a las plataformas tener información sobre los antecedentes positivos de las personas. Se ha dicho que la principal causa es que los principales bancos no comparten esta información a las centrales de riesgo de crédito; no obstante, en países como Perú, esto parece haberse superado por las características del registro que manejan las centrales de riesgo.

En materia de barreras estratégicas advertimos dos casos. En el Reino Unido la banca tradicional empezó a invertir en plataformas de *crowdfunding*, pues se advirtió que la regulación prudencial es menos exigente, con lo cual se estarían creando empresas con un poder de mercado que puede dificultar el acceso a nuevos participantes (situación que estaría permitida en la norma peruana, como se verá). Asimismo, en la medida de que las plataformas no son empresas prestadoras de servicios de pago, usualmente deben recurrir a la banca tradicional a fin de contratar alguno de sus servicios, situación que permite a los bancos tomar medidas en contra del desarrollo de la plataforma como es el cobro de tarifas más elevadas, o denunciar el acceso al sistema financiero vía el sistema de prevención de lavado de activos y financiamiento del terrorismo (situación que podría suceder en el Perú con la alternativa de creación de cuentas *escrow*).

IV. COMENTARIOS AL DECRETO DE URGENCIA 013-2020 Y SU REGLAMENTO

A. Aspectos generales de la norma

Con fecha 23 de enero de 2020 se publicó en el diario Oficial El Peruano, el Decreto de Urgencia 013-2020 (en adelante, DU), que promueve el financiamiento de las micro, pequeñas y medianas empresas (en adelante, mipyme), emprendimientos y *startups*; mientras que el 20 de mayo de 2021 se publicó la Resolución de Superintendente 045-2021-SMV/02 que aprobó su Reglamento (en adelante, Reglamento). El objeto de ambas normas es establecer el régimen jurídico de la actividad del financiamiento participativo financiero (en adelante, FPF), así como de las sociedades autorizadas para administrar las plataformas a través de las

[13] Para el desarrollo de este título, hemos tomado como referencia los trabajos de Havrylchyk (2018) y Strausz (2017).

[14] Para el desarrollo de este título, hemos tomado como referencia a Havrylchyk (2018).

cuales se realiza dicha actividad (artículo 15 del DU y artículo 1 de su Reglamento).

Se define el FPF como

> la actividad en la que a través de una plataforma se pone en contacto a personas naturales domiciliadas en el país o personas jurídicas constituidas en el país, que solicitan financiamiento a nombre propio, denominados receptores, con una pluralidad de personas naturales, jurídicas o entes colectivos, denominados inversionistas, que buscan obtener un retorno financiero (Decreto de Urgencia 013-2020, 2020, art. 18; Resolución de Superintendente 045-2021-SMV/02, 2021, art. 18).

Se reconoce como modalidades de FPF al *crowdfunding* de valores y al *crowdlending* (Decreto de Urgencia 013-2020, 2020, art. 19; Resolución de Superintendente 045-2021-SMV/02, 2021, art. 4). Se excluye del ámbito de aplicación de la norma a todas aquellas modalidades que no persiguen un retorno financiero, así como aquellas donde solo participa un único demandante con un único ofertante de fondos (que persiga retorno financiero), o cuando el financiamiento se realice con recursos propios de aquellas empresas gestoras de un medio de comunicación electrónico o digital[15].

Cabe resaltar que las operaciones de *factoring* también se encuentran fuera del ámbito de aplicación de la norma (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 4.2), lo cual fue justificado (en países como España[16]), en tanto el *crowdfunding* no tiene por objeto el financiamiento ordinario de sus actividades (préstamos a corto plazo), sino proyectos empresariales[17]. Sin perjuicio de que no es objeto del presente trabajo realizar una crítica a esta excepción, es importante advertir la inconsistencia de limitar el *crowdfunding* a este tipo de operaciones por dos motivos:

a) La potencialidad y éxito del *factoring* en el país se multiplicará con el uso de medios de divulgación masivos que significará la captación de más ahorro del público. Sumado a ello, el público al que se encuentra dirigido no es necesariamente un público especializado.

b) La norma también admite el financiamiento de proyectos personales que no es otra cosa que la financiación de asuntos domésticos, como puede ser la compra de un auto o la ampliación edificatoria de un inmueble.

Por otro lado, la ley establece que la SMV es la entidad competente para establecer el régimen jurídico de las sociedades administradoras de plataformas de FPF, de los servicios que puedan prestar y demás asuntos vinculados a su operación (Decreto de Urgencia 013-2020, 2020, art. 21). Se le reconoce la facultad de establecer excepciones a las obligaciones, así como la potestad para tipificar infracciones e imponer sanciones a los agentes supervisados (con multas de hasta 700 UIT), entre otras medidas (como la suspensión o cancelación de la autorización, y medidas correctivas como restricciones tecnológicas para impedir su funcionamiento). Se precisa que no se encuentra dentro de su ámbito de supervisión los proyectos de financiamiento, receptores y la integridad de la información revelada, sin perjuicio de lo cual sí tienen competencia para determinar la información mínima que deben difundir.

Por su parte, se reconoce que el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (en adelante, Indecopi) es la autoridad competente para conocer las presuntas infracciones a las disposiciones contenidas en el Código de Consumo y en el Decreto Legislativo 1044, así como para imponer las sanciones y medidas correctivas que resulten aplicables (Decreto de Urgencia 013-2020, 2020, art. 21.6).

Se plantea un régimen de acceso al mercado de las empresas que depende de la reglamentación de la SMV. Precisamente el Reglamento plantea un esquema de habilitación en dos etapas (común en el ámbito financiero): autorización de organización

[15] Se ha tomado conocimiento de que la razonabilidad de la excepción es 'proteger' al inversionista. En caso exista un solo inversionista, se trata de un negocio P2P que no califica como financiamiento colectivo. Por otro lado, tampoco se encuentra dentro del alcance de la norma el financiamiento otorgado por la misma plataforma de comunicación digital a favor del promotor de un proyecto (no nos queda claro si, para estar fuera del ámbito de aplicación, la plataforma debe constituirse como único inversor).

[16] Para revisar el sustento de la exclusión de las operaciones de *factoring* en el financiamiento participativo, véase el documento de preguntas y respuestas sobre *FinTech* que emitió la Comisión Nacional del Mercado de Valores (2019).

[17] A nuestro juicio, no se trata de replicar lo que ocurre en otras jurisdicciones, sino también analizar los fundamentos de la regulación y analizar si es consistente o no establecer las mismas restricciones. En el caso del f*actoring*, se ha obviado a uno de los principales pilares de la regulación: la captación del ahorro de público a través de medios masivos. Esta excepción, por el lado de las sociedades administradoras de emprendimientos de *crowdfactoring*, puede representar un gran 'alivio' por la carga regulatoria que no están obligados a cumplir, con lo cual la evolución de esta industria dependerá de las buenas prácticas que implementen empresas como Finsmart, que vienen realizando un gran trabajo.

y autorización de funcionamiento (2021, título II, cap. I & II, respectivamente). Dentro de los requisitos más importantes para la obtención de la autorización de organización advertimos los siguientes:

a) Que los accionistas, directores y gerentes de la sociedad administradora, en todo momento, no deban estar incursos en los impedimentos contenidos en el Anexo B de las normas comunes a las entidades que requieran autorización de organización y funcionamiento a la SMV, aprobado mediante Resolución SMV 039-2016-SMV/01 (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 15.1).

b) Los gerentes de la sociedad administradora deben contar con reconocida y demostrable capacidad o experiencia profesional, de acuerdo con el cargo a desempeñar, la naturaleza y complejidad de la operación. La capacidad profesional se acredita con el grado de bachiller, maestría o grado superior; mientras que la experiencia profesional con no menos de dos años (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 15.2). Cabe indicar que, en el proyecto de reglamento publicado en el mes de noviembre de 2020, la SMV propuso cuatro años como plazo de experiencia profesional mínimo.

c) Un capital social de S/ 300 000 (trescientos mil soles) íntegramente aportado y pagado en efectivo (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 22). Cabe indicar que el proyecto de reglamento planteó un capital mínimo de S/ 400 000 (cuatrocientos mil soles), el cual podía cumplirse con una combinación de aporte en efectivo más una carta fianza bancaria que dé lugar a dicho monto[18] [19]. Sin perjuicio de ello, es preciso observar que el artículo 23 del DU ha señalado que el monto del capital dependerá de las operaciones y riesgos asociados a la actividad, por lo que sorprende la decisión adoptada por la SMV (Decreto de Urgencia 013-2020, 2020).

   Este requisito merece un comentario especial por el potencial de obstaculizar el desarrollo de la industria. En primer lugar, debemos preguntarnos cuál es el objeto del requerimiento de un capital mínimo. La SMV, en la matriz de comentarios a la propuesta de reglamento[20], ha explicado que se trata de un parámetro prudencial que se aplica a todas las entidades bajo el ámbito de supervisión de la SMV, y que busca que estos cuenten con los niveles de solvencia necesarios para asumir las exigencias y responsabilidades para las que han sido autorizadas. Sobre el particular, es muy interesante lo señalado por la Asociación Peruana de Capital Semilla en la matriz de comentarios referida, lo cual es consistente con la naturaleza jurídica del *crowdfunding* explicada líneas arriba: "Si bien el capital mínimo es un aval de solvencia económica, se debe considerar que las administradoras solo serán conectores '*matchmakers'* de oferta de inversionistas con demanda de financiamiento de proyectos. No son un intermediario financiero*"* (Superintendencia de Mercado de Valores [SMV], 2018).

   Dada la naturaleza de las actividades de las sociedades administradoras, es oportuno replantearse los riesgos a los que se encuentra expuesta y si es necesario mantener un requerimiento de capital de esa magnitud. No debemos perder de vista que el modelo de negocio del *crowdfunding* es el de la **economía colaborativa** en el que el 'mediador' solo cumple una función de contacto. Véase también que sus responsabilidades en la custodia del dinero se han acotado bastante con las herramientas establecidas para viabilizar los servicios de pago involucrados. De hecho, como analizaremos, no le correspondería asumir a la sociedad administradora este tipo de servicios.

Respecto de los servicios que puede prestar la sociedad administradora, el Reglamento los clasifica en dos tipos: (i) obligatorios y (ii) adicionales. Los servicios obligatorios están vinculados principalmente a la provisión de la infraestructura tecnológica para el contacto entre inversores y receptores[21], así como la recepción, selección y publicación

[18] El importe máximo de la carta fianza debía ser del 40% del monto antes indicado (artículo 23 del proyecto de reglamento).

[19] El Reglamento 2020/1503 prevé que los proveedores de servicios de financiación participativa dispongan, en todo momento, de salvaguardias prudenciales por un importe no menor de € 25 000 (veinticinco mil euros) o, en el caso de que resulte mayor, la cuarta parte de los gastos fijos generales del ejercicio anterior (con algunas condiciones) (2020, art. 11). Nótese la diferencia con la propuesta de reglamento de la SMV, lo cual nos alerta a que se explicite la justificación.

[20] Véase el documento emitido por la SMV (2018).

[21] Los promotores de los proyectos que requieren financiación a través de las plataformas son denominados 'beneficiarios' por el DU, motivo por el cual se usarán de forma indistinta ambos términos.

de los proyectos (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 24). Asimismo, constituye un servicio obligatorio la "identificación, selección y clasificación" (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 42.1) a los receptores y los proyectos, sobre la base de una metodología que deberá ser accesible a los usuarios de la plataforma, a fin de optimizar el estándar de transparencia. Cabe indicar que el proyecto de reglamento de la SMV señalaba que este servicio obligatorio consistía en la identificación y clasificación de riesgos[22], lo cual fue corregido por el Reglamento, pues entendemos que es una labor que excedía a las obligaciones de transparencia que natural y esencialmente deben cumplir las sociedades administradoras.

Respecto de los servicios adicionales, el DU solo previó los servicios de cobranza, no obstante, en el Reglamento se ha establecido un listado enunciativo de servicios y una cláusula general, con la que estamos totalmente de acuerdo, pues promueve la iniciativa de las sociedades administradoras (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 25). Los supuestos referidos son los siguientes:

a) "Ofrecer herramientas, aplicaciones y otras utilidades que permitan al inversionista preseleccionar, sobre la base de criterios objetivos, entre los proyectos publicados, aquellos en los cuales invertir, antes de realizar su instrucción de inversión" (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 25.2). Este servicio adicional es consistente con lo dispuesto en el proyecto de reglamento[23], que dispuso expresamente que la información objetivamente provista a los inversores potenciales no constituye recomendaciones personalizadas o asesoramiento financiero, lo cual brindaba cierta claridad en el régimen jurídico aplicable a las sociedades administradoras en lo que respecta a asuntos vinculados a la transparencia de los proyectos.

b) "Capacitación en materias asociadas con la actividad de FPF y asesoría en áreas de tecnología de la información, mercadeo, publicidad y diseño para promocionar los proyectos" (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 25.3).

c) Otros servicios adicionales siempre que estén asociados o complementen las modalidades de financiamiento participativo y no contravengan lo dispuesto en la normativa vigente. Para ello, la sociedad administradora deberá solicitar autorización al órgano competente de la SMV, adjuntando un documento en el que se describa el servicio (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 25.4).

En el ámbito de la protección al inversionista, el artículo 32 del DU faculta a la SMV para establecer los límites máximos de recursos a recaudar por proyecto, receptor e inversionistas, considerando su naturaleza y monto máximo de inversión en una operación. Las sociedades administradoras velan por el cumplimiento de tales límites. El artículo 31 del Reglamento definió los límites, de acuerdo al siguiente detalle (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 31.2):

a) Límites por proyecto: Para proyectos personales el límite asciende a 50 UIT con un plazo máximo de financiamiento de tres (03) años. Por su parte, para proyectos empresariales se estableció un límite ascendente de 500 UIT[24] (inicialmente el proyecto de reglamento propuso un límite máximo de 250 UIT).

b) Límites por receptor: que en el caso de las personas naturales asciende a 100 UIT y en el caso de personas jurídicas asciende a 750 UIT (el proyecto de reglamento solo estableció 500 UIT). Se realiza la misma crítica que el punto anterior sobre el desincentivo generado por este tipo de límites.

c) Límites por tipo de inversionista: el inversionista no institucional tiene como límite el 20% del monto total de un proyecto, o el 20% del total de sus ingresos anuales o del total de su patrimonio (el que resulte mayor), considerando los últimos doce meses.

[22] Se dice que las sociedades administradoras establecen libremente las metodologías a aplicar para el cumplimiento de dicho fin, a partir de los criterios y de los niveles de riesgo que la SMV establezca.

[23] Último párrafo del numeral 4 del artículo 25 del proyecto de reglamento.

[24] Estos límites son mirados con mucho cuidado en la experiencia comparada, a fin de evitar situaciones que se presten para el 'arbitraje regulatorio', esto es, supuestos en que una persona puede optar por someterse a la regulación que más le convenga, frustrando los objetivos de la regulación no elegida. Esto se ha visto mucho en el *crowdfunding*, pues muchas empresas prefieren 'levantar' capital a través de este mecanismo, pues las cargas regulatorias son menores, respecto de la normativa vinculada al mercado de valores. Véase el numeral 4 del artículo 20 del DU (Decreto de Urgencia 013-2020, 2020).

A los inversionistas institucionales no se les aplica límites, sin embargo, debe garantizarse la pluralidad de inversionista en el proyecto, no pudiendo constituirse como único inversionista.

Un comentario general respecto a estos límites es que muchos emprendimientos se verían afectados, pues vienen publicando proyectos por montos mayores. Nos referimos principalmente a los límites aplicables a los receptores, lo cual ha sido oportunamente señalado en la matriz de comentarios al proyecto de reglamento. En este escenario se ha recomendado flexibilizar los límites a través de un esquema gradual que permita ampliar los límites conforme a las características de los proyectos.

Dentro de las principales obligaciones de las sociedades administradoras de plataformas de FPF se encuentran (Decreto de Urgencia 013-2020, 2020, art. 25):

a) Contar con metodologías y criterios para la evaluación y selección de los proyectos, los cuales deben ser publicados en la plataforma.

b) Gestionar el riesgo operacional a través de planes de continuidad del negocio.

c) Informar las características de los valores o de préstamos y los riesgos asociados con los mismos; así como de los servicios que presta, tarifas y demás gastos aplicables.

d) Publicar toda información relevante sobre los receptores y los proyectos, tales como su situación financiera y evolución, respectivamente. El proyecto de reglamento exigió que también se publique la metodología para clasificar a los receptores y proyectos de acuerdo con el nivel de riesgos que implica para los inversionistas, y deberá estar sujeto a las directrices de la SMV (numeral 4 del artículo 24).

e) Realizar advertencias y recabar las declaraciones del inversor sobre: (i) la publicación de proyectos en la plataforma no es una recomendación de inversión, ni la emisión de una opinión o garantía de obtención de retornos financieros para los inversionistas; (ii) los riesgos de pérdida total del dinero invertido; (iii) que no se encuentra dentro del ámbito de supervisión de la SMV los proyectos, los receptores, ni la información proporcionada a estos; así como (iv) declararse incompetente para resolver reclamos, denuncias de los receptores o inversionistas relacionados con los proyectos.

f) Difundir –entre otra información– el número o porcentaje de incumplimientos, tasa de morosidad, tarifas y comisiones aplicables a los receptores e inversionistas.

g) Adoptar las políticas y procedimientos necesarios para prevenir los riesgos asociados a conflictos de intereses vinculados con su actividad.

h) Realizar sus funciones con imparcialidad, lealtad y diligencia.

i) Segregar las cuentas donde se gestionen recursos propios de la sociedad administradora, de aquellas cuentas en las que se canalicen los fondos de los receptores e inversionistas.

j) Durante la recaudación de fondos se debe actualizar diariamente el estado de participación de tales fondos para el desarrollo de los proyectos de FPF. El proyecto de reglamento propone que la plataforma advierta la participación de inversionistas institucionales (numeral 7 del artículo 30).

El DU prohíbe que las sociedades administradoras realicen las siguientes actividades (Decreto de Urgencia 013-2020, 2020, art. 26):

a) Recibir en las cuentas donde se gestionen los recursos propios de la sociedad administradora, fondos de los receptores o inversionistas obtenidos como consecuencia del ofrecimiento de valores o préstamos;

b) Conceder créditos o préstamos a los receptores, o inversionistas;

c) Asegurar a los receptores la recaudación de los fondos;

d) Garantizar a los inversionistas la obtención de un retorno financiero o la devolución de los fondos;

e) Realizar recomendaciones personalizadas a los inversionistas sobre los proyectos de FPF que se ofrezcan en su plataforma;

f) Participar, directa o indirectamente, como receptores o inversionistas en proyectos de FPF que se ofrezcan a través de la plataforma bajo su administración;

g) Reconocer como receptores a emisores de valores inscritos en el Registro o a las entidades que se encuentren bajo supervisión de

la Superintendencia de Banca y Seguros del Perú (en adelante, SBS).

La normativa aprobada también establece las características y condiciones del funcionamiento del financiamiento participativo (Decreto de Urgencia 013-2020, 2020, art. 28), siendo los más resaltantes los siguientes:

a) Los proyectos son de tipo personal o empresarial, y es desarrollado íntegramente en el territorio peruano (numeral 1).

b) Debe existir un objetivo de financiamiento y plazo máximo de recaudación (numeral 2).

c) Se reitera que los beneficiarios, proyectos y la información contenida en este no están bajo la supervisión de la SMV (numeral 4). La norma establece que los receptores sí son responsables por la integridad de la información proporcionada (Decreto de Urgencia 013-2020, 2020, art. 30.1).

d) La sociedad administradora no responde por la viabilidad de los proyectos de FPF, ni por la rentabilidad del mismo (art. 28.3). No obstante ello, el DU abre la posibilidad de extender la responsabilidad de las sociedades administradoras, cuando la inexactitud, falsedad u omisión en la divulgación de la información le resulte atribuible (Decreto de Urgencia 013-2020, 2020, art. 30.2).

e) Los receptores no pueden publicar simultáneamente el mismo proyecto en más de una plataforma (art. 28. 5).

B. Comentarios y propuestas al ámbito de aplicación de la norma

El artículo 15 ("Alcance") establece que las disposiciones contenidas en el presente título tienen como objetivo establecer el marco jurídico para regular y supervisar la actividad del FPF (Decreto de Urgencia 013-2020, 2020). Por su parte, el artículo 18 del DU establece que el FPF es una actividad realizada a través de una plataforma que pone en contacto personas naturales "domiciliadas en el país" o personas jurídicas "constituidas en el país" que solicitan financiamiento a nombre propio (receptores) con una pluralidad de personas (inversionistas) que buscan obtener un retorno financiero (Decreto de Urgencia 013-2020, 2020).

Sobre el particular, debemos llamar la atención a que el factor de conexión de la actividad económica con la legislación peruana es el domicilio o constitución del 'receptor', obviando cualquier referencia al domicilio o constitución de los 'inversionistas'. Es más, la SMV, en la matriz de comentarios al proyecto de reglamento, ha señalado que la finalidad del DU es establecer medidas que contribuyan a mejorar el acceso al financiamiento de las mipyme –finalidad que no se condice con la participación de receptores no domiciliados o no constituidos en el Perú– y el financiamiento de proyectos desarrollados fuera del país (2018). Sobre el particular, es preciso hacer referencia a la piedra angular de la regulación sobre *crowdfunding* que es la protección de los inversionistas (ahorro del público).

Tal como se encuentra redactado el ámbito de aplicación de la norma, no se estaría protegiendo el ahorro del público peruano, sino el ahorro de cualquier persona natural o jurídica que contrata con un 'receptor' domiciliado o constituido en el Perú. Por ejemplo, estaría 'escapándose' de la regulación aquellos emprendimientos de personas jurídicas constituidas en el extranjero cuyo objetivo son los inversionistas peruanos para un proyecto que se desarrollará en Perú.

Atendiendo a esta situación es que encontramos mucho fundamento en el planteamiento de la normativa española. Precisamente el artículo 47 de la Ley 5/2015 (2015) establece un ámbito de aplicación consistente con el objetivo de la regulación de *crowdfunding*, que se manifiesta en las siguientes premisas:

a) Estarán sujetas a la regulación las plataformas que ejerzan la actividad en el territorio nacional, al igual que los inversores y promotores (numeral 1). Como puede observarse, se prescinde de toda referencia al domicilio o la constitución pues lo importante es que la 'intermediación' se realice en el territorio español. No importa si la plataforma se constituyó en Argentina o Italia, pues lo clave es determinar si se dirige al público domiciliado en España.

b) Se plantea que no estará dentro del ámbito de aplicación de la norma cuando un residente en España participe por iniciativa propia (como inversor o promotor) en una plataforma con domicilio social en el extranjero que preste los servicios de intermediación propios del *crowdfunding* (numeral 2). Lo que quiere la norma es que el ejercicio de 'intermediación' tenga como objetivo el cliente residente en España, por lo cual si el inversionista (por sus propios medios) toma conocimiento de una posibilidad de inversión en el extranjero, la regulación española no se le aplicaría.

c) Atendiendo a lo anterior, se establecen dos supuestos consecuentes con las dos primeras premisas y son: (i) que no se considera que el inversor participa por iniciativa propia en un emprendimiento colgado en una plataforma, cuando esta anuncie, promocione o capte clientes o posibles clientes en España; y, (ii) cuando la empresa dirija sus servicios específicamente a inversores y promotores residentes en territorio español (numeral 3). Ambos supuestos cierran la lógica regulatoria de la Ley 5/2015, que a nuestro criterio debería ser analizada por el legislador peruano para efectos de cubrir vacíos que puedan perjudicar el monitoreo del desarrollo de la industria.

Prescindiendo parcialmente de esta lógica, el Reglamento ha precisado que el ámbito de aplicación de la regulación comprende la actividad de financiamiento participativo que se realice en "territorio nacional" (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 1.1). Sin embargo, se indica que los proyectos de FPF deban desarrollarse íntegramente en el territorio peruano, lo cual no aporta a la lógica de aplicar la legislación a todo proyecto que se dirija directamente al inversor peruano. Además, el numeral 3 del artículo 1 de la normativa establece que la regulación no es aplicable a las actividades de receptores (promotores domiciliados en el Perú) e inversionistas en plataformas domiciliadas en el extranjero (Resolución de Superintendente 045-2021-SMV/02, 2021). Esto quiere decir que la norma no se aplicará a la captación de inversionistas en el mercado peruano de proyectos que se realicen en el exterior.

Este análisis nos deja una interrogante adicional ¿deberían las plataformas domiciliadas en el Perú o extranjero que captan clientes en el extranjero para un proyecto que se desarrollará en Perú someterse a la regulación peruana? Esta pregunta exige algunas reflexiones que deben meritarse para afinar el ámbito de aplicación de la norma. En su oportunidad, le corresponderá a la SMV absolver estas interrogantes.

Por otro lado, quedan dudas sobre los vacíos que se generarían al momento de interpretar el alcance de "proyecto desarrollado íntegramente en Perú" (en esta época de prestación de servicios a distancia), pues puede ocurrir que el proyecto no sea íntegramente desarrollado en territorio peruano (pues puede formar parte de un plan de expansión internacional de un emprendimiento peruano que se ejecuta parcialmente en el extranjero). El proyecto de reglamento ha cerrado la posibilidad de que se publiquen proyectos que no son desarrollados en el territorio nacional (numeral 13 del artículo 36), por ello es importante incidir en esta discusión, a fin de no truncar los objetivos de internacionalización de emprendimientos peruanos en busca de financiación.

Otro tema de interés es que el financiamiento objeto del *crowdfunding* en el Perú no se limita a un emprendimiento empresarial, sino también aplica a proyectos personales. Es decir, puede aplicar para el financiamiento de actividades empresariales o personales de personas naturales, como sería el caso de los créditos hipotecarios e incluso los vehiculares (aunque los límites cuantitativos y temporales antes señalados no lo hagan viable en términos financieros). Se debería de precisar o aclarar el alcance del término 'proyectos personales' a través de un documento de preguntas y respuestas, por ejemplo.

Finalmente, queremos llamar la atención a una excepción al alcance de la regulación establecida en el artículo 4 numeral 2, punto 2, en virtud del cual se excluye el supuesto en que un único demandante se ponga en contacto con un único ofertante de fondos a través de la plataforma; o cuando el financiamiento se realiza con los recursos propios de la empresa que gestiona la plataforma (Resolución de Superintendente 045-2021-SMV/02, 2021). Sobre el particular, debemos indicar que –para nosotros– el objeto de la regulación del *crowdfunding* es la protección del inversor en el marco de un llamado al ahorro público, con lo que, si un proyecto publicado en una plataforma puede ser financiado por solo un inversionista, eso no debe interferir en la aplicación de toda la normativa aplicable.

La posibilidad de que más de un potencial inversor pueda conocer esta oferta de financiamiento participativo lo obliga al cumplimiento de todos los requisitos. Si lo que se quiere es evitar el cumplimiento de la exigencia, el receptor debe optar por un mecanismo de intermediación directa prescindiendo de la plataforma o por lo menos debe evitar que se publicite a través de esta herramienta. Entendemos la preocupación por la pluralidad de inversionistas, pero sería más consistente con los objetivos de la regulación el meritarse los mejores esfuerzos de la sociedad administradora para alcanzarlo, mas no consagrarlo como una finalidad en sí misma.

Asimismo, encontramos una contradicción (en el mismo DU), pues con la excepción vinculada a la empresa que gestiona la plataforma se le permitiría ser la única inversionista de un proyecto publicado en esta herramienta tecnológica, colisionando con la prohibición establecida en el artículo 26 numeral 6 de participar directa o indirectamente como inversor (Decreto de Urgencia 013-2020, 2020).

C. Los servicios permitidos en el marco del financiamiento participativo financiero en el Perú

De acuerdo al DU (Decreto de Urgencia 013-2020, 2020), dentro del catálogo de servicios que puede prestar una plataforma encontramos los servicios obligatorios, los servicios adicionales determinados por la SMV (art. 24), así como las actividades o servicios prohibidos (art. 26). Es decir, el funcionamiento de la plataforma se restringe a las actividades del artículo 24 y lo que disponga la SMV.

En contraposición, el Reglamento 2020/1503 si bien hace referencia a algunos servicios auxiliares (tales como la creación de un tablón de anuncios, la determinación del precio de un valor, la evaluación del riesgo de crédito de promotores y proyectos), no limita que las plataformas participen en otros servicios. Así pues, el artículo 12 del Reglamento 2020/1503 no hace ninguna referencia a exigir un objeto social exclusivo y el numeral 13 del precitado artículo establece que los proveedores de servicios de financiación participativa pueden participar en actividades distintas a las cubiertas por la autorización, de conformidad con la normativa vigente (2020).

Lo que se pretende en la UE es el reconocimiento de la multifuncionalidad de las plataformas y no limitar su actividad empresarial. Se estructura la norma pensando en que los servicios adicionales o auxiliares sean libremente determinados por cada operador, y proteger el interés de los inversores e integridad del mercado a través de las prohibiciones. Por ejemplo, si lo que se pretende es no permitir el tablón de anuncios (una especie de embrión de mercado secundario), debería explicitarse esta restricción antes de no consignarlo como un servicio adicional permitido, pues las características y necesidades de la industria se encuentran en permanente interacción y perfeccionamiento.

Bajo una razonabilidad similar, después de un período de deliberación, la SMV aprobó el Reglamento del FPF. Concretamente se ha permitido que las sociedades administradoras presten servicios adicionales no previstos expresamente por la norma, siempre que sean compatibles con el marco normativo vigente, previo procedimiento administrativo (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 25.4). Cabe indicar que el proyecto de reglamento no fue redactado en esa dirección, pues solo se previeron dos servicios adicionales: cobranza, y asesoría en tecnología de la información, mercadeo, publicidad y diseño para promocionar los proyectos.

D. La responsabilidad sobre el contenido de la información relevante del receptor y proyecto

Como señalamos, la transparencia en el mercado de capitales es una línea de actuación aplicable tanto al *crowdfunding* de valores como al *crowdlending*, pues en ambos casos se comparte la especial necesidad de información de los inversores en un contexto en el que los emisores o promotores cuentan con más información y estiman mejor los riesgos del emprendimiento que inician. En este punto, queremos incidir en la responsabilidad de cada uno de los agentes involucrados en el ámbito de la información.

1. Responsabilidad del receptor y la plataforma

La norma peruana establece que la obligación de entrega de información recae tanto en el 'receptor' de la inversión como en la sociedad administradora. Por un lado, el DU establece que las sociedades administradoras tienen la obligación de "publicar toda la información relevante sobre los receptores y los proyectos de financiamiento participativo financiero" (Decreto de Urgencia 013-2020, 2020, art. 25.4), por ejemplo, la actualización de los aportes o la información transmitida por el receptor. En ese sentido, el artículo 30 señala que los 'receptores' difunden, a través de las plataformas, la información mínima que determine el regulador, así como aquella requerida por la plataforma, actualizándola, de ser necesario (Decreto de Urgencia 013-2020, 2020).

Asimismo, el artículo 31 dispone que el 'receptor' es responsable frente a los inversionistas respecto de la integridad, cantidad, veracidad y actualización de la información que difunda a través de las plataformas y responde en caso haya suministrado información contraria a lo exigido por el DU (Decreto de Urgencia 013-2020, 2020). No obstante, agrega que la responsabilidad **puede extenderse** a la sociedad administradora, en aquellos casos en los que la inexactitud, falsedad u omisión en la divulgación de la información le resulte atribuible. Esto es confirmado por el Reglamento, el cual establece que "la responsabilidad puede extenderse a la Sociedad Administrador, en aquellos casos en los que la inexactitud, falsedad u omisión en la divulgación de la información le resulte atribuible o le resulte conocida" (Resolución de Superintendente 045-2021-SMV/02, 2021, art. 45.4).

Sobre el particular, debemos señalar que la plataforma presta servicios de intermediación, cuyo objeto es seleccionar proyectos y poner en contacto a los promotores de estos con inversores. Usualmente no se les asigna la responsabilidad por la

completitud, calidad o integridad de la información, sino más bien les corresponde evaluar con la debida diligencia la adecuación del proyecto a los requisitos exigidos por ley. Es decir, se limita a realizar un examen y análisis del proyecto de forma superficial, esto es, sin centrarse en la rentabilidad o viabilidad del proyecto (Gállego Lanau, 2020).

Sin embargo, sí existen supuestos en que la plataforma es responsable por la información suministrada y han sido trabajados por doctrina especializada (Gállego Lanau, 2020). Hemos querido presentar los principales supuestos trabajados en Europa, para lo cual se adecuaron a nuestro ordenamiento jurídico:

a) Por incumplir las obligaciones de información general sobre el funcionamiento de la plataforma y lo riesgos de la financiación participativa. El numeral 1 del artículo 25 establece que las sociedades administradoras deben contar con metodologías y criterios para la evaluación, y selección de los proyectos. Asimismo, la norma exige, en el numeral 3 del artículo 25, que se informe sobre las características de los valores o préstamos, así como los riesgos asociados a los mismos y las condiciones de financiamiento.

   A pesar de ser una obligación de fácil atención (pues basta con publicar esta información en el portal) su incumplimiento podría generar incluso la nulidad del contrato con la plataforma por vicios en el consentimiento (Gállego Lanau, 2020).

b) Por no recabar las expresiones del inversor. El numeral 10 del artículo 25 del DU establece como una obligación de las sociedades administradoras que requieran a los inversores una declaración donde indiquen, entre otros aspectos, que tienen conocimiento del funcionamiento y riesgos de este mecanismo, de la responsabilidad limitada de la plataforma, y que los receptores y sus proyectos no son supervisados o aprobados por la SMV.

   Si bien es cierto esta expresión puede ser vista como un blindaje legal a favor de las sociedades administradoras, su incumplimiento puede generar que los inversores invoquen la nulidad del contrato con la plataforma. Se ha dicho que no correría la misma suerte el contrato de inversor entre el receptor y el inversor (Gállego Lanau, 2020).

c) Por incumplir la obligación de publicar toda la información relevante sobre los receptores y los proyectos ((Decreto de Urgencia 013-2020, 2020, art. 25.4). En el Reglamento, la SMV plantea algunos supuestos como la evolución del proyecto y la situación financiera del receptor; no obstante, aún no termina siendo muy precisa la referencia a información relevante, motivo por el cual deberá analizarse caso por caso (artículos 24 y 42). Esta obligación podría incluir la de difundir el contenido mínimo exigido por la normativa vigente.

   Un tema importante es que la norma establece el nivel de diligencia con que debe conducirse la plataforma, pues el verbo rector de la obligación es 'publicar', por ende, debe descartarse cualquier referencia a 'conseguir' u 'obtener' información por sus propios medios. Entonces, el incumplimiento sería no publicar información que tenía disponible sobre determinado receptor o proyecto.

d) Incumplimiento sobre la integridad de la información. De acuerdo con el DU, los receptores son responsables de la integridad, suficiencia y comprensión de la información difundida a través de la plataforma (Decreto de Urgencia 013-2020, 2020, art. 30.1 & 31.1). Sin embargo, el numeral 2 del artículo 31 extiende la responsabilidad a la sociedad administradora en aquellos casos en los que la inexactitud, falsedad u omisión en la divulgación le resulte atribuible (Decreto de Urgencia 013-2020, 2020). Sobre el particular, a continuación vamos a presentar algunas situaciones:

   - Siempre que el origen de la información sea el receptor (promotor), si la información difundida es falsa o existen omisiones relevantes no será responsabilidad de la plataforma.

   - Si las informaciones falsas, engañosas u omisiones relevantes son generadas por la plataforma, o alguna persona vinculada a este, entonces será responsable.

   - Cuando no se publique correctamente la información suministrada por el receptor, la sociedad administradora también será responsable. Esto podría generarse por una omisión de información relevante (efectivamente transmitida por el receptor) o por la modificación de la información relevante por motivos comerciales.

   - Cuando la plataforma conoce que la información es falsa y aun así la publica

también debe responder la sociedad administradora.

- Un supuesto aún más discutible es cuando, aun no teniendo conocimiento de que la información suministrada es falsa, existen alertas o indicios más que razonables para sospecharlo. Si la plataforma ignora estas señales, se puede alegar que no está actuando con diligencia y lealtad (Decreto de Urgencia 013-2020, 2020, art. 25.8) y, por ende, le corresponde responder frente a los inversores.

e) Por incumplimiento en la identificación y clasificación de los receptores y de los proyectos (Decreto de Urgencia 013-2020, 2020, art. 24.3). Si bien es cierto que se les otorga libertad a las sociedades administradoras para establecer la metodología a aplicar, esta debe ceñirse a los criterios y niveles de transparencia que establece la SMV. Sobre el particular, el Reglamento de la SMV ha señalado algunas pautas que deben considerarse para la elaboración de la metodología de nivel de riesgos, tales como: (i) publicar información del sector, industria y localización del proyecto; (ii) en caso de préstamos, debe analizarse la solvencia económica del receptor; (iii) en caso de valores, se debe analizar el historial de negocio y experiencia de los receptores realizando actividades relacionadas al proyecto; y (iv) la clasificación de riesgo del proyecto sobre la base una metodología previamente informada (Resolución de Superintendente 045-2021-SMV/02, 2021, arts. 24. 3 & 42).

Sobre el particular, se ha dicho que la prestación de este servicio aleja a las plataformas de ser meros escaparates donde se publican los proyectos de los promotores; por ende, se debe exigir un sistema de responsabilidad específico, como ocurre con las agencias de calificación crediticia, quienes responden por negligencia grave (Gállego Lanau, 2020). Como puede advertirse, si bien es cierto que el proyecto de reglamento de la SMV delimita la actuación de la plataforma en muchos casos, en otros, aún queda un nivel de discrecionalidad fuerte, por ejemplo, al momento de evaluar el proyecto en sí mismo, por lo cual la responsabilidad de la plataforma está muy presente en este ámbito de la evaluación de riesgos de los proyectos.

2. Responsabilidad de la SMV

Respecto de la SMV, en el DU se ha reiterado que los proyectos de FPF, los receptores, y la integridad y veracidad de la información revelada por estos no están bajo la supervisión de la SMV, no obstante, sí puede establecer los estándares de conducta de mercado (Decreto de Urgencia 013-2020, 2020, arts. 21.3, 25.4 & 28.4). Es decir, 'te regulo, pero no te superviso'.

Esta situación trae una primera implicancia que es la ausencia de un mecanismo que promueva o incentive el cumplimiento de la normativa en materia de transparencia, especialmente a los receptores. Si bien es cierto que existen sectores en que la regulación carece de un régimen de incentivos o sancionador explícito (principalmente debido a la madurez del sector y sus agentes), no parece ser la lógica en este sector (aún joven), en el que la regulación europea, por ejemplo, reprime inconductas de la plataforma y del receptor[25].

De lo que se trata no es seguir a milímetro cada proyecto, sino institucionalizar el *crowdfunding*, a través de una entidad que proteja al inversor frente al receptor en temas neurálgicos, lo cual –sin duda– no está cubierto por la competencia del Indecopi, quien solo podría ocuparse de los conflictos generados a propósito de la relación de consumo inversionista-plataforma y receptor-plataforma. Es un asunto en el que se requiere ser consecuente, pues da la sensación de que, por un lado, se limitan mucho las actividades de las plataformas; y, por otro, se quiere ser muy laxos con la supervisión de su funcionamiento y se brindan muchas facilidades para la operación.

E. La imparcialidad como directriz de funcionamiento para las sociedades administradoras y la gestión de los conflictos de intereses

Como se ha podido advertir, el funcionamiento de las plataformas de *crowdfunding* involucra la prestación de servicios tanto a promotores como a inversores, pues –inicialmente– pone a disposición de ambos un ambiente de interacción de intereses económicos, en el que podría desarrollarse con cierta imparcialidad, motivo por el cual el propio

[25] Artículo 23 del Reglamento 2020/1503 (2020):

> 9. Los Estados miembros velarán por que la responsabilidad por la información que figure en una ficha de datos fundamentales de la inversión recaiga, como mínimo, en el promotor del proyecto o en sus órganos de administración, dirección o supervisión.

DU y su Reglamento exigen un comportamiento en este sentido (Decreto de Urgencia 013-2020, 2020, art. 25.8; Resolución de Superintendente 045-2021-SMV/02, art. 32.2).

Nuestro interés en este apartado es demostrar que la imparcialidad no puede ser interpretada como una directriz irrestricta en el funcionamiento de las plataformas de *crowdfunding*, motivo por el cual queremos adentrarnos en su **funcionamiento contractual**. De acuerdo con diversos autores, el contrato de mediación o corretaje es la categorización más cercana a las operaciones básicas del *crowdfunding*, pues coinciden sus elementos característicos (Alonso Espinosa, 2018, pp. 341-342; Lázaro Sánchez, 2018, pp. 30-31; Macanás Vicente, 2018, p. 76):

a) No hay una relación de dependencia o representación.

b) El promotor contrata los servicios de la sociedad administradora, con el objeto de que esta lo contacte de forma masiva con potenciales inversores y, de esa forma, facilitar la conclusión de un contrato.

c) La sociedad administradora no actúa en representación de los inversores, pues su labor se limita a poner a su disposición las condiciones para que contraten. Esto la diferenciaría de otros tipos de contratos de gestión de intereses ajenos como es el contrato de comisión[26], aunque consideramos que, en determinados casos, pueda ser discutible, vista la actuación personalizada de la sociedad administradora.

d) Es un servicio oneroso.

e) El mediador realiza todos sus esfuerzos para contactar al promotor con potenciales inversores, motivo por el cual no suscribe un contrato de mediación con los potenciales inversores, a pesar de lo cual sí que presta servicios de sociedad de la información (desde el punto de vista de la regulación europea).

f) La retribución normalmente responde a una obligación de medios, aunque en la práctica muchas plataformas pactan una retribución adicional por la obtención del resultado[27].

g) La mediación se realiza en el mejor interés de las partes.

Sin perjuicio de ello, existe una característica que Macanás Vicente plantea como esencial –según nuestro parecer, discutible– la cual es la **imparcialidad** del mediador (2018, p. 98). Para sustentar ello, se hace referencia a doctrina civil italiana de inicios del siglo XX, la cual respalda el reconocimiento de la imparcialidad por la función económico-jurídica del contrato. Sobre el particular, debemos señalar que, a diferencia de España y Perú, el contrato de mediación en Italia es un contrato típico y responde a una muy elaborada doctrina, y a una particular ideología (Gázquez Serrano, 2007). Considerando ello, la principal fuente para interpretar los alcances del contrato no podría ser la doctrina o la normativa extranjera, sino más bien la jurisprudencia (en la que no hemos reportado nada sobre el particular) y la costumbre, en la que podemos advertir un marcado comportamiento tendiente a que el prestador del servicio incline sus intereses hacia la parte que paga por el servicio[28].

Por el contrario, parte de la doctrina ha identificado que el mediador **no siempre está obligado a actuar de modo imparcial,** sino que actuará en beneficio del comitente, procurándole la conclusión del negocio en las condiciones más ventajosas posibles. Atendiendo a ello, Gázquez Serrano (2007) señala que solo existen dos escenarios en los que el mediador debe actuar de modo imparcial:

a) Cuando las dos partes acuden al mediador con la única finalidad de que medie en las

[26] Se ha defendido que el contrato que suscribe la sociedad administradora y el promotor es un contrato de comisión, pues se trataría de un **mandato** que tiene por objeto un acto de comercio (puesta en contacto con inversores). Se trataría de una obligación de presar un servicio por encargo de otra. Como puede observarse, el elemento más importante es realizar una actuación en beneficio de un tercero.

[27] En este punto, algunos autores sostienen que la naturaleza del contrato de mediación exige que las obligaciones sean de resultado (Alonso Espinosa, 2018). Sin embargo, Macanás Vicente (2018) explica que es compatible con el contrato de mediación la obligación de medios, y que más bien fue producto de la práctica contractual que se fue exigiendo el resultado como prueba de diligencias de las gestiones de contacto.

[28] No obstante, en el ámbito nacional, Vaisman-Araujo (2018) se inclina por defender la 'imparcialidad' de algunos intermediarios como son las 'plataformas digitales'. En doctrina nacional, Rivadeneyra (1994) también sostiene la imparcialidad del 'corredor', aunque no desarrolla o justifica la natural desviación del interés del corredor por el pago de la retribución. A pesar de que no es el espacio para desarrollarla, nuestra posición se sustenta en que, efectivamente, el corredor o mediador no debe ser dependiente o representar a la persona que realiza el encargo, pero ello no significa que deba actuar de forma neutral o imparcial, sino más bien a prestar el servicio bajo sus propios recursos y lineamientos en el mejor beneficio de su cliente.

negociaciones preparatorias del contrato a concluir entre ellos.

b) Cuando ambas partes son clientes del mediador y están vinculadas con este por sendos contratos de mediación, y el corredor considera que la oferta de una se ajusta a la demanda de la otra. La misión del mediador aquí debe ser eminentemente objetiva, tratando de conseguir la composición más justa de los intereses opuestos de ambas partes.

Como es razonable, en ambos casos se debe exigir una actuación imparcial del mediador, pues existe una relación contractual (remunerada) con cada una de las partes, lo cual es posible en la legislación española y peruana, pues estamos frente a un contrato atípico en el que prevalece la voluntad de las partes.

Estando a lo expuesto, podemos afirmar que la imparcialidad no es una característica inherente del contrato de mediación en España y Perú, pues estamos frente a un contrato atípico, por ende, el contenido negocial dependerá de la voluntad de las partes. Asimismo, como señalamos, otra razón de peso para descartar la imparcialidad son los usos y costumbres del mercado, en el que los intermediadores perciben una retribución por sus servicios y, por ende, sirven al mejor interés de su cliente. Un caso típico es el de corredor inmobiliario o de seguros, el cual debe actuar en el mejor interés de su cliente (el tomador del seguro)[29].

Adicionalmente a lo expuesto, un tema clave en este asunto es que –en la práctica– las plataformas de *crowdfunding* prestan servicios auxiliares como la publicidad de los proyectos, el asesoramiento empresarial a los promotores, mecanismos de ejecución de órdenes de inversión automática, alertas de inversión (que no calificación como asesoramiento al inversor), entre otros. No es menos común que la propia plataforma, en los países que es posible en términos legales, pueda invertir en los proyectos de la propia plataforma o incluso constituirse como promotor[30].

Considerando la multifuncionalidad de las plataformas de *crowdfunding*, podemos denotar que no operan exclusivamente como un intermediario, sino que prestan servicios que naturalmente inclinan sus intereses hacia uno de sus clientes. En esa línea, participan incluso como inversores o promotores (cuya justificación se desarrollará cuando comentemos sobre estas prohibiciones en la normativa peruana), convirtiéndose en una especie de *market-maker*, pues crean un mercado interno de determinados productos para sus clientes (agentes superavitarios), asegurando así la liquidez que requiere el mercado de agentes deficitario.

Nuestra propuesta fue desarrollada en un trabajo más extenso (Jiménez Alemán, 2021) y, evidentemente, apuesta por la flexibilidad de los principios rectores con que se manejan los principales centros de negociación como son las bolsas de valores, en los cuales se exige estándares de imparcialidad bastante altos. En el análisis de la regulación española nos llamó la atención una excepción a la prohibición de los organismos rectores de participar por cuenta propia en el mercado, y que se aplicaba solo a un tipo de centro de negociación, denominado Sistemas Organizados de Contratación (en adelante, SOC)[31], mediante el cual se le permitía negociar por cuenta propia aquellos instrumentos de deuda soberana para los que no existe mercado líquido[32]. Los argumentos presentados fueron utilizados para justificar la flexibilización en la regulación española de *crowdfunding*, la cual permite la participación de la sociedad administradora como inversora y promotora.

Sobre la base de lo expuesto, podemos afirmar que el funcionamiento del *crowdfunding* no ha exigido (desde un plano contractual o práctico) una imparcialidad o neutralidad irrestricta por

[29] En este caso, lo que la jurisprudencia española defiende es la independencia del corredor de seguro respecto de la compañía aseguradora, pues no debe tener ningún vínculo con esta (distinto al caso del agente de seguro que sí tiene una relación con la compañía aseguradora). Al respecto, revisar Sentencia del Tribunal Supremo 63/2007, de 07 de febrero de 2007.

[30] Por ejemplo, en el caso de México, el artículo 17 de la Ley para Regular las Instituciones de Tecnología Financiera (2018) permite que las instituciones de financiamiento colectiva puedan actuar como mandatarias o comisionistas de sus clientes, en función de los parámetros que determine la Comisión Nacional Bancaria y de Valores el regulador (CNBV) (la reguladora).

[31] Según lo denota la Directiva 2014/65 del Parlamento Europeo y del Consejo (2014), un SOC es:

> [un] sistema multilateral, que no sea un mercado regulado o un SMN en el que interactúan los diversos intereses de compra y de venta de bonos y obligaciones, titulizaciones, derechos de emisión o derivados de múltiples terceros para dar lugar a contratos (considerando 23).

[32] En esa oportunidad, defendemos que la razonabilidad de esta excepción es que la iliquidez del valor no le permite al organismo rector **negociarlo** en un mercado secundario, por lo cual no representa un riesgo en el mercado de capitales desde la óptica del uso de información privilegiada y de la integridad del mercado. Asimismo, también puede decirse que la falta de liquidez de los valores es una característica que aleja este tipo de actividades de riesgos sistémicos.

parte del comitente (como lo establece el DU), por lo cual estas características responden más bien a un estándar de conducta que debe matizarse. Esta premisa puede ser confirmada con el Reglamento 2020/1503, el cual no ha elevado la 'neutralidad' al nivel de principio, sino que lo ha exigido como un estándar de comportamiento[33]. En ese sentido, podemos indicar que lo más adecuado es asumir la existencia de conflictos de intereses y, como consecuencia de ello, descartar una conducta estrictamente 'imparcial' o 'neutral', correspondiendo más bien la gestión de los conflictos con la implementación de medidas razonables aplicables para cada caso en concreto.

Para ejemplificar la aplicación de esta regla de conducta, podríamos referirnos al caso en que se permita a la plataforma el uso de herramientas de filtrado (servicio usual en este ámbito), a fin de que el inversor pueda seleccionar los proyectos más afines con sus preferencias de inversión. En este tipo de casos una medida de neutralidad clásica sería que la plataforma no deba pagar ni aceptar ninguna remuneración, descuento o beneficio no pecuniario por **orientar** las órdenes de los inversores a una determinada oferta concreta de su plataforma o en otra. De lo que se trata es proporcionar información a los clientes de manera neutral, sobre la base de las características objetivos del producto (tales como sector económico, instrumento utilizado, tipo de interés, categoría de riesgo) y preferencias del potencial inversor, evitando así cualquier tipo de recomendación.

F. Las prohibiciones de que la sociedad administradora actúe como inversionista o promotor

La prohibición de que las sociedades administradoras funcionen como inversionistas o promotores en su propia plataforma (Decreto de Urgencia 013-2020, 2020, art. 26.6) es una medida clásica para evitar los conflictos de intereses, aunque, en muchos casos, puede ser utilizada como elemento que alinee los intereses de las plataformas con los inversores y promotores, como hemos explicado líneas arriba. A continuación, se comentará cada una de las prohibiciones y se realizarán algunas reflexiones para repensar su tratamiento.

1. Como inversor

Es preciso señalar que el recientemente publicado Reglamento de FPF ha permitido que, **de manera excepcional,** la sociedad administradora participe únicamente como inversionista en proyectos bajo la modalidad de préstamos o valores representativos de deuda que se ofrezcan a través de la plataforma bajo su administración, siempre que su participación no supere el 10% del monto objetivo de financiamiento de un proyecto. Una condición adicional es que el pago del principal más intereses a favor de la sociedad administradora esté subordinado al cumplimiento de las obligaciones del receptor contraídas con los demás inversionistas. Esta situación debe ser informada a los inversionistas de forma clara y accesible (Resolución de Superintendente 045-2021-SMV/02, 2021, 35.6).

Este supuesto comprende la inversión directa de la sociedad administradora, o de personas vinculadas a esta, en los proyectos seleccionados por la plataforma. Esta situación es la que más atención ha generado en los reguladores, pues pone de manifiesto la pluralidad de intereses que pueden concurrir en la plataforma y merecen una actuación de su parte para actuar en el mejor interés de sus clientes. Como es lógico, el interés de la plataforma como inversionista entra en conflicto con el interés de los demás promotores, pues la sociedad administradora aspirará a que ese proyecto en particular obtenga la meta de financiamiento y sea productivo[34].

Países como el Reino Unido, Italia, Bélgica, Austria, México, España, Finlandia e Israel (Havrylchyk, 2018) expresamente han reconocido la posibilidad de que la sociedad administradora participe como inversor en los proyectos seleccionados y colgados en la plataforma, por lo cual es muy relevante la gestión del conflicto de intereses en estos países. Por ejemplo, en España, la propia Ley 5/2015 faculta a la plataforma y sus sujetos vinculados a actuar como inversor (2015, arts. 63.1 & 63.3), siempre que su participación no supere el 10% del objetivo de financiación de cada proyecto o le permita controlar la empresa[35].

Esta situación evidencia que las plataformas cumplen un rol importante para el impulso del

[33] Véase el considerando 18, 19 y 26, así como el artículo 3.3 y 8 del Reglamento 2020/1503 (2020).

[34] En España, el Reglamento 2020/1503 (2020) permitió que las plataformas participen como inversionistas de los proyectos que seleccionen, lo cual fue sopesado con la obligación de transparencia sobre este movimiento. Es preciso indicar que esta situación genera un efecto distorsionador en los inversores que perjudica en términos efectivos a los demás promotores, pues la obligación de 'comunicar' esta situación (así como los criterios adoptados para la decisión) generará un incentivo o llamado de atención a los demás inversores para invertir en dicho proyecto.

[35] Un sector de la doctrina sostiene que esta práctica se justifica en la medida en que las plataformas completan el importe de financiación solicitada por el promotor, de manera que, en último término, depende de ellas el éxito o fracaso de los proyectos (Sánchez Ruiz, 2019).

crowdfunding, lo cual justifica que esta opción no sea eliminada, sino más bien se recurra a la gestión de los conflictos de intereses. Si bien es cierto que una medida idónea para eliminar los conflictos de intereses es prohibir que la sociedad administradora actúe como inversor, pues manejan información privilegiada que pueden utilizarla a su favor (en tanto conocen el proyecto desde su formulación), consideramos que existen propuestas menos lesivas, que podemos enumerar a continuación:

a) Que la plataforma solo pueda intervenir como inversor a fin de 'completar' la financiación de un proyecto en última instancia, es decir, en defecto de la presencia de otros inversionistas.

b) Que la plataforma haga transparente esta situación de forma tal que los inversores conozcan de esta situación. Si bien es cierto que esta medida no elimina el conflicto de intereses, es oportuno que todos los inversionistas lo conozcan.

c) La participación del regulador a fin de autorizar *ex ante* la participación de la plataforma como inversor, constatar el cumplimiento de los estándares de transparencia y el filtro de la información (como en el caso de *equity crowdfunding* regulado en Israel)[36].

d) En el supuesto de que se comunique esta situación, deben generarse mecanismos para no distorsionar la percepción de los inversionistas (pues puede ser interpretado como una 'llamamiento' a la inversión de determinados proyectos, considerando el conocimiento y posición de la sociedad administradora). Para ello, una opción es darle transparencia a esta participación, solo cuando el inversionista haya manifestado un interés en la inversión sin el sesgo de la presencia de la sociedad administradora.

e) Limitar el porcentaje de inversión, en cuanto al porcentaje y al tiempo. Por ejemplo, que la plataforma solo pueda realizar inversiones en la última fase de captación de fondos.

f) Implementar la práctica *skin in the game* a fin de que las plataformas inviertan en todos los proyectos que seleccionen. Este es una herramienta para alinear los intereses de los promotores, inversores y la propia plataforma, pues todos tendrían un interés en común: el éxito del proyecto.

Es muy importante revisar la reacción de los agentes involucrados en el mercado. Una muy interesante fue el comentario realizado al proyecto de reglamento por la empresa Airhouse Company S.A.C., la cual explicó que la prohibición inicialmente propuesta impedía a la sociedad administradora compartir los riesgos con los inversionistas, lo cual a su vez impedía la alineación de intereses, toda vez que tendrían mayor cuidado en la evaluación de los proyectos, puesto que su dinero también está incluido en dicho financiamiento. También manifestó que los potenciales inversionistas en las reuniones sostenidas les preguntaron por qué no invierten en los proyectos que publica en su plataforma, reiterando que se sentirían más seguros de invertir si la sociedad administradora también participa como inversionista.

Como puede observarse, muchas medidas se complementan y su implementación requiere creatividad, por lo cual saludamos la postura de la SMV, a fin de no limitar esta función de la plataforma que usualmente es reconocida en la experiencia comparada[37].

2. Como promotor

Como indicamos en la descripción de este supuesto, no es raro que las plataformas se constituyan por grandes fondos de inversión o incluso entidades bancarias (permitido por el propio DU, numeral 4 del artículo 20), que a la vez tengan interés en participar activamente en determinados proyectos. Por tanto, este supuesto incluye tanto la participación directa de la sociedad administradora como la indirecta, a través de personas vinculadas. Es preciso indicar que no es poco común que las plataformas emitan valores por cuenta propia para financiar la expansión de sus actividades, lo cual es permitido en algunos países como México[38].

[36] La idea es verificar que toda la información disponible pueda ser visualizada por los potenciales inversores, para lo cual no solo se requerirá información del proveedor de servicio de financiación participativa, sino también del promotor. Sería conveniente que en este punto la SMV pueda sugerir el refuerzo de determinada información en favor de la transparencia.

[37] Un caso particular es la Unión Europea. El numeral 1 del artículo 8 del Reglamento 2020/1503 indica que los proveedores de servicios de financiación participativa no tendrán participación alguna en las ofertas de financiación que se encuentren en sus plataformas; no obstante, permite que las personas vinculadas al proveedor (por ejemplo, socios y directivos) puedan invertir en los proyectos de la plataforma, siempre que sea revelado a los potenciales inversores (segundo párrafo del numeral 2 del artículo 8).

[38] Artículo 19, inciso V de la Ley para regular las Instituciones de Tecnología Financiera (2018).

En España, la Ley 5/2015 establece que los proveedores de servicios de financiación participativa solo pueden participar, directa o indirectamente, como promotores siempre que el objetivo de financiación agregado de dichos proyectos no supere en cada ejercicio el 10% de los fondos efectivamente recaudados por los proyectos de su plataforma, y sea debidamente informado a los inversores de forma clara y accesible (2015, art. 63.2-3)[39].

Si bien es cierto que en el ámbito peruano se ha restringido la participación de la plataforma como promotor, consideramos que podría ser repensado este aspecto, en el sentido de encontrar medidas alternativas antes de frenar el avance del *crowdfunding*. La particularidad de este caso respecto del anterior (actuando como inversor) es que en esta situación la plataforma tiene mayor manejo de la información y, por ende, el riesgo de que la información sea manipulada es mayor. En esa línea de pensamiento, una medida adecuada para la gestión del conflicto de intereses, además de las propuestas en el punto anterior, sería reforzar la transparencia. De acuerdo a las circunstancias del conflicto de intereses, a continuación, algunas propuestas para una gestión efectiva:

a) Que el nivel de información exigible sea mayor. Sería recomendable que el regulador establezca el nivel mínimo de información.

b) La sociedad administradora debe tener un grado mayor de responsabilidad sobre el alcance de la información.

c) Que una firma independiente compruebe la veracidad del proyecto, y además califique el riesgo del proyecto, de acuerdo a los parámetros que establezca el regulador.

d) La separación de funciones dentro del proveedor de servicios de financiación participativa, lo cual ha sido contemplado por el Reglamento 2020/1503 (2020, art. 40.1), que permita que el área de selección de proyectos no tenga contacto directo con el área encargada de las inversiones o los propios socios.

e) Que la plataforma participe como inversor a fin de que asuma el riesgo del emprendimiento. Podría tomarse como referencia el principio *skin in the game*[40] (Galacho Abolafio, 2017). En este caso, la participación de la plataforma debería ser considerable (al menos 30%).

En el mercado de valores se han planteado otro tipo de medidas como la implementación de 'murallas chinas' o la creación de empresas 'independientes' para la participación en distintos mercados (para diferenciar las actividades del emisor y del *dealer*), las cuales son también atendibles, aunque su efectividad dependerá mucho de la institucionalidad de las entidades. Por ejemplo, en el caso italiano, la regulación exige que, en caso se realicen ofertas de instrumentos de propia emisión, deben adoptarse medidas adecuadas para la gestión eficaz del conflicto de intereses, lo cual incluye abstenerse de realizar dichas ofertas, cuando estos conflictos no puedan ser manejados adecuadamente para evitar efectos negativos para los inversionistas. Las medidas incluyen la participación de un tercero independiente que garantice la debida diligencia de la transacción y la verificación de la información al más alto nivel directivo.

G. La prohibición de prestar el servicio de asesoramiento financiero a los inversionistas a través de recomendaciones personalizadas

El numeral 5 del artículo 26 del DU establece que las sociedades administradoras se encuentran prohibidas de realizar recomendaciones personalizadas (Decreto de Urgencia 013-2020, 2020). En la misma línea, el numeral 5 del artículo 35 del Reglamento prohibió que las sociedades administradoras brinden asesoramiento financiero o recomendaciones de inversiones en su plataforma o de terceros (Resolución de Superintendente 045-2021-SMV/02, 2021). Las razones que justificarían esta prohibición se centrarían en el carácter reservado de la actividad o los conflictos de intereses que genera esta situación.

En algunos países como España, si bien se restringió que las plataformas realicen recomendaciones personalizadas, pues esta actividad se encuentra reservada; no obstante, se permite que los socios de las plataformas asesoren a inversores sobre los proyectos publicados en la plataforma cuando estén autorizados a prestar el

[39] Es preciso también reiterar que la normativa comunitaria ha proscrito que el proveedor y determinadas partes vinculadas puedan constituirse como promotores. Véase el artículo 8 del Reglamento 2020/1503 (2020), en el que se indica que no podrán participar como inversor o promotor las siguientes personas: (i) los socios que posean al menos el 20% del capital social o de los derechos de voto; (ii) sus directivos o empleados; y (iii) ninguna persona física vinculada a esos socios o directivos o empleados. En ese sentido, puede interpretarse que pueden actuar como inversor de un proyecto de la plataforma, aquellos socios que tengan un porcentaje menor del 20% del capital social, así como sus partes vinculadas.

[40] Este criterio también es aplicado en técnicas de financiamiento como el *project finance.*

servicio de asesoramiento financiero y apliquen una política efectiva en materia de conflictos de intereses[41]. Cabe indicar que el Reglamento 2020/1503 permite la gestión individualizada de cartera, cuya principal característica es la ausencia de discrecionalidad del proveedor de servicios de financiación participativa[42].

Respecto del alcance del término 'recomendaciones personalizadas', parece ser importado de la normativa española. En el ordenamiento peruano no hemos incorporado este término, por lo cual creemos conveniente tomar en consideración la definición establecida en Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Mercado de Valores española, en la que se define el 'asesoramiento en materia de inversión':

> **Artículo 140.- Servicios y actividades de inversión.**
>
> 1. Se consideran servicios y actividades de inversión los siguientes: […]
>
> g) El asesoramiento en materia de inversión […]. No se considerará que constituya asesoramiento, a los efectos de lo dispuesto en este apartado, **las recomendaciones de carácter genérico y no personalizadas que se puedan realizar en el ámbito de la comercialización de valores e instrumentos financieros**. Dichas recomendaciones tendrán el valor de comunicaciones de carácter comercial. Asimismo, tampoco se considerará recomendación personalizada las recomendaciones que se divulguen exclusivamente al público (2015) [el énfasis es nuestro].

Esto también pudo ser precisado por la Comisión Nacional de Mercado de Valores (agencia reguladora española) en un documento denominado Guía sobre la prestación del servicio de asesoramiento en materia de inversión (2010)[43], en el que se indica que el carácter 'personalizado' del servicio significa que se preste de forma explícita o implícitamente como idónea para esa persona en particular, basándose en sus circunstancias personales[44].

En este contexto, el concepto de 'recomendaciones personalizadas' calificaría como un servicio de asesoramiento financiero en materia de mercado de valores (Real Decreto Legislativo 4/2015, 2015, art. 207). De acuerdo con Otiniano Campos y Salas Vigo (2017), este servicio puede ser definido en los siguientes términos:

> Así, el servicio de asesoría financiera es en primer lugar un consejo, una opinión o recomendación efectuada por un asesor con conocimientos especializados en el mercado de valores. Es un servicio que está orientado a descubrir las necesidades financieras de cada inversionista, teniendo en cuenta las particularidades de cada uno –edad, situación personal y profesional, entre otros- y, por tanto, tiene carácter personalizado. Asimismo, la asesoría financiera toma en cuenta lo acontecido en el pasado, en el presente y lo que podría suceder en el futuro, con la finalidad de que el servicio de asesoría se adapte al momento en el que se brinda. Finalmente, este servicio se presta a solicitud del inversionista y debe brindarse de manera adecuada, de modo que busque beneficiar al inversionista, ayudándolo a tomar decisiones de inversión informadas.

---

41 Véase el artículo 63, numeral 1, inciso g) de la Ley 24/1988 del Mercado de Valores (1988).

42 El Reglamento permite este tipo de actividades a los proveedores de servicio de financiación participativa y ha señalado que los modelos de negocio que utilicen procesos automatizados por los que el proveedor de servicios de financiación participativa asigne automáticamente fondos a un proyecto según los parámetros y los indicadores de riesgo predeterminados por el inversor, también llamados inversión automática, deben considerarse como gestión individualizada de carteras de préstamos (Reglamento 2020/1503, arts. 2.1.g & 3.4).

43 Elaborada por el Departamento de Supervisión de ESI-ECA de la Comisión Nacional del Mercado de Valores y publicada el del 23 de diciembre de 2010.

44 Cabe indicar que esta interpretación se realizó en el año 2010, cuando aún se encontraba vigente el Real Decreto 217/2008, de 15 de febrero de 2008, sobre el régimen jurídico de las empresas de servicios de inversión y de las demás entidades que prestan servicios de inversión. Cabe indicar que la definición establecida en dicho cuerpo legal tenía un poco más de detalle. Precisamente, el derogado artículo 5, inciso 1.g definía el asesoramiento en materia de inversión como

> la prestación de recomendaciones personalizadas a un cliente, sea a petición de éste o por iniciativa de la empresa de servicios de inversión, con respecto a una o más operaciones relativas a instrumentos financieros. No se considerará que constituya asesoramiento, a los efectos de lo previsto en este apartado, las recomendaciones de carácter genérico y no personalizadas que se puedan realizar en el ámbito de la comercialización de valores e instrumentos financieros. Dichas recomendaciones tendrán el valor de comunicaciones de carácter comercial. Asimismo, tampoco se considerará recomendación personalizada las recomendaciones que se divulguen exclusivamente a través de canales de distribución o al público […]. La recomendación deberá presentarse como idónea para esa persona, basándose en una consideración de sus circunstancias personales y deberá consistir en una recomendación para realizar alguna de las siguientes acciones […] (Real Decreto 217/2008, 2008).

Sin perjuicio de la experiencia comparada y a la luz de nuestro marco normativo, las razones por las que no se debería limitar la prestación de este servicio a las plataformas de *crowdfunding* son las siguientes:

a) El servicio de asesoramiento financiero no es una actividad reservada, es decir, no está sujeto a la obtención de un título habilitante, por lo cual cualquier persona puede brindarlo y no encontrarse bajo la supervisión de la SMV (Otiniano Campos & Salas Vigo, 2017). Sin perjuicio de ello, la ley permite que este servicio sea prestado por las sociedades agentes de bolsa y las sociedades de intermediación de valores (Real Decreto Legislativo 4/2015, 2015, arts. 194 & 207, respectivamente).

b) Existen *FinTech* que vienen prestando el servicio de asesoramiento financiero (por ejemplo, Finanzas con O'alone, Unicuenta, askRobin o Factoring Lab), muchas de las cuales no cuentan con habilitación legal como sociedades de intermediación de valores o sociedades agentes de bolsa[45].

No puede negarse que, en este tipo de relaciones principal-agente, se presentan conflictos de intereses producto de las relaciones que mantiene el asesor financiero con los emisores, o ejerciendo actividades como 'colocador' o 'inversor', lo cual obligaría a que dicha situación sea 'gestionada' a través de una política clara y transparente, siendo la última opción restringir su prestación por ser la opción más lesiva a los intereses de las partes.

Restringir que los administradores de las plataformas o socios de éstas presten el servicio de asesoría financiera obligaría a que, por ejemplo, las sociedades intermediarias de valores no realicen labores de asesoramiento financiero en la medida de que exista un conflicto de intereses con sus clientes (inversores), lo cual en la práctica no ocurre, y lejos de ello es comúnmente aceptado convivir con este tipo de conflictos de intereses en el ámbito del mercado de valores. Este es el caso de la Unión Europea en donde es permitida la asesoría en materia de inversión de carácter no independiente.

Atendiendo a ello, una opción regulatoria más adecuada sería que las plataformas que pretendan prestar el servicio de asesoría financiera se sometan a las reglas de conducta de mercado flexibles, que pueden incluir, por ejemplo, la obligación de que los asesores efectúen la evaluación del perfil de inversión de sus clientes y en función de ello recomendar productos, práctica que debería reforzarse con infracciones ante su incumplimiento, por ejemplo[46]. También puede optarse por permitir la prestación del servicio de 'gestión individualizada de carteras de préstamos', en virtud del cual el proveedor del servicio asigna, de una cantidad predeterminada de fondos de un inversor, a uno o varios proyectos de financiación de conformidad con un mandato individual otorgado por el inversor a su libre albedrío y de manera individualizada.

H. La plataforma como proveedor de servicios de pago

El numeral 9 del artículo 25 del DU establece como una obligación de las sociedades administradoras a segregar las cuentas donde se gestionen recursos propios de la sociedad administradora, de aquellas cuentas en las que se canalicen los fondos de los receptores e inversionistas (Decreto de Urgencia 013-2020, 2020). Se permite que para este fin constituyan cuentas abiertas en algunas de las empresas del sistema financiero, así como otras opciones (considerablemente más onerosas) como la constitución de un fideicomiso o el uso de dinero electrónico. De acuerdo a la Décima Quinta Disposición Complementaria Final del DU, las cuentas bancarias en las que se canalicen los fondos de los receptores o inversionistas no pueden ser afectadas por obligaciones de la sociedad administradora ni de terceros (Decreto de Urgencia 013-2020, 2020).

Sobre este punto, el artículo 30 del Reglamento ha dispuesto que la sociedad administradora está obligada a segregar las cuentas donde se gestionen sus recursos propios, de aquellas donde se canalicen los fondos de los receptores e inversionistas (Resolución de Superintendente 045-2021-SMV/02, 2021). Se exige además que las cuentas donde se canalizan los fondos de los clientes no puedan ser administradas directamente por la sociedad administradora. Para este fin la norma plantea tres posibilidades:

a) El uso de cuentas bancarias *escrow* abiertas en una entidad supervisada por la SBS que permita el cumplimiento de las obligaciones

[45] Para más información, véase la página web de la Asociación Fintech Perú.

[46] De acuerdo al artículo 17 del Reglamento, se exige que el agente que realice actividad de asesoría de inversiones debe efectuar una evaluación del perfil de inversión de estos clientes, y recomendar productos y servicios que corresponden a su perfil de inversión (Resolución de Superintendente 045-2021-SMV/02, 2021).

contractuales y legales, tales como la identificación de los inversionistas y receptores.

b) Fideicomiso administrado por entidades supervisadas por la SBS y autorizadas a actuar como fiduciarios, en el que la sociedad administradora actúa como fideicomitente. Son beneficiarios del fideicomiso los inversionistas.

c) Cuentas de dinero electrónico, para lo cual la sociedad administradora debe garantizar que dichas cuentas se usen únicamente para analizar los fondos de los receptores e inversionistas.

El servicio descrito se denomina servicio de pago y no es objeto de una regulación específica, salvo algunos esfuerzos particulares como el del Banco Central de Reserva del Perú[47]. Uno de los primeros intentos en conceptualizar el término 'servicio de pago' lo encontramos en la Directiva 2007/64/CE del 13 de noviembre de 2007, sobre servicios de pago en el mercado interior de la Unión Europea, en el que se le define como cualquiera de las actividades comerciales establecidas en el Anexo de la norma[48]. En esta definición se incluyen los típicos conceptos como el depósito o retirada de efectivo de una cuenta, envío de dinero, transferencias entre cuentas de pago, ejecución de operaciones de pago mediante tarjeta de pago o dispositivo similar (mediante cuentas de pago o a través de líneas de crédito).

La Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros (Ley 26702, 2017) ha contemplado este tipo de servicios dentro del grupo de actividades que pueden realizar las entidades sujetas a su supervisión[49]. La norma establece que pueden ser prestados por empresas bancarias, empresas financieras, cajas rurales de ahorro y crédito, cajas municipales de ahorro y crédito, cajas municipales de crédito popular, entidades de desarrollo para la pequeña y microempresa (edpymes), cooperativas de ahorro y crédito autorizadas a captar recursos del público[50].

Uno de los principales tópicos de la regulación de los servicios de pago es garantizar una gestión adecuada de los fondos, pues el negocio exige que el dinero sea temporalmente administrado o custodiado por el proveedor del servicio de pago. Eso indudablemente genera un riesgo que se ha visto conveniente mitigar a través de exigencias prudenciales, en función del volumen de operaciones del proveedor. En el presente caso, se omiten estas exigencias prudenciales a fin de sustituirlo por una cuenta de custodia temporal, a la cual se le otorga un estatus jurídico particular. Indudablemente

---

47 Nos referimos al Reglamento del Servicio de Pago con Códigos de Respuesta Rápida (QR), en el que el servicio de pago se define como "la transferencia de recursos de las Cuentas de Fondos del Consumidor hacia las cuentas del Comercio, utilizando para ello el Código QR presentado por el Comercio" (Circular 003-2020-BCRP, 2020).

48 Los servicios de pago descritos en la Directiva 2007/64/CE son

- Servicios que permiten el depósito de efectivo en una cuenta de pago y todas las operaciones necesarias para la gestión de una cuenta de pago.
- Servicios que permiten la retirada de efectivo de una cuenta de pago y todas las operaciones necesarias para la gestión de una cuenta de pago.
- Ejecución de operaciones de pago, incluida la transferencia de fondos, a través de una cuenta de pago en el proveedor de servicios de pago del usuario u otro proveedor de servicios de pago:
  - Ejecución de adeudos domiciliados, incluidos los adeudos domiciliados no recurrentes
  - Ejecución de operaciones de pago mediante tarjeta de pago o dispositivo similar,
  - Ejecución de transferencias, incluidas las órdenes permanentes.
- Ejecución de operaciones de pago cuando los fondos estén cubiertos por una línea de crédito abierta para un usuario de servicios de pago:
  - Ejecución de adeudos domiciliados, incluidos los adeudos domiciliados no recurrentes.
  - Ejecución de operaciones de pago mediante tarjeta de pago o dispositivo similar.
  - Ejecución de transferencias, incluidas las órdenes permanentes.
- Emisión y/o adquisición de instrumentos de pago.
- Envío de dinero.
- Ejecución de operaciones de pago en las que se transmita el consentimiento del ordenante a ejecutar una operación de pago mediante dispositivos de telecomunicación, digitales o informáticos y se realice el pago al operador de la red o sistema de telecomunicación o informático, que actúa únicamente como intermediario entre el usuario del servicio de pago y el prestador de bienes y servicios (2007, Anexo).

49 En el numeral 29 del artículo 221 de la referida legislación se establece lo siguiente: "Efectuar cobros, pagos y transferencias de fondos, así como emitir giros contra sus propias oficinas y/o bancos corresponsales" (Ley 26702, 2017).

50 Una reflexión sobre el particular nos brinda Álvarez Meza (2018), quien indica que la "prestación de servicios de pago" es una actividad reservada a la licencia bancaria. No obstante, debemos advertir que existen emprendimientos que vienen prestando servicios de pago y son avalados por la regulación actual: (i) Mercado Pago, negocio que presta directamente

es un servicio no estándar que brindarán las empresas del sistema financiero, lo cual generará una contraprestación debida.

Como puede advertirse, el DU y su Reglamento plantean opciones que pretenden sustituir parcialmente la regulación de los servicios de pagos en el contexto del financiamiento participativo, para lo cual se proponen opciones igualmente satisfactorias, en algunos casos onerosas (como el caso del fideicomiso), y en otros novedosas como el uso del dinero electrónico o cuentas *escrow*, cuyo éxito dependerá de su factibilidad operativa (esperamos que se haya consultado esta opción entre las entidades del sistema financiero).

Sin perjuicio de la laxitud de la regulación de los servicios de pago en este ámbito (visto, por ejemplo, la Directiva 2015/2366 sobre servicios de pago en el mercado interior que deroga expresamente la mencionada Directiva 2007/64/CE), consideramos atendible la elección del legislador, pues se trata de una actuación promotora de la industria y prudente a su vez, pues crea un instrumento mercantil idóneo para proteger a las partes expuestas. Sin perjuicio de ello, se debe tener una mirada vigilante por los riesgos que presentará esta actividad en cualquier caso.

V. BUENAS PRÁCTICAS EN EL ÁMBITO DEL *CROWDFUNDING*

La experiencia comparada en materia de *crowdfunding* nos proporciona información sobre buenas prácticas que merecen ser exploradas.

A. Promover el uso y fortalecimiento de las centrales privadas de información crediticia

Una práctica en el ámbito del *crowdfunding* que equilibra el nivel de información entre las partes involucradas es el registro de información de las centrales de riesgo (en adelante, CEPIR). Este puede ser uno de los pocos elementos de información que los inversores y plataformas tienen a su disposición para evaluar el riesgo de crédito de los promotores que se presentan como personas naturales. En este contexto es importante conocer el alcance de la información contenida en este registro.

Así pues, como elemento facilitador de la transparencia en el mercado, el registro manejado por las CEPIRs contiene toda la información que permita evaluar la solvencia económica de las personas naturales, no importando si tiene la condición de consumidor o proveedor de bienes y servicios. El objetivo es difundir información de riesgos negativos (principalmente incumplimientos en el pago de obligaciones de dar suma de dinero) y positivos (la conducta de cumplimiento del deudor), lo cual nos brinda valiosa información sobre la trayectoria de la persona y su historial de crédito[51].

A diferencia de la experiencia española, las principales CEPIR en Perú realizan un reporte y tratamiento de la información de riesgo, lo cual involucra antecedentes positivos como negativos, con lo cual se puede realizar un análisis de la solvencia de las personas más sólido. Las plataformas de *crowdfunding* podrían utilizar esta información que puede ser cruzada con otras herramientas como el *big data*. Todo esto podría generar información sobre el comportamiento del deudor, patrones de pago, lo cual es clave para atender al sector de promotores que asisten a la banca tradicional y cuyo interés puede ser satisfecho también por la banca tradicional.

Cabe indicar que esta propuesta es distinta al denominado régimen de *open banking* lo cual está vinculado a los accesos a las cuentas de los consumidores (principalmente aplicado a los proveedores de servicios de pago y algunos servicios financieros auxiliares), mas no a los antecedentes positivos de crédito de cada uno.

B. La protección del inversor

1. Equilibrio entre los niveles de protección al inversionista en función de su perfil y la promoción del financiamiento participativo

Como se conoce, en el ámbito del mercado de valores la protección del inversor en determinadas circunstancias debe ser matizada, a fin de apor-

servicios de pago con la reciente Circular 003-2020; y (ii) Kambist, *FinTech* vinculada a los servicios de cambio de moneda que presta servicios de pago en la práctica y además se encuentra registrada por la propia SBS mediante Resolución 00335-2017. Existen otros emprendimientos de servicios de pago, que si bien es cierto no tienen un reconocimiento expreso por parte del regulador, vienen actuando con bastante éxito en Perú, tales como Culqui, PayPal, PayU, Pago Efectivo, Payme. Una de las razones puede ser lo prematuro de la industria, lo cual no debe ser interpretado como una permisividad irrestricta, pues entidades las entidades competentes (como el Banco Central) vienen observando de cerca el desenvolvimiento del mercado.

51 Desde un punto de vista referencial, la naturaleza del registro que maneja las CEPIRs se ha podido evidenciar en su defensa en procesos constitucionales de *habeas data*. Entre otras, se ha podido advertir la sentencia del Tribunal Constitucional recaída en el Expediente 03700-2010-PHD/TC (2014).

tar al dinamismo con que evoluciona. Atendiendo a ello es que las reglas de conducta de mercado para determinados emisores se atenúan en función del tipo de inversor al que está dirigida la emisión. Este es el caso de los inversores institucionales, en cuyo caso la propia norma relaja algunos requisitos de transparencia, debido a las características de estos actores[52].

Sobre la base de esta consideración, una opción que se contempló es la clasificación de inversores en función de su experiencia en la industria, a fin de aplicar una protección reforzada como sería aplicar test de idoneidad o conveniencia (como se realiza en la UE), y en función de ello recomendar su participación en la plataforma a partir de límites cuantitativos. En la experiencia comparada, países como Bélgica, Francia e Israel han implementado test para verificar la idoneidad y conveniencia de la inversión respecto del inversor (Havrylchyk, 2018).

El Reglamento hace referencia a las categorías de inversionistas institucionales y no institucionales a fin de establecer algunas particularidades en su régimen jurídico. Así, por ejemplo, el numeral 1 del artículo 31 de la referida normativa establece un límite particular de inversión para los proyectos personales, el cual asciende a 50 UIT en un plazo no mayor de tres años (Resolución de Superintendente 045-2021-SMV/02, 2021). Este límite, a nuestro criterio, frustra la posibilidad de que el *crowdfunding* pueda ingresar a mercados muy interesantes en términos financieros, como el de los créditos hipotecarios o vehiculares (debido a las garantías que respaldan el crédito), tanto por el monto como por el plazo. Esta limitación también aplica a los proyectos empresariales, pues el efecto es **desincentivar** la utilización de plataformas de financiamiento participativo en su etapa inicial. Esta postura ha sido corroborada en la matriz de comentarios del proyecto de reglamento con empresas como AirOrHouse, plataforma especializada en financiamiento de proyectos inmobiliarios.

Por otro lado, en el camino de una efectiva protección del consumidor financiero, la regulación en materia de intermediación de valores solo exige que el agente que realiza asesoría de inversiones evalúe el perfil de inversión de los clientes y, sobre la base de ello, recomendar productos y servicios acordes con ello[53]. Esto se encuentra más cercano a un test de conveniencia, donde se pretende verificar el conocimiento de los riesgos de la inversión. Sin embargo, una buena práctica sería incorporar una especie de **test de idoneidad**, el cual pretende conocer sobre su **formación, conocimientos y experiencia** previos en mercados de valores, su **situación financiera** (fuente y nivel de ingresos regulares, patrimonio, gastos y pagos periódicos). Posteriormente, se preguntarán sobre los **objetivos** de inversión (lo cual ya es exigido por la normativa vigente).

De esta forma, la plataforma podría implementar un sistema de alertas reforzadas sobre los riesgos que tomaría al caso en concreto. Incluso, en caso no se suministre la información requerida, podría rehusarse a prestar el servicio. Esta medida puede contribuir al acceso responsable de esta herramienta por parte del público que no cuenta con mucha experiencia en este tipo de actividades económicas.

2. La protección al inversor no experimentado a través del derecho de revocación de oferta

Una de las medidas adoptadas en la normativa comunitaria es el período de reflexión durante el cual el **inversor potencial no experimentado** puede revocar una oferta de inversión o una manifestación de interés en una oferta concreta de financiación participativa sin dar una justificación y sin que se le aplique una penalidad. Se trata de brindarle un plazo de reflexión adicional, el cual no deberá durar más de cuatro días naturales desde que se realizó la oferta de inversión[54].

En Perú se ha regulado este supuesto bajo el nombre de **cancelación del compromiso de inversión** de forma bastante amplia. El artículo 47 del Reglamento señala que los inversionistas pueden cancelar su compromiso de inversión antes de finalizar el plazo de financiamiento o luego de conocida la identidad del receptor, cuyo plazo deberá ser determinado por cada sociedad administradora (Resolución de Superintendente 045-2021-SMV/02, 2021). Además, se sostiene que la sociedad administradora deberá considerar penalidades para los inversionistas que soliciten cancelar sus compromisos de inversión fuera del plazo que establezcan en sus reglamentos internos. Cabe recordar que la propuesta de reglamento estableció un plazo máximo para la cancelación de la inversión de cuarenta y ocho (48) horas antes de finalizar el plazo de financiamiento o, en el caso de proyectos personales, luego de conocida la identidad del receptor.

52 Este tratamiento puede encontrarse en el Reglamento del Mercado de Inversionistas Institucionales, aprobado mediante Resolución de Superintendencia 00021-2013, del 26 de setiembre de 2013.

53 Véase el artículo 17 del Reglamento de Agentes de Intermediación (Resolución de Superintendencia 00034-2015, 2015).

54 Véase el artículo 22 del Reglamento 2020/1503 (2020).

Sobre el particular, en la matriz de comentarios del proyecto de reglamento, la SMV ha señalado que un procedimiento para la cancelación de compromisos de inversión **dota de mayor confianza al inversionista** para tomar su decisión inicial de inversión, sabiendo que podrá cancelarla previo al cierre de financiamiento en caso cambie alguna de las condiciones bajo las cuales aceptó inicialmente financiar un proyecto (2018).

A nuestro criterio, esta medida les resta seguridad y firmeza a las transacciones, y, por ende, seriedad a los compromisos. Como se ha indicado en la matriz de comentarios del proyecto de reglamento, tal como se encontraba redactado esta disposición genera 'incertidumbre' a los receptores respecto al monto de financiamiento real al que finalmente se tendrá acceso. Esto es, resta previsibilidad al financiamiento exitoso del proyecto. En esa línea, también se ha indicado que esta prerrogativa a favor de los inversores hará 'impracticable' el funcionamiento del esquema de financiamiento participativo, debido a la incertidumbre de los compromisos de inversión. La potencial empresa receptora se verá perjudicada y perderá posibilidades alternativas de financiamiento, pues ni siquiera podrá considerar un buen avance en la colecta como indicador de que recibirá el préstamo.

Asimismo, se advierte que esta herramienta puede servir para manipular el nivel de financiamiento alcanzado, a fin de atraer (de forma fraudulenta) más inversores. La posibilidad de desistirse de la decisión de inversión facilita comportamientos oportunistas, más aún si se considera que la sociedad administradora debe constantemente actualizar la meta de inversión y que los inversionistas muchas veces se guían por información no necesariamente vinculada al proyecto en sí mismo, sino por su recepción en la comunidad de inversionistas.

Para el suscrito, la opción aprobada por el Reglamento también es criticable por dos motivos:

a) La aplicación de la penalidad a quien cancele su compromiso de inversión no mitiga el riesgo de que las cancelaciones puedan ocurrir en el último momento, por lo cual se deberían alargar plazos de colecta o que esta se frustre (por lo limitado de los plazos), perjudicando no solo al receptor, sino también al resto de inversionistas que participan en la colecta.

b) Siempre es preferible que la autoridad adopte un plazo razonable, pues dejarlo al arbitrio de las sociedades administradoras puede involucrar que se limite al máximo y en la práctica no sea posible ejercerlo. Un ejemplo de este tipo de situaciones la encontramos en el artículo 22 del Reglamento 2020/1503 (2020) y el **derecho de desistimiento** regulado en la experiencia española con el Texto Refundido de Ley General para la Defensa de los Consumidores y Usuarios, Real Decreto Legislativo 1/2007, de 16 de noviembre (2007)[55].

C. Implementación de servicios de alertas y de ejecución de órdenes automatizado

El **servicio de alertas** es una facilidad que viene utilizándose en la experiencia comparada, el cual tiene por objeto que las plataformas comuniquen a los inversores los proyectos que cumplen las características previamente informadas (por ejemplo, proyectos en determinada industria, bajo la modalidad *crowdlending*, con una determinada tasa de interés y con colaterales líquidos).

Como puede advertirse, no se trata de un servicio de asesoría financiera, pues la plataforma se limita a emitir alertas en función de las preferencias de los inversores. Tampoco puede configurar como un servicio de ejecución de órdenes, pues se trata de avisos y no un compromiso de inversión. De hecho, el servicio de alerta debería ser remunerado. Actualmente, el DU no regula expresamente este servicio, por lo cual se encuentra en el campo de la SMV, quien lo ha incorporado en el numeral 2 del artículo 25 del Reglamento como un servicio obligatorio[56].

Respecto del **servicio de ejecución automatizada de órdenes**, el DU tampoco hace mención expresa, aunque el proyecto de reglamento lo planteó como una actividad prohibida (Resolución de Superintendente 012-2020-SMV/01, 2020, art. 36.6).

[55] Por medio de este derecho el consumidor puede desistir en el plazo de catorce días desde la celebración del contrato de prestación de servicios, o desde la recepción de los bienes, sin justificación, ni penalización alguna.

[56] El texto del artículo establece lo siguiente

> Artículo 25.- Servicios adicionales
>
> […]
>
> 25.2 Ofrecer herramientas, aplicaciones u otras utilidades que permitan al Inversionista preseleccionar, sobre la base de criterios objetivos, entre los Proyectos publicados, aquellos en los cuales invertir, antes de realizar su instrucción de inversión (Resolución de Superintendente 045-2021-SMV/02, 2021).

Cabe indicar que, si bien el Reglamento no hace una referencia expresa a esta prohibición, el artículo 35 sí proscribe que las sociedades administradoras presten asesoramiento financiero, realicen recomendaciones de inversión o destaquen en la plataforma ciertos proyectos en detrimento de otros (con excepción del listado por ordenamiento de fecha, monto, sector u otro parámetro objetivo, lo que está referido al supuesto descrito en el párrafo anterior) (Resolución de Superintendente 045-2021-SMV/02, 2021).

Sobre el particular, en la matriz de comentarios al proyecto de reglamento, la SMV (2018) ha explicado que se ha otorgado posibilidad de desarrollar facilidades tecnológicas que posibiliten al inversionista preseleccionar entre los diversos proyectos que se publiquen en una plataforma y simplificar, de esta forma, el proceso de selección entre las diversas alternativas que se le presenten. Cabe subrayar que dicha facilidad implica la selección sobre la base de criterios establecidos por el inversionista, mas no la ejecución automática de la instrucción de inversión, la misma que debe ser realizada únicamente por el inversionista, lo cual además es consecuente con la exigencia de que este último conozca la identidad del receptor antes de realizar su instrucción de inversión. Es decir, la SMV ha considerado oportuno no permitir el servicio de ejecución de órdenes automatizado.

Como se sabe, este servicio puede ser prestado por los agentes intermediarios, de acuerdo a la Ley de Mercado de Valores (Decreto Legislativo 861, 1996); no obstante, la experiencia comparada viene demostrando lo provechoso de este mecanismo para agilizar la inversión. En la normativa española, este servicio solo se reserva para los inversores acreditados (con experiencia). En otros países como el Reino Unido e Israel también se ha previsto, mientras en otros (como México, Francia, Bélgica y Finlandia) no se ha prohibido (Havrylchyk, 2018). En el ámbito de la normativa comunitaria, se ha señalado que los modelos de negocio que utilicen procesos automatizados por los que el proveedor de servicios de financiación participativa asigne automáticamente fondos a un proyecto según los parámetros y los indicadores de riesgo predeterminados por el inversor, también llamados inversión automática, deben considerarse como gestión individualizada de carteras de préstamos y están permitidos[57].

En la práctica se ha logrado identificar que este servicio servía a los intereses de los inversionistas institucionales, quienes aprovechando su posición de negociación, acaparaban la mayor cantidad de proyectos más atractivos. Si bien es cierto que esta situación venía impactando a los intereses de los inversionistas no institucionales, quienes no tenían la oportunidad de participar en este tipo de proyectos, este tipo de situaciones pueden ser bien gestionadas por el administrador de las plataformas (Jiménez Alemán, 2021) a fin de 'equilibrar' las posiciones, por ejemplo, reservando un porcentaje de participación en este tipo de proyectos para los inversionistas no acreditados que han manifestado su interés previo a las plataformas[58]. La dirección de la regulación peruana es la misma, pues se pretende la pluralidad de inversionistas, con lo cual se encuentra en la esfera de las sociedades administradoras cumplir con este objetivo con sus mejores esfuerzos.

VI. CONCLUSIONES

Debido al impacto económico provocado por el COVID-19, el financiamiento es una pieza clave de la recuperación económica, por lo cual es importante analizar algunos ajustes que puedan facilitar y potenciar el crecimiento del FPF. Como hemos advertido, el *crowdfunding* es una industria cuyo principal atractivo es la interacción entre promotores e inversores a través de una plataforma; no obstante, está sujeto a fallos de mercado que deben ser monitoreados y, en su oportunidad, corregidos para su adecuado funcionamiento. Este es el caso de la falta de transparencia que genera dos fallas de mercado muy conocidas: selección adversa y el riesgo moral. En ambos casos, tal como se ha desarrollado, la solución es fortalecer la transparencia, aunque existen otras herramientas para alinear los intereses de las partes involucradas como es la inversión obligatoria del intermediario o del mismo promotor en el proyecto, a fin de incentivar un verdadero compromiso y diligencia.

En el plano del DU, se han detectado interesantes aciertos como es la inclusión de los proyectos personales, permitiendo su uso (aunque limitado) en el ámbito de créditos hipotecarios y vehiculares, a fin de brindar liquidez a profesionales independientes en proyectos personales. No obstante, se observan algunos aspectos que deben ser analizados por la autoridad competente, que en su mayoría deben ser precisados a nivel reglamentario o

[57] Véase los artículos 2, inciso 1.g) y 3, numeral 4 del Reglamento 2020/1503 (2020).

[58] Consideramos que no sería proporcional extender esta prerrogativa a los inversores no acreditados que no hayan manifestado su interés por determinado tipo de inversión, pues este tipo de comunicaciones o mecanismos de inversión automatizado son servicios remunerados que deben aportar una ventaja para sus comitentes.

incluso desarrollados por las propias plataformas. En primer lugar, nos referimos al ámbito de aplicación de la norma. Debería analizarse la pertinencia de fijar el ámbito de aplicación de la norma en función de los inversores nacionales, pues la principal justificación de la regulación a este nivel es la asimetría informativa generada en una relación de promotor e inversor.

Asimismo, también es necesario precisar el alcance de la responsabilidad de las sociedades administradoras de las plataformas respecto de las obligaciones de transparencia establecidas en la normativa vigente. Una interpretación literal nos conduciría a que –incluso– puedan ser responsables por la completitud, pertinencia e integridad de la información suministrada, lo cual no sería admisible. Distinto sería el escenario en que la sociedad administradora publique proyectos, cuya información no cumple los requerimientos mínimos exigidos por la SMV.

Sobre la imparcialidad, podemos concluir que no se trata de una característica inherente a la mediación, por ende, no puede exigirse este comportamiento *per se* a las plataformas FPF, más aún cuando naturalmente se inclinan a obtener rendimientos por la obtención de las metas de financiamiento por parte de los beneficiarios. Esto es reforzado por la multifuncionalidad de las plataformas que naturalmente inclina los intereses de la sociedad administradora hacia uno de sus clientes, lo cual desdibuja el esquema de intermediario imparcial. En ese sentido, lo que corresponde es descartar una conducta estrictamente 'imparcial' o 'neutral', correspondiendo más bien la gestión de los conflictos con la implementación de medidas razonables aplicables para cada caso en concreto.

Bajo la misma premisa, la posibilidad de que la sociedad administradora actúe como inversor o promotor no debe ser descartada, pues la experiencia en otros países demuestra que esta función puede dinamizar el crecimiento de las plataformas FPF, y el conflicto de intereses generado puede ser gestionado a través de medidas que refuercen la transparencia, que limiten su participación, que generen compromiso (con fórmulas como el esquema *skin in the game*), o se habilite esta posibilidad previo permiso de la autoridad, o sea, utilizado para 'completar' la inversión del proyecto.

Sobre la prohibición de prestar el servicio de asesoramiento financiero a los inversionistas a través de recomendaciones personalizadas, se requiere una revisión, pues esta actividad no se encuentra sujeta a autorización previa en el Perú. Atendiendo a ello, sería aconsejable evaluar la pertinencia de preferir la gestión del conflicto de intereses generado versus la situación actual de prohibir la actividad a cargo de las sociedades administradoras y personas vinculadas.

Respecto de las buenas prácticas, debe potenciarse el uso de las centrales privadas de información crediticia, pues ofrece una herramienta de transparencia clave en la evaluación del riesgo crediticio de los beneficiarios, sumado a lo cual siempre puede complementarse con herramientas como el *big data.* Sobre la práctica de proteger al inversor en función de su experiencia y conocimientos, es recomendable evaluar esta alternativa implementada en algunos países como Bélgica, Francia o Israel. Finalmente, también es aconsejable que la SMV evalúe incluir en su catálogo de servicios facultativos, a fin de brindar mayor predictibilidad al mercado.

Como se ha visto, el régimen jurídico del FPF en el Perú contiene las principales características de la regulación en otros países, no obstante, es recomendable analizar algunos aspectos de cara a fortalecer la herramienta y dinamizar el mercado. La gestión de los conflictos de intereses es una carga que debe evaluarse, a fin de que el abanico de servicios que puedan prestar las sociedades administradoras pueda extenderse.

REFERENCIAS

Alonso Espinosa, F. (2018). Protección de la inversión a través de las plataformas de financiación participativa. En F. de la Vega García, & E. Lázaro Sánchez (dirs.), *Crowdfunding: cooperación colectiva al servicio de la financiación* (pp. 339-360). Aranzadi Thomson Reuters.

Álvarez Meza, W. (2018). Desafíos normativos de la intermediación de pagos en el Perú: Lecciones desde el contexto regulatorio europeo. En G. Alvarez de Hoyle (coord.), *Temas de Protección al Consumidor y Regulación Financiera* (pp. 276-297). Círculo de Derecho Administrativo.

Comisión Nacional del Mercado de Valores (2010). *Guía sobre la prestación del servicio de asesoramiento en materia de inversión*. https://www.cnmv.es/DocPortal/GUIAS_Perfil/GuiaAsesoramientoInversion.pdf

(2019). *Preguntas y Respuestas dirigidas a empresas FinTech sobre actividades y servicios que pueden tener relación con la CNMV*. http://www.cnmv.es/docportal/Legislacion/FAQ/QAsFinTech.pdf

Cox, J., Hillman, R., Langevoort, D., Lipton, A., & Sjostrom, W. (1991). *Securities Regulation:*

Cases and Materials. Wolters Kluwer Law & Business.

Cuena Casas, M. (2019). Fintech y crédito responsable: Big Data y credit scoring. En F. Zunzunegui (dir.), *Regulación Financiera y Fintech* (cap. 4). Thomson Reuters Aranzadi.

(2019). *Las fintech de préstamos o crowdlending - La contratación a través de plataformas intermediarias en línea*. Reus editorial.

Delgado, J., & Pérez Asenjo, E. (2009). Antitrust y Tarjetas de Pago: En busca de la Tasa de Intercambio Óptima. *Perspectivas del Sistema Financiero,* (97), 49-58.

Galacho Abolafio, A. (2017). Crowdfunding y shadow banking: plataformas de financiación participativa (PFPS) y la protección de los inversores. *Revista de Derecho Bancario y Bursátil, 36*(145), 173-203.

Gállego Lanau, M. (2020). Los remedios ante el incumplimiento de las obligaciones de transparencia en las plataformas de financiación participativa. En M. Alonso Pérez & E. Hernández Sáinz (dirs.), *Servicios digitales, condiciones generales y transparencia* (pp. 195-226). Aranzadi Thomson Reuters.

Gázquez Serrano, L. (2007). *El contrato de mediación o corretaje.* La Ley.

Gilson, R., & Kraakman, R. (1984). The Mechanism of Market Efficiency. *Virginia Law Review Association,* (70), 549- 644.

Havrylchyk, O. (2018). *Regulatory framework for the loan-based crowdfunding platforms* (Working Paper 1513). https://doi.org/10.1787/24ad924a-en

Jiménez Alemán, J. (2021). Análisis de los conflictos de intereses en la financiación participativa: alertas y propuestas en un nuevo escenario de interacción financiera. *Revista de Derecho del Sistema Financiero: mercados, operadores y contratos,* (1), 223-274.

Kirby, E., & Worner, S. (2014). *Crowd-funding: An Infant Industry Growing Fast* (IOSCO Research Department Working Paper SWP3/2014). https://www.iosco.org/research/pdf/swp/Crowd-funding-An-Infant-Industry-Growing-Fast.pdf

Lázaro Sánchez, E. (2018). Crowdfunding: una fórmula de cooperación económica en la era digital. En F. de la Vega García, & E. Lázaro Sánchez (dirs.), *Crowdfunding: cooperación colectiva al servicio de la financiación* (pp. 19-46). Aranzadi Thomson Reuters.

López Ortega, R. (2016). Las plataformas de financiación participativa (*crowdfunding*) en la Ley 5/2015, de 27 de abril, de fomento de la financiación. *Revista de Derecho Bancario y Bursátil, 35*(144), 83-106.

Macanás Vicente, G. (2018). Calificación y caracteres del contrato de mediación con la plataforma de *crowdfunding*. En F. de la Vega García, & E. Lázaro Sánchez (dirs.), *Crowdfunding: cooperación colectiva al servicio de la financiación* (pp. 73-103). Aranzadi Thomson Reuters.

Moreno Serrano, E. (2016). Configuración jurídica del "*crowdfunding*" como forma alternativa de financiación. En L. González-Serrano, & E. Moreno Serrano (coords.), *Crowdfunding: aspectos legales* (cap. 1). Aranzadi Thomson Reuters.

Otiniano Campos, G., & Salas Vigo, M. (10 de julio de 2017). *¿Regular o no regular? El reto que trae el servicio de asesoría financiera* [ponencia]. 21º Conferencia Anual de la Asociación Latinoamericana e Ibérica de Derecho y Economía (ALACDE).

Rivadeneyra Sánchez, J, (1994). La mediación contractual: contrato de corretaje. En L. Pizarro Aranguren (coord.), *El Derecho Civil peruano: perspectivas y problemas actuales* (pp. 238-263). Fondo Editorial de la Pontificia Universidad Católica del Perú.

Rodríguez de las Heras Ballell, T. (2016). La responsabilidad de las plataformas: alcance, límites y estrategias. En L. González-Serrano, & E. Moreno Serrano (coords.), *Crowdfunding: aspectos legales* (cap. 15). Aranzadi Thomson Reuters.

Rodríguez Martínez, I. (2018). El servicio de mediación electrónica de las plataformas de financiación participativa: marco regulador. *Revista de Derecho Bancario y Bursátil, 37*(149), 219-254.

Sánchez Ruiz, M. (2019). Deberes legales y conflictos de intereses de las plataformas de financiación participativa. *Revista de Derecho Bancario y Bursátil, 38*(153), 11-40.

Strausz, R. (2017). A Theory of Crowdfunding: A Mechanism Design Approach with Demand Uncertainty and Moral Hazard. *American Economic Review, 107*(6), 1430-1476. https://doi.org/10.1257/aer.20151700

Superintendencia de Mercado de Valores [SMV] (2018). *Matriz de comentarios recibidos al Proyecto de Reglamento de la actividad de financiamiento participativo financiero y sus sociedades administradoras*. https://www.smv.gob.pe/Uploads/Matriz_comentarios_Reg_FPF.pdf

Vaisman-Araujo, S. (2018). *Plataformas digitales que facilitan transacciones de consumo: delimitación de responsabilidades de los proveedores frente a los usuarios finales en el marco del Derecho de Protección al Consumidor* (tesis de licenciatura en Derecho). Universidad de Piura, Lima, Perú.

Vieira Dos Santos, J. (2017). Portuguese Crowdfunding Act. *Revista de Derecho Bancario y Bursátil, 36*(147), 227-252.

Zunzunegui, F. (2015). *Régimen jurídico de las plataformas de financiación participativa (Crowdfunding- Spanish Crowdfunding Act)* (Working Paper 3/2015). http://dx.doi.org/10.2139/ssrn.2628249

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Circular 003-2020-BCRP, Banco Central de la Reserva del Perú, 31 de enero de 2020 (Perú).

Decreto de Urgencia 013-2020, Decreto de Urgencia que promueve el financiamiento de la MIPYME, emprendimientos y Startups, Diario Oficial *El Peruano*, 22 de enero de 2020 (Perú).

Decreto Legislativo 861, Ley de Mercado de Valores, Diario Oficial El Peruano, 22 de octubre de 1996 (Perú).

Directiva 2007/64 del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE, 2007 O.J. (L 319) 1.

Directiva 2014/65 del Parlamento Europeo y del Consejo, de 15 de mayo de 2014, relativa a los mercados de instrumentos financieros y por la que se modifican la Directiva 2002/92/CE y la Directiva 2011/61/UE, 2014 O.J. (L 173) 349.

Ley para Regular las Instituciones de Tecnología Financiera, *Diario Oficial de la Federación,* 9 de marzo de 2018 (Méx.).

Ley 5/2015, Ley de fomento de la financiación empresarial (B.O.E. 2015, 5) (Esp.).

Ley 26702, Ley General del Sistema Financiero y Sistema de Seguros, Diario Oficial *El Peruano,* 13 de julio de 2017.

Real Decreto 217/2008, sobre el régimen jurídico de las empresas de servicios de inversión y de las demás entidades que prestan servicios de inversión y por el que se modifica parcialmente el Reglamento de la Ley 35/2003, de 4 de noviembre, de Instituciones de Inversión Colectiva, aprobado por el Real Decreto 1309/2005, de 4 de noviembre (B.O.E. 2008, 217) (Esp.).

Real Decreto Legislativo 1/2007, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (B.O.E. 2007, 1) (Esp.).

Real Decreto Legislativo 4/2015, por el que se aprueba el texto refundido de la Ley del Mercado de Valores (B.O.E. 2015, 4) (Esp.).

Reglamento 2020/1503, de 7 de octubre de 2020, relativo a los proveedores europeos de servicios de financiación participativa para empresas, y por el que se modifican el Reglamento (UE) 2017/1129 y la Directiva (UE) 2019/1937, 2020 O.J. (L 347) 1 (UE).

Resolución de Superintendencia 00034-2015, Reglamento de Agentes de Intermediación, Superintendencia del Mercado de Valores, 19 de diciembre de 2015 (Perú).

Resolución de Superintendente 012-2020-SMV/01, que autoriza la difusión del Proyecto de "Reglamento de la Actividad de Financiamiento Participativo Financiero y sus Sociedades Administradoras", Diario Oficial *El Peruano,* 26 de noviembre de 2020 (Perú).

Resolución de Superintendente 045-2021-SMV/02, que aprueba el Reglamento de la actividad de financiamiento participativo financiero y sus sociedades administradoras, Diario Oficial *El Peruano,* 19 de mayo de 2021 (Perú).

S.T.S., 7 de febrero de 2007, (No. 63/2007) (Esp.).

10.18800/themis.202101.015

INTELIGENCIA ARTIFICIAL Y VALORACIÓN DE LA PRUEBA: LAS GARANTÍAS JURÍDICO-CONSTITUCIONALES DEL ÓRGANO DE CONTROL

ARTIFICIAL INTELLIGENCE AND THE ASSESSMENT OF EVIDENCE: THE LEGAL-CONSTITUTIONAL GUARANTEES OF THE SUPERVISING BODY

Pere Simón Castellano*
Universidad Internacional de la Rioja (UNIR)

Judicial proceedings and trials will be digital or they will not be. Overcoming the debate about the convenience of embracing the technological advance does not imply accepting integrated positions de facto*. The COVID-19 pandemic has further highlighted the troubles and deficits of Spanish judicial proceedings. A slow justice, paralyzed due to remote work and without resources or guarantees to hold trials at a distance, is not justice. Excuses are running out today faster than ever, since new levels of effectiveness, efficiency, and speed, with full respect of procedural guarantees, can be reached with the use of most modern new technologies.*

This article explores the possibilities of using artificial intelligence systems in a specific area: the assessment of evidence. In this context, the hypothesis that the article aims to demonstrate is that although the human presence will continue to be necessary in judicial proceedings, artificial intelligence systems could support the free assessment of evidence by the judge and cover those gaps where the human mind shows its most erratic side, such as during corroborations.

Keywords: Artificial Intelligence; criminal proceedings; free assessment of evidence; Spain.

El proceso judicial será tecnológico o no será. Superar el debate acerca de la conveniencia de abrazar el avance tecnológico no implica aceptar de facto posiciones integradas. La pandemia del COVID-19 ha acentuado aún más –si cabe– las miserias y disonancias del proceso judicial en España. Una justicia lenta, paralizada ante la necesidad de teletrabajar y sin recursos con garantías para celebrar juicios a distancia, no es justicia, y hoy se agotan más rápido que nunca las excusas, puesto que nuevas cuotas de eficacia, eficiencia y celeridad, con pleno respeto a las garantías procesales, pueden alcanzarse con el empleo de las más modernas y nuevas tecnologías.

El presente trabajo pretende explorar las posibilidades de empleo de los sistemas de inteligencia artificial en un ámbito muy concreto: el de la valoración de la prueba. En este contexto, la hipótesis que el artículo pretende demostrar es que la presencia humana seguirá siendo necesaria, si bien los sistemas de inteligencia artificial podrían apoyar y asistir la libre valoración de la prueba por parte del juzgador y colmar aquellas lagunas donde el ser humano muestra su faceta más errática; por ejemplo, en las corroboraciones.

Palabras clave: Inteligencia artificial; proceso penal; libre valoración de la prueba; España.

* Abogado. Doctor en Derecho por la Universitat de Girona. Exsocio fundador de Pridatect. Profesor contratado doctor en Derecho Constitucional en la Universidad Internacional de la Rioja (UNIR) (Logroño, España). Profesor de Derecho Penal Económico, Propiedad Industrial y Nuevas Tecnologías, Protección de Datos y Ciberdelincuencia en Universidad Internacional de La Rioja. Abogado independiente. Abogado en Font Advocats (Barcelona, España). Contacto: pere.simon@unir.net

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 27 de diciembre de 2020, y aceptado por el mismo el 8 de abril de 2021.

I. INTRODUCCIÓN: DE LOS USOS POSIBLES DE LA INTELIGENCIA ARTIFICIAL EN LAS ADMINISTRACIONES PÚBLICAS Y EN EL SENO DEL PROCESO JUDICIAL

Internet lo ha revolucionado todo. La forma cómo nos comunicamos y relacionamos, la inmediatez en el acceso, la velocidad del mensaje y la importancia que le damos a la información que nuestras 'amistades' nos trasladan. En un mundo inundado de información irrelevante (Harari, 2018, p. 11), cada vez resulta más fácil descontextualizar lo que leemos y compartimos (Dumortier, 2009), subsumidos en una arquitectura en red, sin jerarquía, que pone en tela de juicio la aplicación de criterios y principios que tradicionalmente han permitido a los operadores jurídicos dar respuesta a aquellos casos difíciles en los que colisionan distintos bienes jurídico-constitucionales que bien merecen tutela (Simón Castellano, 2012; Cabellos Espiérrez, 2018).

En este complejo escenario de cambio constante al que nos aboca la postmodernidad líquida, surge con fuerza una nueva técnica que es capaz de predecir conductas humanas e, incluso, conocer mejor que el propio individuo cuáles son sus preferencias y necesidades, y, por ende, saber cuáles son las opciones o decisiones que más le conviene tomar. Nos referimos a los sistemas de inteligencia artificial (en adelante, IA), esto es, sistemas expertos que piensan y actúan como humanos, o bien piensan y actúan siguiendo la lógica racional. Sobre este particular, hemos analizado con mayor detenimiento los efectos de la IA en el seno de la administración de justicia en otro foro (Simón Castellano, 2021a).

Más allá de la precisión terminológica de lo que puede o debe entenderse por un sistema experto de inteligencia artificial, cuyo objeto de debate complicaría de sobremanera no exceder la extensión de este trabajo, resulta necesario constatar, de un lado, (i) los cimientos en los que se basa la estructura de esta moderna técnica y, del otro, (ii) los campos y realidades tangibles en los que ya se puede apreciar un uso notable de algoritmos basados en el aprendizaje autónomo.

En relación con la primera de las categorías, el punto de partida para que podamos hablar de inteligencia artificial se encuentra en las técnicas que permiten el procesamiento masivo de datos, con independencia de si los podemos clasificar *stricto sensu* como datos personales. Sin tratamiento de datos ni sistema de procesamiento masivo, no existen sistemas inteligentes o, lo que es lo mismo, nadie puede proponer ni emular la actuación humana si opera en el vacío. Requiere, entonces, de información y datos –cuantos más mejor– puesto que un mayor conocimiento y procesamiento permitirá obtener resultados más próximos a lo que el usuario realmente requiere o necesita, laminando y reduciendo así las posibilidades de que se produzcan sesgos por la poca calidad de la información o por la pobreza de los datos facilitados. El uso de algoritmos que disponen reglas lógicas para establecer una respuesta que emule, como decíamos anteriormente, la forma de pensar y actuar de los humanos (Mayer-Schönberger & Cukier, 2013, p. 13) necesariamente encuentra su *prius* formal y material en el procesamiento ingente de datos, personales o no.

Además, un matiz conceptual importante gira en torno a los llamados algoritmos avanzados que permiten el aprendizaje automático, más conocidos como sistemas de *machine learning*. Estos tienen un mayor potencial de impacto y una mayor fiabilidad, por la capacidad de aprender de los datos y de la experiencia. La principal arista del empleo por parte de los poderes públicos de este tipo de sistemas de aprendizaje profundo es la falta de transparencia (Cerrillo i Martínez, 2019) en un algoritmo que muta o se transforma, que se modifica y perfecciona, de forma autónoma, sin que el usuario sea capaz de descubrir de forma sencilla las razones por las que este ha adoptado o propuesto una decisión o resultado.

Por lo que se refiere a los usos tangibles de la inteligencia artificial, cabe señalar que, actualmente, los sistemas de inteligencia artificial son empleados en los ámbitos del procesamiento del lenguaje natural, la visión computarizada y la robótica, para fines muy diversos (Kaplan, 2017, p. 53). Los algoritmos están muy presentes en nuestra realidad cotidiana. Especialmente han sido empleados con notable fortuna, aunque también con una fiabilidad a vueltas bastante pobre en procesos de *marketing online* y publicidad comportamental, y condicionan con creces las decisiones que se toman, por ejemplo, en el ámbito del consumo de productos y servicios en línea. Para algunos autores, somos ya esclavos de la tiranía de los algoritmos (Edwards & Veale, 2017, pp. 19-20).

Una tiranía, en cierto modo, cada vez más tangible, puesto que el empleo de la inteligencia artificial está en claro auge (Cerrillo i Martínez & Peguera Poch, 2020) o, como algunos autores afirman, "está de moda" (De Asís Roig, 2018, p. 28). Un corolario que no resulta difícil de alcanzar si tenemos en cuenta la atención creciente que los mercados le están prestando, así como con los informes de prestigiosas firmas que le auguran un crecimiento imparable a lo largo de la próxima década (Eggers *et al.*, 2018, p. 3). Se manifiesta que la IA trans-

formará definitivamente la forma en la que vivimos, y proyectará sus efectos sobre las relaciones del trabajo y la producción automatizando tareas manuales o rutinarias, en el marco de una nueva, llamada cuarta, revolución industrial que vendrá acompañada de un nuevo paradigma en el que el aprendizaje constante y la especialización no serán una opción (Frey & Osborne, 2017, p. 38).

Sin embargo, más allá de su crecimiento imparable, ¿qué fines plausibles pueden tener los sistemas de inteligencia artificial en las administraciones públicas, en general, y en la administración de justicia, en particular? ¿Qué transformaciones puede proyectar sobre las estructuras de instituciones tan sensibles como los principios y garantías del proceso judicial?

Ya disponemos, en la actualidad, de numerosos ejemplos del empleo de sistemas autónomos de inteligencia artificial en las administraciones públicas: Atlanta predice el riesgo de incendio de los edificios; Hampton, el riesgo de riadas; y Chicago y Las Vegas identifican los locales que serán objeto de inspección, entre muchos otros (De Souza, 2018). Otras administraciones han empezado a utilizar esta moderna técnica para detectar fraudes a la seguridad social; para alertar del conflicto de intereses y evitar la corrupción en los procesos de licitación y contratación pública; con el fin de asistir a médicos para el tratamiento de enfermedades; para asignar subvenciones o evaluar profesores; para detectar el abandono escolar, estableciendo alertas automáticas basadas en el comportamiento de empleados públicos, etc.

Como reacción, la doctrina ha estudiado con profundidad tal posibilidad (Martínez Martínez, 2019; Valero Torrijos, 2019; Cotino Hueso, 2019; Boix Palop, 2020), si bien con carácter general para todas las administraciones públicas y desde el prisma de los efectos y retos jurídicos que plantea la inteligencia artificial.

El legislador, por su parte, a vueltas se ha posicionado abrazando tal posibilidad, incluso con demasiada premura y sin suficientes cautelas. Es el caso de la Ley 22/2018, de 6 de noviembre de 2018, de la Generalitat Valencia, que prevé un sistema de alertas tempranas anticorrupción (en adelante, SATAN) basado en los criterios de Falciani, respecto del que no tenemos constancia alguna de que se esté utilizando. La Agencia Española de Protección de Datos (en adelante, AEPD), en el Informe 385661/2017 (2018), y la doctrina (Cotino Hueso, 2020) han valorado de forma crítica la citada ley, pues consideran que restringe de forma inadmisible los derechos al no cumplir los requisitos constitucionales respecto a sus límites ni los establecidos en el artículo 23 del Reglamento General de Protección de Datos de la Unión Europea (en adelante, RGPD). La celeridad de la respuesta del legislador no siempre va acompañada de la necesaria calidad, y, por ello, también disponemos de la primera resolución judicial que ha declarado ilegal un algoritmo sobre evaluación de características personales de los ciudadanos. Nos referimos a la Sentencia de 5 de febrero de 2020 del Tribunal de Distrito de la Haya, asunto C/09/550982/HA ZA 18-388 (*NJCM et al./Países Bajos*, 2020; Fernández Hernández, 2020c; Cotino Hueso, 2020).

Frente a la asimetría y teniendo en cuenta las primeras experiencias contradictorias, el legislador europeo parece decidido a aportar cierta seguridad jurídica al respecto. El 20 de octubre de 2020, el Pleno del Parlamento Europeo aprobó su propuesta de regulación de la inteligencia artificial, cuya principal finalidad es impulsar la innovación a partir de normas éticas que promuevan la confianza en la tecnología[1].

La propuesta, que nace del Parlamento Europeo y tiene como destinatario a la Comisión Europea, se refiere a tres áreas básicas: las normas éticas que deben regir la inteligencia artificial, las reglas sobre la responsabilidad por las consecuencias derivadas de su uso y, finalmente, las reglas sobre derechos de propiedad intelectual vinculadas al uso de los sistemas inteligentes. Tal regulación, esperada en forma de reglamento, persigue garantizar cierta uniformidad de las futuras normas que se elaboren sobre esta materia en el marco de la Unión Europea, al establecer principios rectores que exigen que la IA se desarrolle desde un enfoque antropocéntrico, es decir, centrada y hecha por el ser humano. También, se busca que se garantice la seguridad, transparencia y responsabilidad derivada de su uso, así como la disponibilidad de salvaguardias contra la parcialidad y la hipotética o eventual discriminación del algoritmo. Asimismo, que incorpore el derecho a la reparación en caso de que se produzcan daños ilegítimos y exige la responsabilidad social, ambiental y el respeto de la privacidad y la protección de datos. Sea como fuere, se trata de un proyecto en tramitación y habrá que estar atentos a su recepción por parte de la Comisión Europea y su futura aprobación.

[1] Véase la Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)).

Por lo que aquí interesa, y retomando el camino trazado, corresponde analizar los usos de la IA en el seno del proceso judicial y en la administración de justicia, lo que puede tener mucha lógica y sentido, por ejemplo, para la propia gestión del seguimiento de archivos, con indiferencia de la naturaleza del proceso o del orden jurisdiccional (Simón Castellano, 2021a). La creación de alertas tempranas por parte del algoritmo en función de la inmensa cantidad de datos procesados y la experiencia previa que este haya acumulado puede contribuir a simplificar su gestión y aumentar la eficiencia (European Commision For The Efficiency Of Justice [CEPEJ], 2018, p. 63). Además, los discursos en torno a la digitalización y modernización de la justicia mediante sistemas de IA van mucho más allá de la eliminación del papel, cuya importancia radica en que la información ahora está digitalizada y es 'tratable', con un potencial enorme para fines muy diversos, desde la estadística hasta la gestión, aunque todo redunde en la agilización de la justicia y la automatización de buena parte de la labor judicial (Ercilla García, 2020).

Siguiendo en el plano general, las técnicas de IA pueden mejorar el acceso a la jurisprudencia sobre la base del aprendizaje automático, y son un activo considerable para complementar búsquedas o vincular varias fuentes legales y jurisprudenciales, incluso mediante técnicas de visualización de datos (CEPEJ, 2018, p. 63). También la inteligencia artificial puede contribuir a fortalecer la relación entre la justicia y los ciudadanos, haciendo a la primera más transparente gracias a los *chatbots,* que pueden configurarse para facilitar el acceso a las diversas fuentes de información existentes utilizando lenguaje natural, compartiendo información (plantillas de documentos, solicitudes o modelos contractuales básicos) o incluso generándola en línea (CEPEJ, 2018, p. 63).

La inteligencia artificial, en la jurisdicción civil y social, debería tener mucho recorrido en la llamada resolución extrajudicial de conflictos y controversias, ámbito en el que el empleo de sistemas expertos solo puede redundar en beneficios para todas las partes, así como en el ámbito del llamado *Online Dispute Resolution* (en adelante, ODR). Sirva como ejemplo el uso de técnicas de justicia predictiva por parte de las compañías aseguradoras, que calculan y evalúan las posibilidades de éxito de acudir a los tribunales y, en el caso que este resulte inferior a un determinado porcentaje, prefieren acudir a sistemas de resolución extrajudicial de conflictos, evitando los costes del proceso judicial.

Otros usos, inclusive más cuestionables, de la inteligencia artificial son los relativos al perfilado de jueces y magistrados, y los destinados a anticipar, en sentido literal, el sentido de las resoluciones judiciales. Cuantificar y analizar exhaustivamente la actividad de un juez contribuiría a disponer de unos resultados que, en el mejor de los casos, podría considerarse un asesoramiento cuantitativo y cualitativo para los propios jueces, con fines puramente informativos y de asistencia en la toma de decisiones (CEPEJ, 2018, p. 66). Así, el análisis por parte de sistemas expertos de la predictibilidad y previsibilidad de las decisiones judiciales estaría orientado exclusivamente a reducir el margen de discrecionalidad de los jueces, considerado en ocasiones excesivo (Fernández Hernández, 2020b). Estas herramientas, empero, podrían estar abiertas al abuso si se emplean no solo para gestionar los asuntos judiciales de manera más eficiente, sino también para evaluar el grado de desempeño de los jueces, incluido el análisis de supuestos sesgos ideológicos en sus patrones de comportamiento.

Los esfuerzos en el ámbito de la jurisdicción penal se pueden englobar, básicamente, en los fines relacionados con la actividad predictiva –o *predictive policing*– y en el llamado 'reconocimiento facial' (González Fuster, 2020). En cuanto a la actividad predictiva, destacamos la posibilidad de apoyarnos en el avance tecnológico con el fin de revelar patrones de una probable comisión de actos delictivos o a la identificación de posibles víctimas de futuros delitos, permitiendo su interceptación antes de que ocurran al más puro estilo que mostró al mundo el paradigma cinematográfico de Minority Report. La predicción del crimen es una tendencia imparable cuya *vis* expansiva ha marcado notablemente los avances en materia de seguridad a nivel mundial y en Europa desde los atentados del 11 septiembre de 2001 (Souza de Menezes & Agustina, 2020), con todos los problemas asociados a la calidad de la predicción, que necesariamente debe estar basada en una base de datos suficiente, en términos cuantitativos y cualitativos (Richardson *et al.*, 2019).

El uso de estos instrumentos de predicción por parte de los jueces de la jurisdicción penal en Europa es muy escaso (González Fuster, 2020); no obstante, ya disponemos de resultados de experiencias significativas en modelos en perspectiva comparada, más concretamente, en Estados Unidos y Reino Unido. Me refiero a los programas Correctional Offender Management Profiling for Alternative Sanctions (en adelante, COMPAS) y el Harm Assessment Risk Tool (en adelante, HART), que calculan el riesgo de reincidencia de una persona que ha sido anteriormente condenada.

Lo cierto es que las principales conclusiones o propuestas formuladas por los citados algoritmos mostraron un preocupante sesgo; por ejemplo, en

el caso de COMPAS, se demostró la existencia de un sesgo racial indirecto en los modelos que predicen el riesgo de reincidencia mediante el uso de variables sustitutivas que no son neutrales. Aunque no es pacífico, estudios afirman que, aplicando el citado algoritmo, los acusados negros tenían casi el doble de probabilidades, en relación con los blancos, de ser considerados en situación de alto riesgo de reiteración delictiva (Babuta *et al.*, 2018, p. 7). Los proyectos COMPAS y HART han sido objeto de duras críticas por las organizaciones no gubernamentales ProPublica y Big Brother Watch, las que subrayan los problemas que se proyectan por aplicar un enfoque discriminatorio o determinista en el diseño del algoritmo.

En cuanto a las tecnologías de reconocimiento facial, estas son objeto de notable controversia y limitaciones por lo que se refiere a su utilización, especialmente por parte empresas privadas. Lo cierto es que se han implementado, hasta la fecha, muchas iniciativas de reconocimiento facial en países como China, Rusia, Estados Unidos, Suecia, entre otros, tanto por parte de autoridades como por parte de empresas privadas (González Fuster, 2020, pp. 24-25). La idea es prevenir el delito o dar cumplimiento a prohibiciones emitidas por sujetos de derecho público o privado, mediante la identificación con reconocimiento facial del infractor. Ciertas iniciativas han obtenido un beneplácito expreso por parte de las autoridades nacionales de protección de datos, como es el caso de la autoridad de protección de datos danesa, que autorizó el empleo de sistemas de reconocimiento facial por parte de un club de fútbol para evitar la entrada en el estadio de personas que tenían el acceso prohibido (IT-Pol, 2019).

Por su parte, los sistemas de Inteligencia Artificial Judicial de Valoración de Riesgo (en adelante, IAJVR), siguiendo la terminología propuesta por Miró Llinares (2018, p. 107), son otra opción con una funcionalidad muy distinta a las anteriores, la mayoría apoyados hoy en día en sistemas expertos *Human in Command*, no basados en una *black box* o en procesos de aprendizaje autónomo o *deep learning*. Los sistemas que emplean la IAJVR están basados en la automatización de las herramientas actuariales de valoración del riesgo y son aplicables a los procesos de toma de decisiones que requieren conjurar el riesgo, por ejemplo, en la aplicación de medidas cautelares o, tras la condena, en el ámbito penitenciario y en la ejecución penal. Se trata de un concepto clave que hemos tenido la ocasión de estudiar en profundidad, por lo que se refiere a potenciales usos, ventajas e inconvenientes, así como límites, en relación con la medida cautelar más polémica, la prisión provisional, en otro foro (Simón Castellano, 2021b).

En resumen, y en términos generales, la inteligencia artificial se utiliza o se está estudiando para utilizarla en los sistemas jurídicos europeos con diversos fines, entre los que destacan los de facilitar el acceso a la justicia (por ejemplo, mediante los *chatbots*), apoyar medidas alternativas de solución de conflictos en el ámbito civil, para el perfilado de jueces (Council Of Bars And Law Societies Of Europe [CCBE], 2020), para el análisis predictivo y prevención *ex ante* del delito y, finalmente, para el reconocimiento facial del infractor.

II. INTELIGENCIA ARTIFICIAL, VALORACIÓN DE LA PRUEBA Y ARGUMENTACIÓN PROBATORIA

Hemos analizado hasta este punto los usos y finalidades plausibles de los sistemas de inteligencia artificial, tanto en las administraciones públicas, en general, como en la administración de justicia, en particular. Intencionadamente, no mencionamos hasta el momento a la posibilidad de que los sistemas expertos puedan ser empleados *ad hoc* de la valoración de la prueba y la argumentación probatoria en sede judicial.

Constituye al respecto una obra de referencia obligada, el trabajo Inteligencia artificial y proceso judicial del Dr. Nieva Fenoll (2018), que anticipa de una forma muy acertada el impacto de los sistemas de IA en la valoración de la prueba. Lejos de establecer un sistema de automatismos nada respetuoso con la vigencia de nuestro modelo de libre valoración de prueba[2], por contraposición a otros modelos en perspectiva comparada como el de las *hearsay rules* de Estados Unidos, la IA podría, en cambio, contribuir a ofrecer resultados basados en datos bastante objetivables en función de los medios de prueba empleados (Nieva Fenoll, 2018). Todo ello, como decíamos, también en sistemas de libre valoración de ella, lo que ya de entrada implica una apreciación probatoria más compleja.

Todo proceso penal estructurado con base en una concepción racionalista de la prueba debe tener como objetivo darle al juez las herramientas

[2] Cuando hablamos de la libre valoración de la prueba nos referimos a la regla que permite al órgano judicial competente apreciar las pruebas existentes en el procedimiento según su libre convencimiento y sin tener que otorgarles a algunas de ellas un valor o credibilidad superior que venga predeterminada por la ley (Diccionario panhispánico del español jurídico, 2020). Esta es la definición que ofrece el Diccionario panhispánico del español jurídico en el que colaboran la Real Academia Española, la Cumbre Judicial Iberoamericana y la Asociación de Academias de la Lengua Española.

necesarias para que la valoración de la prueba dependa, en la medida de lo posible, de criterios objetivos y explicables (Ferrer Beltrán, 2002; Ferrer Beltrán, 2007), y no de instituciones generales cubiertas detrás del tantas veces incoherente 'telón' de la inmediación (Taruffo, 1992/2002; Nieva Fenoll, 2010). Es en este ámbito, y para este caso concreto particular, en el que debemos valorar la posibilidad real de que los sistemas de IA ofrezcan una oportunidad, también, para expulsar de las salas de justicia los atávicos heurísticos judiciales o, lo que es lo mismo, las emociones, gustos, prejuicios, preferencias, aficiones y otros elementos que no siempre resultan confesables y que están muy presentes en la valoración que realiza el juzgador.

A. ¿Cómo valoran las pruebas los jueces?

Solo si comprendemos como valoran las pruebas los jueces seremos capaces de articular una fórmula algorítmica que emule o replique su proceso lógico y psicológico de valoración probatoria. Los seres humanos somos automáticos, recurrentes, en una mayor medida de lo que podemos pensar, en nuestro día a día, en nuestro actuar cotidiano. Como señalan Kahneman y Sunstein, nos gusta repetir nuestras experiencias y ritos más ancestrales (en HarvardCPL, 2014). Los jueces también son personas y no podrían escapar a algo tan humano como la forma en la que se accede al conocimiento y cómo este, sumado a otros factores, influye decisivamente en las decisiones que luego tomamos. Los humanos somos automáticos y los jueces, por ende, también son mecánicos en la mayoría de las ocasiones.

Por si lo anterior fuera poco, además, los jueces no operan en el vacío. Ni pueden, ni deben hacerlo. Lo que sucede en el exterior nos condiciona, nos aflige y llega a afectar nuestra toma de decisiones. Es lo que Kahneman (en HarvardCPL, 2014) llama el efecto del contexto y enlaza con la afección y la emoción. O lo que fue, en su día, brillantemente expuesto por Chayes (1976), cuando nos advertía que el juzgador no puede actuar aislado del entorno social y las decisiones que este toma en los litigios de interés público son fruto de un diálogo natural, permanente e inevitable con otros elementos sociales y políticos –académicos, prensa, el Poder Ejecutivo, el legislador, agencias administrativas y el público en general–.

Los jueces también tienen ideología y se rigen por motivos ideológicos (Posner, 2011). Sería falaz no reconocerlo, aunque otra cosa bien distinta es que hayan recibido una formación que les permite tomar decisiones basadas en la ley y en la interpretación que un jurista puede hacer de esta. Esta formación profesional de jueces y magistrados actúa como límite interno a los atajos intuitivos más salvajes de nuestra psicología cognitiva. Señala Nieva Fenoll (2018, p. 44) que la carga de trabajo o la sobrecarga, mejor dicho, acostumbra a provocar un alejamiento de las realidades a juzgar y empeña al juzgador a dejarse llevar por su ideología.

Así las cosas, los jueces toman decisiones en el marco de un ejercicio cognitivo que vincula la experiencia –vital y profesional–, las emociones y el contexto, el diálogo con otros elementos políticos y sociales, la ideología base, los heurísticos de pensamiento descritos por Kahneman, Slovic y Tversky (1982), la memoria y estadística *prima facie* –es decir, aquello que recuerdan y que les viene a la cabeza de forma casi automática sobre casos anteriores–, la intuición (Myers, 2002, p. 16), la fatiga –mental y física– y la comodidad–placer, satisfacción e incluso el éxito pretérito en situaciones análogas–.

¿Podemos trasladar al algoritmo este proceso de valoración humana del juzgador, de los hechos, y hacerlo, además, expulsando o mitigando los atávicos heurísticos judiciales? En otro foro, y en relación con la adopción de la siempre polémica medida de prisión provisional, hemos defendido enérgicamente una respuesta afirmativa (Simón Castellano, 2021b). Veamos, empero, cómo podría extrapolarse o traducirse todo ello al ámbito de la valoración probatoria.

B. La valoración de la declaración de las personas

Las leyes procedimentales incorporan diferentes pruebas –testifical, declaración de las partes, etc.– que podrían englobarse dentro de una categoría superior, de declaración de las personas. ¿Qué podrían aportar los sistemas de IA en este contexto? Hoy en día, los jueces valoran la credibilidad de las personas de acuerdo con los factores situacionales y en función de su experiencia vital anterior. Sin embargo, la memoria humana es finita y limitada, así que carece de precisión matemática y los cálculos estadísticos humanos, fundamentados en metaanálisis, suelen acabar incurriendo en sesgos de confirmación, de comodidad y anclaje o de discriminación, entre otros. Las circunstancias que afectan a la credibilidad del testimonio de las personas son parcialmente objetivables (Nieva Fenoll, 2018, p. 81), lo que significa que estas podrían digitalizarse o traducirse en lenguaje de programación.

El problema pasa por el cómo, puesto que construir una herramienta que recoja todos los datos del caso concreto y que los combine adecuadamente para valorar la credibilidad de la declara-

ción no es una tarea fácil. Buena muestra de ello es el programa ADVOKATE, empleado para valorar la credibilidad de los testigos, que se basa en la distancia del observador, la visibilidad, el conocimiento previo entre el testigo y la persona observada, la competencia y conocimiento que se atribuye al testigo –edad, estudios, capacidad mental, etc.–, si se detectan errores en la descripción y contraste de la realidad, el tiempo de observación y el tiempo discurrido entre los hechos y la declaración (Bromby & Hall, 2002, pp. 143-152).

Como se observa, se trata de fórmulas que pueden proyectarse sobre un algoritmo, sobre bases estadísticas y sistemas de cálculo que objetivan la intuición humana y la perfeccionan, acercándonos más a la realidad de los hechos. Estas fórmulas deberían incluir, siguiendo a Nieva Fenoll (2018, p. 84 & ss) (i) la coherencia de la declaración; (ii) la contextualización o capacidad del interrogado de recuperar la descripción del escenario en el que sucedieron los hechos; (iii) la corroboración en otros medios de prueba de lo declarado; y (iv) la existencia o no de comentarios extra, oportunistas, que solo buscan reforzar retóricamente la declaración y que, a la postre, nos indican que el declarante puede tener algún fin metajurídico o voluntad de proyectar una realidad determinada al juzgador. En el proceso habría que descartar expresamente el estudio gestual (Ekman, 2011). De todos ellos, el parámetro de la corroboración es el que con mayor facilidad puede ser evaluado a través de la IA, puesto que el ser humano es incapaz de procesar a gran velocidad y chequear o comprobar la coincidencia o inexactitud de lo que se declara con las otras pruebas practicadas. Así las cosas, la IA sería de gran utilidad en las corroboraciones, en las que el ser humano se muestra más débil por las dificultades inherentes de su procesamiento.

Nieva Fenoll (2018, pp. 88-89) señala también como fin potencial de la IA el que esta pueda ser aplicada para descartar preguntas dirigidas por parte de los interrogadores o preguntas que de fondo impliquen valoraciones profundamente subjetivas, que obligan de facto al declarante a asumir inconscientemente ciertas premisas, excluyendo así las preguntas no neutrales del interrogatorio. Finalmente, la aplicación de la IA a la neurociencia en el seno del proceso penal (Balbuena Pérez, 2017; Julià Pijoan, 2020) es otro campo de gran recorrido, si bien este ámbito debería ser explorado con las mayores cautelas posibles por la imposibilidad de detectar los falsos recuerdos y las mentiras inconscientes que son, precisamente, la mayoría de las que se escuchan en un proceso judicial.

C. La valoración de la documental aportada

Resultan indubitados los efectos benéficos del empleo de sistemas de IA para la valoración de los documentos, sea cual sea el soporte y el formato en el que se presente la información. Ténganse en cuenta los sistemas de procesamiento masivo de datos, o *big data,* y las posibilidades de analizar ingentes cantidades de información de forma lógica y ofrecer los resultados de forma estructurada. No se trata solo de capacidad de sumar grandes cantidades de información, sino también de la posibilidad de analizar con eficacia el lenguaje del documento, el vocabulario, las expresiones, la fiabilidad y autenticidad, así como técnicas que avanzan en la comprensión de un documento emulando el proceso cognitivo humano. Los sistemas de IA pueden comprender el significado de los textos, sea cual sea su idioma, y procesarlo ofreciendo una visión que ayudará a complementar la interpretación y valoración humana del juzgador, que ahora puede apoyarse en estas modernas técnicas.

D. La valoración de la prueba pericial

También, en el ámbito de la prueba pericial muchas son las posibilidades en relación con el empleo de los sistemas expertos de la IA. La pericial permite al juzgador, como jurista, acercarse a un ámbito del conocimiento o a un ámbito científico que desconoce profundamente. Lo hará sobre la base de la pericia y conocimiento de un experto de ese sector, apoyándose en sus resultados de forma crítica, aplicando distintos criterios de valoración, tanto del currículo del perito, como sustantivos, de fondo, como los llamados criterios Daubert de admisión de prueba pericial (Vázquez Rojas, 2015). Unos criterios que se construyen jurisprudencialmente en tres sentencias conocidas como la trilogía Daubert[3] y que han supuesto la modificación, en 2011, del artículo 702 de las *Federal Rules of Evidence*, cuyos efectos se proyectan incluso en los criterios doctrinales y jurisprudenciales que ayudan al juez español a valorar la prueba pericial más allá de la regulación sobre la valoración de la prueba contenida en el artículo 348 de la Ley de Enjuiciamiento Civil (2000) (en adelante, LEC).

Respecto a la valoración del currículo, es evidente que los sistemas de procesamiento masivo pueden

[3] Nos referimos a las sentencias de la Corte Suprema de los Estados Unidos, *Daubert c. Merrell Dow Pharmaceuticals* (1993); *General Electric Co. c. Joiner* (1997); *Kumho Tire Co. c. Carmichael* (1999).

indicar información muy relevante, detectando plagios o descubriendo méritos aparentes. Más allá de la creación de fórmulas o reglas lógicas que detallen un porcentaje de *expertise* determinado, los sistemas de IA también pueden leer los trabajos y aportaciones previas del supuesto experto para determinar si este realmente lo es, identificando la creatividad y originalidad de sus aportaciones (Nieva Fenoll, 2018, pp. 94-95).

En relación con los criterios Daubert, el principal reto es el digitalizarlos o automatizarlos. Parece evidente que un sistema experto de IA, en su modalidad más simple, de aplicación de algoritmos con reglas lógicas, bien podría resultar de utilidad a tal efecto, con los efectos benéficos de poder explicar el funcionamiento de la máquina con transparencia y publicidad. Por el contrario, un modelo de aprendizaje autónomo profundo o *deep learning* no permitiría tal extremo, al evolucionar el algoritmo dentro de la llamada *black box*. De esa manera, una vez expulsada la posibilidad de los sistemas de *deep learning*, nos queda observar el núcleo de lo que se pretende automatizar. Los criterios Daubert podrían simplificarse en el estudio o análisis de cinco ítems en relación con la prueba pericial: que la técnica siga un método científico verificado empíricamente; que sea pública y haya sido objeto de revisión por otros expertos; que indique el grado o porcentaje de error; que mantenga estándares y controles sobre la fiabilidad de la técnica; y que exista cierto consenso en la comunidad científica acerca de la técnica empleada. Como se observa, son criterios que podrían ser aplicados por sistemas expertos de IA programados *ad hoc*; de hecho, como señala Nieva Fenoll (2018, p. 97), parecen haber sido configurados realmente para construir un algoritmo sobre ellos.

III. TRANSPARENCIA DEL ALGORITMO E INDEPENDENCIA JUDICIAL: PAUTAS Y CRITERIOS PARA LA CREACIÓN DE UN ORGANISMO DE CONTROL

El empleo de sistemas expertos de IA en sede judicial nunca sustituirá a la persona (Nieva Fenoll, 2018; Simón Castellano, 2021b). Principalmente, porque no pueden superar el mandato constitucional del artículo 117 de la Carta Magna española (Constitución española, 1978), el cual señala que solo jueces y magistrados pueden juzgar y hacer ejecutar lo juzgado. Un androide o máquina no puede –por ahora–, ni debe –en el futuro–, hacerlo. Sin embargo, lo anterior no significa que no se puedan emplear sistemas expertos de IA como apoyo a determinados procesos judiciales, como para la adopción de decisiones tan significativas como la prisión provisional (Simón Castellano, 2021b), la libertad condicional o para la valoración de la prueba. Mientras la función jurisdiccional esté reservada a jueces, siempre necesitaremos contar con la participación decisiva del juzgador, quien, además, debe ser el humano al frente del sistema experto de IA en el ámbito de los llamados sistemas *Human in Command* (en adelante, HIC) o, en caso contrario, debe poder decidir si aplica y cómo los resultados y proyecciones que este ofrezca.

En este ámbito, los sistemas de IA no pueden ser ni implicar una *black box*, tampoco serian admisibles los sistemas técnicos basados en aprendizajes autónomos o *deep learning*. Estos avances no son aplicables a la institución procesal por tratarse de técnicas que no permiten acceder con publicidad y transparencia real al código, que cambia o muta constantemente en función de diferentes parámetros y que, además, no es explicable ni necesariamente razonable desde la óptica humana. No se trata tanto de que esos códigos no puedan publicarse, sino que, si se trata de sistemas de aprendizaje autónomo, probablemente no vamos a ser capaces de explicar o comprender las reglas lógicas, si es que estas existen, que hay detrás del mismo. Ni siquiera su creador o programador, es decir, quién lo diseñó en origen y quién escribió el código, sería capaz de explicar los resultados, valoraciones y decisiones que toma la máquina.

A. Sesgos de la IA y problemas de aplicación práctica

Veamos un ejemplo de cómo los sistemas de IAJVR se han introducido en el ámbito del derecho penal sustantivo y procesal para determinar cuestiones tan relevantes como para fundamentar la libertad condicional, la condena a una pena de prisión de larga duración o la imposición de una medida de seguridad (Romeo Casabona, 2018, pp. 48-55.; Martínez Garay, 2018). Me refiero al caso *Estado de Wisconsin c. Loomis* (2016), en el que el Tribunal Supremo de ese Estado resuelve el caso de un particular, Eric Loomis, que había sido acusado de cinco delitos por participación en un tiroteo efectuado desde un vehículo. Para lo que aquí interesa, el juez de instancia aceptó la conformidad del investigado y al concretar la pena tuvo en cuenta, entre otras cosas, el contenido de un *presentence investigation report* basado en el resultado de la evaluación de Eric Loomis mediante la herramienta COMPAS, que, como se mencionó anteriormente, utiliza IAJVR. Esta arrojaba con relación a Eric Loomis un riesgo alto de reincidencia, en general, y de reincidencia violenta, en particular. El juez condenó a Loomis a una pena de seis años de prisión y otros cinco de supervisión post penitenciaria, razonando que la pena es el resultado de la valoración de distintos factores, entre los que se encuentra el riesgo extremadamente alto de reincidir que le

atribuye la herramienta COMPAS, excluyendo la posibilidad de suspender la condena[4].

Como reacción, Eric Loomis, a través de su representante, interpuso recurso ante el Tribunal Supremo del Estado de Wisconsin, alegando que el uso de la herramienta de IAJVR había vulnerado su derecho a un juicio justo por basarse en información poco fiable o precisa por tratarse de una decisión automatizada, no individualizada a su caso concreto, y por haberse tenido en cuenta indebidamente su género para determinar la pena (De Miguel Beriaín, 2018). Ninguno de los motivos del recurso prosperó. El Tribunal Supremo de Wisconsin aceptó la utilización de los sistemas de IAJVR y su adecuación a las garantías constitucionales argumentando que el derecho de los acusados a un juicio justo no fue violado por el mero hecho de que la defensa no pudiera acceder a una explicación adecuada sobre el tratamiento o la fórmula de los algoritmos del sistema COMPAS (*Estado de Wisconsin c. Loomis*, 2016). Para apoyar esta posición, el Tribunal señaló que la exactitud de los instrumentos utilizados y la capacidad de los jueces para entender su posible mal funcionamiento eran suficientes para asegurar los derechos de los acusados (*Estado de Wisconsin c. Loomis*, 2016, párr. 54-57; 68-72; 83-86). De hecho, indica el Tribunal Supremo de Wisconsin que los sistemas de IAJVR aportan al juzgador información que, unida al resto de circunstancias concurrentes, contribuyen a que la condena se ajuste lo más posible al caso concreto. Lo que los jueces deben hacer cuando manejen estas herramientas es aplicar a sus resultados un margen de discrecionalidad, poniéndolos en el contexto del resto de circunstancias particulares propias del caso y del individuo concreto (Martínez Garay, 2018, p. 492).

Una 'solución' como la señalada no sería viable en un modelo más tuitivo, garantista, desde la óptica del derecho de defensa, como es el español. Los efectos de la sentencia *Estado de Wisconsin c. Loomis* son realmente preocupantes, puesto que esta práctica ha sido aceptada y confirmada en otros Estados. Además, como bien señala el voto particular a la sentencia, esta doctrina es muy insatisfactoria al producirse en un contexto en el que cada vez más las decisiones serán materialmente tomadas, parcial o totalmente, por los algoritmos y la programación basada en el código fuente aprobado (Romeo Casabona, 2018, p. 39-55). Sea como fuere, la referencia nos sirve como muestra de los problemas que proyecta el empleo de sistemas de IA en el seno del proceso penal. ¿Cómo se defiende el acusado o el investigado de una decisión que se apoya en un algoritmo opaco, cuyo funcionamiento no es transparente y cuyas reglas lógicas son desconocidas? ¿Qué sucede si los sesgos humanos se han proyectado o visto incluso reforzados por el código de la máquina? A nuestro modo de ver, y así lo hemos defendido a profundidad (Simón Castellano, 2021b), la respuesta pasa por la definición de un órgano de control público que garantice los principios de publicidad, transparencia, trazabilidad, auditabilidad y explicabilidad del código, y, muy significativamente, el principio de jurisdiccionalidad y legalidad desde el diseño y por defecto.

B. El órgano de control como garante de la independencia judicial y los principios de naturaleza jurídico-constitucional

El papel del órgano de control es fundamental desde el nacimiento hasta el funcionamiento y gestión de los sistemas expertos de IA que, eventualmente, puedan habilitarse para la valoración de la prueba en sede judicial. Recientemente, en el Boletín Oficial del Estado (en adelante, BOE) de 10 de diciembre de 2020 se publicó la Orden JUS/1179/2020, de 4 de diciembre, por la que se modifica la Orden JUS/1362/2016, de 3 de agosto, por la que se crea la Comisión Ministerial de Administración Digital del Ministerio de Justicia (en adelante, la Comisión) y se regula su composición y funciones. Un órgano que, a nivel nacional, parece estar predestinado a ejercer el control sobre los sistemas de IA en los que se puedan apoyar jueces y magistrados. Se quiere digitalizar la administración de justicia y mejorar la eficacia y eficiencia de los servicios, y el principal problema que se ve es que la lista o composición del órgano sorprende por sus ausencias notables: ningún juez, ni fiscal, ni letrado de la administración de justicia, ni abogado, ni funcionario. Al margen del representante de la Abogacía General del Estado, la Comisión está integrada por personas legas, que no saben ni conocen qué es un procedimiento judicial, ni lo han visto, ni saben los problemas diarios de los juzgados[5]. Tomarán decisiones e impulsarán desde el más absoluto vacío, el de la ignorancia y falta de conocimientos sobre qué necesitan nuestros juzgados y tribunales. No se trata de corporativismo ni de nada parecido. Si queremos introducir modernas tecnologías en sede judicial parece evidente que deberíamos recabar y tener muy presentes en la Comisión que impulsa esa transformación digital a los principales actores del proceso judicial.

[4] Véase la Sentencia de *Estado de Wisconsin c. Loomis* (2016, párr. 19 & ss).

[5] En esta misma dirección lo ha criticado la Asociación Profesional de la Magistratura (2020) en su cuenta de Twitter.

Precisamente, el principio de jurisdiccionalidad y legalidad desde el diseño del sistema de IA es el que exige que jueces y magistrados, los principales actores de la valoración probatoria, participen de forma activa en el órgano de gestión y control de aquel. De esa manera, cuando hablamos de un órgano de control de los sistemas de IA en el ámbito judicial, el órgano de gestión pasa, a *contrario sensu* de la realidad práctica de rabiosa actualidad, necesariamente, por la implicación y participación de todos los actores y agentes implicados en el proceso judicial. Una participación que debe producirse de forma integral cuando se trata de sistemas expertos de IA, es decir, desde el diseño del algoritmo o código, hasta la gestión, control y mejora continua de este.

Nada impide garantizar el control del sistema a través de una comisión que se reúna periódicamente, con independencia de su recurrencia –mensual, trimestral, semestral, etc–, mientras que la gestión diaria esté encomendada a responsables técnicos, que reporten, y den cuenta de la vigencia y efectividad de los controles y medidas técnicas-organizativas establecidas desde la misma. Lo importante, una vez más, es lo sustantivo, esto es que las funciones estén o deban estar claras, la incorporación del control y gestión sobre todos los procesos que impliquen la digitalización y el apoyo mediante sistemas técnicos a jueces y fiscales, incluidos los más modernos o revolucionarios, cuya principal arista es precisamente los sistemas expertos de IA. Además de las funciones, también deber ser clara la determinación de quién integra la Comisión y cómo se adoptan sus acuerdos.

El principal cometido o función del órgano de gestión y control debe ser, precisamente, garantizar ciertos principios de naturaleza jurídico-constitucional que deberían inspirar todo el proceso. Es ese órgano de control, integrado por juristas de diversa procedencia que representan lo mejor de distintas profesiones, junto a otros perfiles multidisciplinares o interdisciplinares, de naturaleza técnica, quien debe garantizar en la practica la publicidad y transparencia[6] de todo el proceso –no solo del sistema de IA, empezando por el detalle de quién participa en el órgano de control y quién tiene el encargo o deber de vigilancia y supervisión concreto–, la trazabilidad[7] del código de IAJVR –detalle de todas las acciones que llevan a cabo todos los agentes con poderes de gestión sobre el código o algoritmo, a modo de *backlog* o *audit trail*–, la explicabilidad[8] –hacer fácil lo difícil, hacer comprensible para una persona lega las principales pautas y reglas lógicas que hacen que el algoritmo proyecte esas estimaciones– y auditabilidad –interna y externa, sometido al escrutinio y revisión periódica de ojos expertos ajenos, que puedan certificar eventuales vulnerabilidades o deficiencias en la configuración técnica del sistema–.

Ese es el *prius* necesario para luego acompañar el sistema de determinadas garantías: la impugnabilidad del código, vehiculada a través de los recursos en el caso concreto, como parte del derecho de defensa, del derecho a recurrir[9], del derecho a tener una segunda oportunidad[10]. En el ámbito de la IA para la valoración de la prueba, las partes deben poder recurrir y protestar las decisiones adoptadas sobre la base de o en apoyo de los sis-

---

6 El Parlamento Europeo, al respecto, ha tenido la oportunidad de subrayar que todo sistema de inteligencia artificial debe desarrollarse respetando los principios de transparencia y de responsabilidad algorítmica de modo que los seres humanos puedan comprender sus acciones; y relacionado con lo anterior, indica que, a fin de generar confianza en la inteligencia artificial y permitir el progreso de la misma, los usuarios deben ser conscientes de cómo se utilizan sus datos personales, así como otros datos y datos derivados de sus datos, cuando se comunican o interactúan con un sistema de inteligencia artificial o con humanos que se apoyan en un sistema de inteligencia artificial (Resolución del Parlamento Europeo 2018/2088(INI), 2019, párr. 158).

7 El Parlamento Europeo, al respecto, ha tenido la oportunidad de subrayar que todo sistema de inteligencia artificial debe desarrollarse respetando los principios de transparencia y de responsabilidad algorítmica de modo que los seres humanos puedan comprender sus acciones; y relacionado con lo anterior, indica que, a fin de generar confianza en la inteligencia artificial y permitir el progreso de la misma, los usuarios deben ser conscientes de cómo se utilizan sus datos personales, así como otros datos y datos derivados de sus datos, cuando se comunican o interactúan con un sistema de inteligencia artificial o con humanos que se apoyan en un sistema de inteligencia artificial (Resolución del Parlamento Europeo 2018/2088(INI), 2019, párr. 158).

8 El legislador europeo ha destacado la importancia de poder explicar los resultados, los procesos y los valores de los sistemas de inteligencia artificial, de modo que resulten comprensibles para los destinatarios que no tengan conocimientos técnicos y que se les proporcione información significativa, condición necesaria para evaluar la equidad y ganarse la confianza (Resolución del Parlamento Europeo 2018/2088(INI), 2019, párr. 161).

9 También sobre este extremo se ha manifestado el Parlamento Europeo, que señala que las personas tienen derecho a saber, derecho de recurso y derecho a reparación cuando la inteligencia artificial se utilice para decisiones que les afecten y conlleven un riesgo significativo para los derechos o libertades individuales o puedan menoscabarlos (Resolución del Parlamento Europeo 2018/2088(INI), 2019, párr. 153).

10 Son muchos los retos sociales derivados de los sistemas de IA predictiva e IAJVR de los cuales resultan estimaciones o proyecciones que clasifican a los ciudadanos sobre la base de una elaboración de perfiles. En este ámbito, el Parlamento Europeo ha subrayado la necesidad de que los ciudadanos no sean objeto de discriminación en función de su clasificación y que deben tener derecho a una "segunda oportunidad" (Resolución del Parlamento Europeo 2018/2088(INI), 2019, párr. 12).

temas expertos, alejando cualquier tipo de duda o sombra sobre la imparcialidad del sistema de IA, garantizando y expulsando cualquier atisbo de sesgo discriminatorio, que pueda poner en tela de juicio que el juzgador, formal o sustantivamente, se haya sustentado en un elemento externo distorsionador, que haya condicionado su valoración del caso concreto de forma decisiva, basándose, como decíamos, en un prejuicio de base discriminatoria.

La asunción de esas funciones por parte del órgano de control, en la práctica, descarta el eventual sesgo de los promotores, es decir, de las empresas privadas. El Parlamento Europeo se ha referido a la necesidad de contar con una mano de obra diversificada en todas las ramas del sector de las tecnologías de la información, y con mecanismos de salvaguardia para evitar distorsiones basadas en el género y la edad en los sistemas de IA (Resolución del Parlamento Europeo 2018/2088(INI), 2019, párr. 168). El órgano de control debería, así, asumir un rol de supervisión de procesos y, muy significativamente, de aquellos que, hipotéticamente, pudieran perturbar de forma directa o indirecta el desarrollo de la IA, participando activamente en su diseño y gestión, y trabajando con métodos cuantitativos y cualitativos de prevención de riesgos como los que funcionan, por ejemplo, en el ámbito de la *compliance*, que permiten la detección de casos en los que los sistemas de IA pueden haber sido manipulados de forma accidental o malintencionada.

IV. REFLEXIONES FINALES

Primera.- A lo largo de este trabajo hemos observado algunos usos razonables acerca del empleo de la IA en la Administración de Justicia. Una administración que, como Tercer Poder, se encuentra ante la oportunidad o el precipicio, y que está condenada a ser digital o a su desaparición (Perea González, 2020).

Segunda.- El uso de la IA en la justicia entraña tantos o más riesgos que oportunidades, especialmente para los derechos, principios y garantías jurídico-constitucionales que reúne el proceso y, muy especialmente, el proceso penal. La pérdida del control y transparencia sobre el algoritmo puede derivar en una afectación de derechos fundamentales de la ciudadanía, tales como el derecho de defensa, la intimidad, la protección de los datos personales, la imparcialidad o independencia judicial o el principio de publicidad y transparencia de las actuaciones judiciales. Por límites espaciales obvios no hemos podido abordar aquí estos retos, si bien hemos tenido ocasión de formular un análisis en detalle en otro foro (Simón Castellano, 2021b).

Tercera.- La valoración de la prueba sin lugar a duda es uno de los ámbitos en los que el empleo de IA tiene más posibilidades y resultaría más útil, al contribuir a objetivar la libre valoración de la prueba del juzgador. Respecto a la prueba documental, las ventajas son indubitadas. Los sistemas de IA pueden comprender el significado de los textos, sea cual sea su idioma, y procesarlo ofreciendo una visión que ayudará a complementar la interpretación y valoración humana del juzgador, que ahora puede apoyarse en estas modernas técnicas. En relación con la prueba pericial, los sistemas de IA pueden contribuir a valorar con acierto y profundidad el currículo del perito y automatizar la aplicación al caso concreto de los criterios Daubert. Finalmente, por lo que se refiere a la valoración de las personas, los sistemas de IA pueden contribuir en aquel aspecto en el que la habilidad humana muestra su faceta más débil, que es, precisamente, las corroboraciones, al poder comprobar o chequear a tiempo real la compatibilidad de la declaración de testigos o partes con el resto de las pruebas admitidas y practicadas en sede judicial.

Cuarta.- Como consecuencia y reacción frente a la suma de la segunda –riesgos inherentes desde la óptica de los derechos y principios constitucionales– y tercera –notables oportunidades para la valoración racional y objetiva de la prueba– conclusión, resulta fundamental el papel que debe desempeñar el organismo de control como principal garante de la aplicación práctica de ciertos principios que, de lo contrario, quedarían en papel mojado. Nos referimos a los principios de publicidad, transparencia, accesibilidad, auditabilidad, explicabilidad y trazabilidad del código o algoritmo, a los que habría que sumar, como novedad y solo por lo que se refiere al empleo de la IA en sede judicial, el principio de jurisdiccionalidad y legalidad desde el diseño y por defecto. Un organismo que debería incluir la visión de los principales actores del proceso judicial, y cuya participación y control debería viajar desde la incepción, es decir, desde el diseño y la primera idea, hasta su implementación y gestión diaria, pasando por la necesaria revisión y mejora continua del sistema.

REFERENCIAS

Asociación Profesional de la Magistratura [@juecesAPM] (11 de diciembre de 2020). Comisión Ministerial de Administración Digital del @justiciagob sin ningún juez, ni fiscal, ni LAJ, ni abogado, ni funcionario. Gente que no conoce un procedimiento, no lo ha visto, ni sabe los problemas diarios de los juzgados. Fracaso asegurado @Jccampm [Enlace e imagen adjuntos] [Tweet]. Twitter. https://twitter.com/juecesAPM/status/1337312803821133824

Babuta, A., Oswald, M., & Rinik, C. (2018). *Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges* (Whitehall Reports, Vol 3, No. 18). Royal United Services Institute for Defense and Security Studies. https://rusi.org/publication/whitehall-reports/machine-learning-algorithms-and-police-decision-making-legal-ethical

Balbuena Pérez, D. E. (2017). *Derecho penal, neurociencia y libertad: una aproximación teórica al replanteamiento de la responsabilidad penal a propósito de las aportaciones neurocientíficas sobre el proceso mental para formación de la voluntad* (3ra ed.). Marben.

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, *104*(3), 671-732. http://dx.doi.org/10.15779/Z38BG31

Belfiore, R. (2013). The Protection of Personal Data Processed Within the Framework of Police and Judicial Cooperation in Criminal Matters. En S. Ruggeri (ed.), *Transnational Inquiries and the Protection of Fundamental Rights in Criminal Proceedings* (pp. 355-370). Springer.

Berrocal Lanzarot, A. I. (2017). *Derecho de supresión de datos o derecho al olvido*. Reus.

Boix Palop, A. (2020). Los algoritmos son reglamentos: La necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones. *Revista de Derecho Público. Teoría y Método*, *1*, 223-269. https://doi.org/10.37417/RPD/vol_1_2020_33

Bromby, M. C., & Hall, M. J. (2002). The Development and Rapid Evolution of the Knowledge Model of ADVOKATE: An Advisory System to Assess the Credibility of Eyewitness Testimony. En T. J. M. Bench-Capon, A. Daskalopulu, & R. G. F. Winkels (eds.), *Legal Knowledge and Information Systems. The Fifteenth Annual Conference* (pp. 143-152). IOS Press.

Cabellos Espiérrez, M. A. (2018). Opinar, enaltecer, humillar: respuesta penal e interpretación constitucionalmente adecuada en el tiempo de las redes sociales. *Revista Española de Derecho Constitucional,* 112, 45-86.

Calders, T., Kamiran, F., & Pechenikiy, M. (2009). Building classifiers with independency constraints. *2009 IEEE International Conference on Data Mining Workshops*, 13-18. https://doi.org/10.1109/ICDMW.2009.83

Cerrillo i Martínez, A. (2019). El impacto de la inteligencia artificial en el derecho administrativo ¿nuevos conceptos para nuevas realidades técnicas?. *Revista General de Derecho Administrativo,* (50).

Cerrillo i Martínez, A., & Peguera Poch, M. (2020). *Retos jurídicos de la inteligencia artificial.* Aranzadi.

Chayes, A. (1976). The Role of the Judge in Public Law Litigation. *Harvard Law Review*, *89*(7), 1281-1316. https://doi.org/10.2307/1340256

Citron, D. K., & Pasquale, F. (2014). The scored society: due process for automated predictions. *Washington Law Review, 89*, 1-33.

Cobacho López, A. (2019). Reflexiones en torno a la última actualización del derecho al olvido digital. Revista de Derecho Político, (1)104, 198-227. https://doi.org/10.5944/rdp.104.2019.24313

Cotino Hueso, L. (2019). Riesgos e impactos del Big Data, la inteligencia artificial y la robótica. enfoques, modelos y principios de la respuesta del derecho. *Revista General de Derecho Administrativo, 50*.

(2020). SyRI, ¿a quién sanciono? Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020. *La Ley Privacidad, (4)*.

Council of Bars and Law Societies of Europe (2020). *Considerations on the Legal Aspects of Artificial Intelligence*. CCBE.

Crawford, K. & Schultz, J. (2014). Big data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review, 55*(1), 93-128.

Creative Destruction Lab (22 de septiembre de 2017). Remarks from Daniel Kahneman [video]. Youtube. https://www.youtube.com/watch?v=gbj_NsgNe7A

De Asís Roig, R. F. (2018). Robótica, inteligencia artificial y derecho. *Revista de privacidad y derecho digital*, *3*(10), 27-77.

De Miguel Beriain, I. (2018). Does the use of risk assessments in sentences respect the right to due process? A critical analysis of the Wisconsin v. Loomis ruling. *Law, Probability and Risk, 1*(17), 45-53. https://doi.org/10.1093/lpr/mgy001

De Souza, K. (2018*). Delivering Artificial Intelligence in Government: Challenges and Opportunities*. IBM Center for Business and Government. https://www.businessofgovernment.org/report/delivering-artificial-intelligence-government-challenges-and-opportunities

Dumortier, F. (2010). Facebook and Risks of 'Decontextualization' of Information. En S. Gutwirth, Y. Poullet, & P. De Hert (eds.), *Data Protection in a Profiled World* (pp. 119-138). Springer.

Edwards, L., & Veale, M. (2017). Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for. *Duke Law & Technology Review*, *16*, 18-84.

Eggers, W. D., Schatsky, D., & Viechnicki, P. (2018). *AI-augmented government. Using cognitive technologies to redesign public sector work*. Deloitte University Press.

Ekman, P. (2011). *Cómo detectar mentiras: una guía para utilizar en el trabajo, la política y la pareja*. Paidós.

Ercilla García, J. (15 de diciembre de 2020). Automatización de la justicia: un ejemplo práctico. *Diario La Ley*. https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEAMtMSbF1CTEAAmNDCzMjI7Wy1KLizPw8WyMDIwNDQ0MLtbz8lNQQF2fb0ryU1LTMvNQUkJLMtEqX_OSQyoJU27TEnOJUtdSk_PxsFJPiYSYAALhfL5tjAAAAWKE

Executive Office of the President National Science & Technology Council Committee on Technology. (2016). *Preparing for the Future of Artificial Intelligence*. https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

Fernández Hernández, C. B. (2020a, 7 de mayo). El Consejo de la Abogacía Europea analiza los efectos de la aplicación de la Inteligencia Artificial en el ámbito jurídico. *Diario La Ley*. https://diariolaley.laleynext.es/dll/2020/05/07/el-consejo-de-la-abogacia-europea-analiza-los-efectos-de-la-aplicacion-de-la-inteligencia-artificial-en-el-ambito-juridico

(2020b, 24 de julio). Informe para el Parlamento Europeo sobre el uso de la inteligencia artificial en los ámbitos policial y judicial. *Diario La Ley*. https://diariolaley.laleynext.es/dll/2020/07/24/informe-para-el-parlamento-europeo-sobre-el-uso-de-la-inteligencia-artificial-en-los-ambitos-policial-y-judicial

(2020c, 13 de diciembre). Primera sentencia europea que declara ilegal un algoritmo de evaluación de características personales de los ciudadanos. *Diario La Ley*. https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDAyNDa3NDJUK0stKs7Mz7M1MjACC6rl5aekhrg425bmpaSmZealpoCUZKZVuuQnh1QWpNqmJeYUp6qlJuXnZ6OYFA8zAQCfSdkrYwAAAA==WKE

Ferrer Beltrán, J. (2002). *Prueba y verdad en el derecho*. Marcial Pons.

(2007). *La valoración racional de la prueba*. Marcial Pons.

Frey, C. B., & Osborne, M. A. (2017). The future of employment: how susceptible are jobs to computerization?. *Technological forecasting and social change, 14*, 254-280. https://doi.org/10.1016/j.techfore.2016.08.019

Gómez Manresa, F., & Fernández Salmerón, M. (2019). *Modernización digital en la administración de la justicia*. Aranzadi.

González Fuster, G. (2020). *Artificial Intelligence and Law Enforcement - Impact on Fundamental Rights*. European Parliament Think Tank Study. https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)656295

Harari, Y. N. (2018). *21 lecciones para el siglo XXI.* Debate.

HarvardCPL (14 de febrero de 2014). Daniel Kahneman, in conversation with Cass Sunstein [video]. Youtube. https://www.youtube.com/watch?v=NUvoEXGD7bE.

IT-POL (19 de junio de 2019). Danish DPA approves Automated Facial Recognition. *European Digital Rights Initiative*. https://edri.org/danish-dpa-approves-automated-facial-recognition/

Julià Pijoan, M. (2020). *Proceso penal y (neuro)ciencia: una interacción desorientada. Una reflexión acerca de la neuropredicción*. Marcial Pons.

Kahneman, D., Slovic, P., & Tversky, A. (1982). *Judgment under Uncertainty: Heuristics and Biases*. Cambridge University Press.

Kaplan, J. (2017). *Inteligencia artificial. Lo que todo el mundo debe saber*. Teell Editorial.

Libre valoración de la prueba (2020). En *Diccionario panhispánico del español jurídico*. https://

dpej.rae.es/lema/libre-valoraci%C3%B3n-de-la-prueba

Martínez Garay, L. (2018). Peligrosidad, algoritmos y due process: el caso State v Loomis. *Revista de Derecho Penal y Criminología*, (20), 485-502. https://doi.org/10.5944/rdpc.20.2018.26484

Martínez Martínez, R. (2019). Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo. *Revista Catalana de Dret Públic*, (58), 64-81. http://dx.doi.org/10.2436/rcdp.i58.2019.3317

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data. La revolución de los datos masivos*. Turner.

Miró Llinares, F. (2018). Inteligencia artificial y justicia penal: más allá de los resultados lesivos causados por robots. *Revista de Derecho Penal y Criminología*, *20*, 87-130.

Myers, D. G. (2002). *Intuición. El poder y el peligro del sexto sentido*. Paidós.

Nieva Fenoll, J. (2010). *La valoración de la prueba*. Marcial Pons.

(2018). *Inteligencia artificial y proceso judicial*. Marcial Pons.

Perea González, A. (24 de junio de 2020). Tercer Poder: la Justicia ante la oportunidad o el precipicio. *Diario el Mundo*. https://www.elmundo.es/opinion/columnistas/2020/06/24/5ef327c921efa062678b45f8.html

Ponce Solé, J. (2019). Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico. *Revista General de Derecho Administrativo, 50.*

Posner, E. A. (2011). *Cómo deciden los jueces* (V. Roca Pérez, trad.). Marcial Pons.

Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty Data, Bad Predictions: how Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice. *New York University Law Review,* (94), 15-55.

Romeo Casabona, C. M. (2018). Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad. *Revista de Derecho, Empresa y Sociedad (R.E.D.S.)*, (13), 39-55.

Sierra, S. (2020). Inteligencia artificial y justicia administrativa: una aproximación desde la teoría del control de la Administración Pública. *Revista General de Derecho Administrativo*, *53*.

Simon Castellano, P. (2012). *El régimen constitucional del derecho al olvido digital*. Tirant lo Blanch.

(2015). *El reconocimiento del derecho al olvido digital en España y en la UE*. Wolters Kluwer - Bosch.

(2021a). Inteligencia Artificial y Administración de Justicia: ¿Quo vadis, justitia?. *Revista Internet, Derecho y Política (IDP), 33.*

(2021b). *Justicia cautelar e inteligencia artificial. La alternativa a los atávicos heurísticos judiciales*. J. M. Bosch Editor.

Souza de Menezes, C., & Agustina, J. (2020). Big Data, Inteligencia Artificial y policía predictiva. Bases para una adecuada regulación legal que respete los derechos fundamentales. En D. Dupuy & J.G. Corvalán (dirs.), & M. Kiefer (coord.), *Cibercrimen III inteligencia artificial, automatización, algoritmos y predicciones en el derecho penal y procesal penal* (pp. 137-182). Editorial B de F.

Taruffo, M. (2002). *La prueba de los hechos* (J. Ferrer Beltrán, trad.). Trotta. (Obra original publicada en 1992).

Valero Torrijos, J. (2019). Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración. *Revista Catalana de Dret Públic*, (58), 82-96. http://dx.doi.org/10.2436/rcdp.i58.2019.3307

Vázquez Rojas, C. (2015). *De la prueba científica a la prueba pericial*. Marcial Pons.

Zarsky, T. (2016). The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making. *Science, Technology, & Human Values, 41*(1), 118-132.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Constitución Española [C.E.], B.O.E. n. 311, Dec. 29, 1978 (Esp.).

Daubert c. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993).

Estado de Wisconsin c. Loomis, 881 N.W.2d 749 (Wis. 2016).

European Commission for the Efficiency of Justice [CEPEJ], European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment, adopted on the 31st plenary (Dec. 3-4, 2018) (UE).

Fed. R. Evid. 702 (amended Dec. 1, 2020) (EE. UU.).

General Electric Co. c. Joiner, 522 U.S. 136 (1997).

Informe AEPD 385661/2017 de marzo relativo al anteproyecto de ley de sistema de alertas tempranas de la Comunidad Valenciana, Agencia Española de Protección de Datos, de 13 de marzo de 2018 (Esp.).

Kumho Tire Co. c. Carmichael, 526 U.S. 137 (1999).

Ley de Enjuiciamiento Civil (B.O.E. 2000, 1) (Esp.).

Ley de Inspección General de Servicios y del sistema de alertas para la prevención de malas prácticas en la Administración de la Generalitat y su sector público instrumental (B.O.E. 2018, 22) (Esp.).

Orden JUS/1179/2020, de 4 de diciembre, por la que se modifica la Orden JUS/1362/2016, de 3 de agosto, por la que se crea la Comisión Ministerial de Administración Digital del Ministerio de Justicia y se regula su composición y funciones (B.O.E. 2020, núm. 322) (Esp.).

Rb Dan Haag 5 februari 2020, NJ 2020, 368 m.nt. van E.J. Dommering (NJCM et al./Países Bajos) (Países Bajos).

Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), 2016 O.J. (L 119) 1 (UE).

Resolución del Parlamento Europeo, de 12 de febrero de 2019, sobre una política industrial global europea en materia de inteligencia artificial y robótica (2018/2088(INI)), 2019 O.J. (C 449) 39.

Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)), 2020 O.J. (C 404) 63.

10.18800/themis.202101.016

INTRODUCCIÓN AL *BLOCKCHAIN*, LOS CONTRATOS INTELIGENTES Y SU RELACIÓN CON EL ARBITRAJE

INTRODUCTION TO BLOCKCHAIN, SMART CONTRACTS AND THEIR RELATIONSHIP WITH ARBITRATION

Gonzalo Hierro Viétiez*
Samaniego Law

Digital transformation is advancing by leaps and bounds. In this scenario, blockchain technology, has successfully positioned itself in the digital and legal world, mainly due to its ability to create an ideal ecosystem for the execution of smart contracts, as well as its usefulness in developing accessible arbitration procedures, especially in small claims disputes.

This article provides an overview of blockchain which, although still in its embryonic stage, has demonstrated significant advances in relation to smart contracts and dispute resolution mechanisms. It also outlines the particular qualities of this technology which, when applied in arbitration, represent multiple benefits as opposed to conventional arbitration.

Keywords: Arbitration; smart contracts; Bitcoin; cryptoassets; technology; cybersecurity.

La transformación digital avanza a pasos agigantados. En este escenario, la cadena de bloques, también llamada blockchain*, se ha posicionado exitosamente en el mundo digital y jurídico, principalmente por su capacidad de crear un ecosistema ideal para la ejecución de contratos inteligentes. Así como su utilidad para desarrollar procedimientos arbitrales accesibles, sobre todo en conflictos de pequeña cuantía.*

En el presente artículo se brinda un panorama general del blockchain *que, aunque aún permanece en etapa embrionaria, ha demostrado avances significativos con relación a los contratos inteligentes y mecanismos de resolución de conflictos. Asimismo, se exponen las cualidades particulares de esta tecnología que, aplicada en el arbitraje, representan múltiples beneficios a diferencia de un arbitraje convencional.*

Palabras clave: Arbitraje; contratos inteligentes; Bitcoin; tecnología; criptoactivos; ciberseguridad.

* Abogado. Master of Laws (LL.M.) por el Fordham University, magíster en Acceso al Ejercicio de la Abogacía por la Universidad Carlos III de Madrid y magíster en Derecho Internacional, Comercio Exterior y Relaciones Internacionales por el Instituto Superior de Derecho y Economía. Asociado en Samaniego Law (Madrid, España). Contacto: gonzalo.hierro@samaniegolaw.com

Nota del Editor: Este artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 18 de enero de 2021, y aceptado por el mismo el 3 de julio de 2021.

I. INTRODUCCIÓN

La sociedad del siglo XXI se encuentra en continua transformación digital. Entre las tecnologías habilitadoras de dicha transformación destacan el internet de las cosas, la robótica, el *big data* y el *blockchain*, entre otros.

La pandemia global provocada por el COVID-19 ha impactado de lleno en ese proceso de cambio, acelerando exponencialmente la velocidad del mismo (Zelada, 2020). La comunidad arbitral no ha sido ajena a este proceso. Como ejemplo de lo dicho, basta recordar que han sido múltiples las cortes arbitrales que tuvieron que publicar, durante los primeros meses de la pandemia, notas sobre posibles medidas destinadas a mitigar los efectos de la pandemia o sobre organización de audiencias virtuales[1].

A raíz de las limitaciones de movilidad impuestas por la pandemia, múltiples plataformas de uso compartido de video se han introducido sin esfuerzo en nuestras vidas, convirtiéndose en herramientas habituales en nuestro quehacer diario. Junto con las plataformas para compartir documentos, se han convertido hoy en elementos básicos de cualquier procedimiento arbitral.

De entre los múltiples avances tecnológicos que, de ser aplicados al arbitraje, producirían mejoras incontestables en el procedimiento arbitral, destaca sobre los demás el de la cadena de bloques o *blockchain*. No cabe duda de que todos hemos oído este término, normalmente asociado con el Bitcoin y los criptoactivos; no obstante, cabe enfatizar que esta aplicación es únicamente la punta del *iceberg*.

A continuación, tras explicar sucintamente, para los no iniciados, en qué consiste la tecnología *blockchain*, describiré cuáles son sus tipos, qué entendemos por contratos inteligentes, qué aplicaciones prácticas tienen hoy en día en el arbitraje y qué ventajas podrían llegar a brindar al mismo en un futuro probablemente no muy lejano.

II. ¿EN QUÉ CONSISTE LA TECNOLOGÍA *BLOCKCHAIN* Y CUÁLES SON SUS TIPOS?

La tecnología *blockchain* fue inventada por una persona (o grupo de personas) bajo el seudónimo de Satoshi Nakamoto en 2008 (hasta la fecha, la identidad del creador o creadores sigue siendo un misterio). Su propósito era que sirviese de libro registro para las transacciones públicas de la criptomoneda Bitcoin.

La mayoría de las definiciones de la tecnología *blockchain* son demasiado técnicas o se centran demasiado en una de sus múltiples aplicaciones.

Según eToro, una de las principales plataformas para la compra y venta de criptoactivos, el *blockchain* es

> una cadena de código lineal que todo el mundo puede ver en su red. Está construida con segmentos de código de un tamaño predeterminado (o 'bloques'), organizados en una secuencia (o 'cadena'). Cada bloque es único y solo puede crearse una vez. Los bloques representan transacciones realizadas dentro de la red, que se muestran en un libro público de registro (2017).

La Fundación del Español Urgente la define como "un registro compartido por millones de ordenadores conectados donde se inscriben y archivan las transacciones de las partes de manera verificable, permanente y anónima sin necesidad de intermediarios" (2017).

Según el International Business Machines (en adelante, IBM), el *blockchain* es "un libro de contabilidad inmodificable y compartido para registrar transacciones, realizar el seguimiento de activos y generar confianza" (s.f. a).

Otros optan por una definición más descriptiva, y probablemente más ajustada y útil, en la medida en que engloba sus múltiples aplicaciones: *blockchain* es una base de datos que almacena información digital de manera altamente segura al ser administrada por ordenadores pertenecientes a una red de punto-a-punto y por el uso de funciones criptográficas (Hanshi *et al.*, 2019, p. 1).

Primavera de Filippi, una de las investigadoras más reconocidas en el mundo del *blockchain*, nos brinda, junto con Aaron Wright, una de las definiciones más completas de la tecnología en su libro Decentralized Blockchain Technology and the Rise of Lex Cryptographia:

> La tecnología Blockchain representa el siguiente paso en la economía peer-to-peer. Al com-

[1] Para mayor información, véase la Nota de orientación de la International Court of Arbitration sobre posibles medidas destinadas a mitigar los efectos de la pandemia del COVID-19 (2020), las Reglas de la CIMA para las Audiencias de pruebas testificales y periciales por medios audiovisuales (2020), y la Nota sobre organización de audiencias virtuales (Centro Internacional de Arbitraje de Madrid, 2020).

> binar redes peer-to-peer, algoritmos criptográficos, almacenamiento de datos distribuidos y mecanismos de consenso descentralizados, proporciona una forma para que las personas se pongan de acuerdo sobre un determinado estado de cosas y registrar ese acuerdo de manera segura y verificable (2015, pp. 4-5).

En cuanto a los diferentes tipos de cadenas de bloques, su clasificación variará dependiendo de la respuesta que demos a las dos preguntas siguientes: (i) ¿quién está autorizado a unirse y leer los datos digitales alojados en los bloques de la cadena? y (ii) ¿quién está autorizado a escribir los datos alojados en la cadena de bloques?

Dependiendo de la respuesta que demos a la primera pregunta, las cadenas de bloques pueden ser públicas, privadas o federadas.

Los *blockchain* públicos son accesibles para cualquier usuario que cuente con un dispositivo con conexión a internet (Lis Data Solutions, s.f.). Este tipo de cadena de bloques únicamente requiere la descarga de la aplicación correspondiente y la conexión con un número determinado de participantes o nodos (Campos Mínguez, 2019, p. 15).

De estas redes destaca la forma de validación de las transacciones a través de los protocolos de consenso, mecanismo que regula la forma en que los nodos llegan a un acuerdo para incorporar las transacciones a un bloque de la cadena.

Hay múltiples tipos de protocolos de consenso (por ejemplo, *proof of work, proof of stake, delegated proof of stake* y *proof of elapsed time*). El protocolo de consenso utilizado en la cadena de bloques pública más conocida, el Bitcoin, es el *proof of work*.

Este protocolo, de manera simplificada, permite que los participantes de la red resuelvan un problema complejo, normalmente empleando operaciones de cómputo. Las soluciones propuestas por los diferentes nodos son posteriormente verificadas por la red y, en su caso, aprobadas (Conejero & Porxas, 2018, p. 24).

Las operaciones de cómputo pueden llegar a ser muy costosas. Expertos han calculado que el consumo de electricidad aproximado de los superordenadores al realizar las operaciones requeridas por el *proof of work* de Bitcoin se encuentra entre 60 y 125 TWh al año (Buhl *et al.*, 2020, p. 603). Esto es, un consumo equiparable al de algunos países como Austria (75 GWh) o Noruega (125 GWh).

Independientemente de cuál sea el tipo de protocolo, el propósito común a todos ellos es poner de acuerdo a la mayor parte de los nodos en una misma red para que reconozcan operaciones legítimas y las validen. Se trata así de proteger la integridad de la red.

Las cadenas de bloques públicas se caracterizan por su descentralización, inmutabilidad y seguridad.

Son descentralizadas, porque no hay un único punto de decisión. Cada nodo toma la decisión que más le conviene en función de las reglas de consenso establecidas. El resultado del conjunto del sistema es la respuesta colectiva. Esto refuerza la seguridad del *blockchain*, ya que impide que los atacantes se centren en un único punto de entrada (Cordero Valvavida, 2019, p. 21).

Son inmutables porque cada bloque contiene un *hash* (un identificador único) del bloque anterior. Este identificador único se obtiene al usar algoritmos criptográficos sobre un conjunto de datos. Estos algoritmos criptográficos obtendrán siempre el mismo resultado si se utilizan sobre el mismo conjunto de datos. En el caso en el que se produzca alguna modificación de los datos de algún bloque dentro de la cadena, aunque sea mínimo, este sería fácilmente identificable, ya que los identificadores no coincidirían.

Su seguridad, además de verse reforzada por la descentralización y la inmutabilidad del *blockchain*, proviene de la encriptación de los datos.

Los *blockchain* privados, a diferencia de los públicos, requieren de una invitación para acceder a ellos. Estas cadenas de bloques dependen de una entidad central que controla todas las acciones dentro de la misma. Los *blockchain* privados, por lo general, se construyen para usos corporativos (Gárate Rivera, 2021).

Al igual que las cadenas de bloques públicas, las privadas se caracterizan por su inmutabilidad y seguridad, pero es importante resaltar que, a diferencia de los *blockchains* públicos, al no ser descentralizadas, tienen una mayor velocidad de transacciones y estas son más baratas. Además, el que el acceso esté restringido y controlado por una entidad central asegura la confidencialidad del registro de las transacciones.

Las cadenas de bloques federadas son una mezcla entre las públicas y las privadas. En ellas, la participación es privada, el control lo ostentan varias organizaciones y la información es accesible de forma pública.

La respuesta a la segunda pregunta, ¿quién está autorizado a escribir los datos alojados en la cade-

na de bloques?, nos indicará si la cadena de bloques es 'permisionada' (*permissioned*) o 'no permisionada' (*permissionless*), esto es, si todos los usuarios están autorizados a escribir los datos en el *blockchain* o solo unos pocos (Benítez Martínez, 2021, p. 161).

En la práctica, la mayor parte de iniciativas *blockchain* son públicas no permisionadas o privadas permisionadas.

Los *blockchains* públicos no permisionados más conocidos son los de Bitcoin y Ethereum, dos criptomonedas.

Dentro de las cadenas de bloques privadas no permisionadas más conocidas se encuentran Hyperledger[2] (de la Fundación Linux, enfocada al desarrollo de *frameworks*, herramientas y librerías destinadas a ser usadas en soluciones *blockchain* en el sector empresarial), Diem[3] –antes llamada Libra– (de Facebook) o R3[4] (una empresa que aspira a desarrollar soluciones *blockchain* adaptadas a instituciones financieras).

Según el informe Deloitte's 2020 Global Blockchain Survey, algunos de los hitos clave de la tecnología, acaecidos en 2019 o 2020, referidos a la aplicación de los criptoactivos, fueron la presentación de Libra, que contaba con el apoyo de más de 100 compañías (entre ellas Visa, eBay y Mastercard) y el anuncio por parte de China del lanzamiento de un Yuan digital (Deloitte, 2020).

Grandes empresas como IBM y el Banco Santander han realizado cuantiosas inversiones en esta tecnología. IBM fue la compañía que registró más patentes en tecnología *blockchain* en 2019[5]. Entre sus proyectos podemos destacar el IBM Food Trust[6], que pretende utilizar la cadena de bloques para facilitar el acceso a los consumidores al historial de producción y transporte de alimentos, así como su asociación con Walmart y Merck en la llamada Pharmaceutical Unity Network[7], en la que las empresas construyeron una plataforma de código abierto para facilitar el *compliance* de sus tecnologías con la *Drug Supply Chain Security Act*. Por su parte, el banco Santander, entre otras iniciativas, lanzó el primer bono con tecnología *blockchain* de principio a fin en septiembre de 2019[8].

Pero no solo las empresas están interesadas en la infinidad de posibilidades de esta tecnología. En abril de 2018 se creó la European Blockchain Partnership (en adelante, EBP)[9], formada por todos los Estados miembros de la Unión Europea y dos miembros del Espacio Económico Europeo (Noruega y Liechtenstein). El objetivo de la EBP es "desarrollar el potencial de los servicios basados en la tecnología *blockchain* en beneficio de los ciudadanos, la sociedad y la economía" (Digital Connecting Europe, s.f.). A raíz de esta iniciativa, se creó la European Blockchain Services Infrastructure (en adelante, EBSI)[10], red de nodos distribuidos por toda Europa que prestará servicios públicos transfronterizos.

Uno de los proyectos más ambiciosos en los que está colaborando la EBSI, empleando *blockchain*, es la llamada Self-Sovereign Identity (en adelante, SSI)[11]. La SSI pretende que sea el individuo el que gestione los elementos que componen su identidad y controle el acceso a esas credenciales. Con la SSI, la facultad de controlar los datos personales reside en el individuo, no en un tercero, lo cual es unánimemente aceptado como un paso en la dirección correcta.

Parte de las razones del poder de atracción de la tecnología *blockchain* a empresas y Estados reside asimismo en los contratos inteligentes, lo que se conoce en inglés como *smart contracts*.

III. LOS CONTRATOS INTELIGENTES Y LOS ORÁCULOS

Blockchain es la tecnología por excelencia para crear contratos inteligentes. A menudo se asocia a los *smart contracts* con Ethereum, una plataforma de código abierto, digital, descentralizada y pro-

2 Véase la página web de Hyperledger (s.f.).

3 Véase la página web de Diem (s.f.)

4 Véase la página web de R3 (s.f.)

5 Para más información sobre las patentes registradas por IBM, véase a Gil (2020).

6 Para más información sobre IBM Food Trust, véase su página web (IBM, s.f. b)

7 Para más información sobre Pharmaceutical Unity Network, véase a Merck (2020)

8 Para más información sobre el bono con tecnología *blockchain* emitido por el banco Santander, véase a Santander (2019).

9 Para más información sobre la EBP, véase a Digital Connecting Europe (s.f.)

10 Para más información sobre la EBSI, véase a Digital Connecting Europe (s.f.)

11 Para más información sobre la colaboración de la EBSI en el diseño y creación de la SSI, véase a Digital Connecting Europe (s.f.)

gramable, conocida por los criptoactivos Ethereum –la segunda criptomoneda más importante del mundo por valor de mercado– y Ethereum Classic.

Según Vitalik Buterin, el cofundador de Ethereum, en los contratos inteligentes un activo o moneda se transfiere a un programa y este ejecuta un código que, en algún momento, validará automáticamente una condición[12]. La condición que se valide determinará automáticamente si el activo debe transferirse a una persona, si debe devolverse a otra persona o alguna otra de las alternativas previamente pactadas.

El informático, jurista y criptógrafo americano de ascendencia húngara, Nick Szabo, que acuñó el término *smart contracts*, los define como "a set of promises, specified in digital form, including protocols within which the parties perform on these promises" (1996, p. 50)[13].

En esa línea, los compara con una máquina expendedora. Cuando el consumidor introduce en la ranura el dinero correspondiente, la máquina automáticamente entrega el producto elegido al consumidor. No obstante, a diferencia del ejemplo de la máquina expendedora, los contratos inteligentes permiten la automatización de todo el proceso, sin que sea necesaria acción alguna de las partes para hacer ejecutar lo pactado.

Además de caracterizarse por ser autoejecutables, su otra faceta clave es que garantizan el cumplimiento sin necesidad de recurrir a las autoridades.

Además de Ethereum, distintas plataformas como Hyperledger o Corda (del Consorcio R3) ofrecen soluciones para desarrollar contratos inteligentes.

Los contratos inteligentes, al ser programas ligados al *blockchain*, necesitan poder acceder directamente a información que se encuentra fuera de la cadena para una correcta ejecución. Para ello, utilizan sistemas conocidos como oráculos.

Según Federico Ast, fundador de Kleros[14], los oráculos son los encargados de introducir datos externos en la cadena de bloques con el objetivo de iniciar la ejecución de los *smart contracts* (2020). En esa línea, los describe como 'puentes' entre el mundo exterior y la cadena de bloques. Quien controla el oráculo, controla la ejecución del contrato.

Por esta razón, es esencial elegir un oráculo que utilice fuentes de datos fiables. En 2020, debido a información de precios incorrecta del oráculo que proporcionaba información a la plataforma de finanzas Compund[15], se ocasionó una liquidación errónea por aproximadamente 100 millones de dólares.

IV. EL ARBITRAJE EN EL *BLOCKCHAIN*

En una reciente encuesta realizada por Pinsent Masons en colaboración con la Queen Mary University of London, una proporción importante de los encuestados consideró que

> [t]he arbitral process is […] a barrier to the fair resolution of what might be described as lower value disputes, i.e., less than USD 10 million. If alternative dispute resolution provides a more efficient route to resolving such smaller value disputes, it may well be the preferred vehicle to achieve this (2019, p. 5)[16].

Con la transformación digital, cada vez se realizan más transacciones *online* entre personas de todo el mundo. Este aumento del número de transacciones, como no podía ser de otra forma, ha dado lugar a un correspondiente incremento del número de disputas.

A lo largo de los últimos años han surgido múltiples iniciativas que han intentado aprovechar la existencia de este nicho de mercado, articulando una solución inspirada en la tecnología *blockchain* y los *smart contracts*. Algunas de estas iniciativas, que se hacen descansar normalmente en el diseño de un procedimiento arbitral accesible para conflictos de pequeñas cuantías y en esas tecnologías, son Bitrated, Confideal, Juris o Kleros.

Bitrated[17] es una plataforma de adjudicación de controversias (lo que se conoce en inglés como *claim adjudication platform*) diseñada para Bitcoin.

---

12 En 2016, Vitalik Buterin definió los smart contracts en una Cumbre Blockchain en Washington, D.C.

13 Traducción libre: "Un conjunto de promesas, especificadas en forma digital, incluidos los protocolos con los que las partes cumplen estas promesas".

14 Para más información sobre Kleros, véase a Ast, George y Lesaege (2019).

15 Para más información sobre Compound, véase su página web (Compound, s.f.)

16 Traducción libre:

> El proceso arbitral es […] una barrera para la resolución justa de lo que podría describirse como disputas de menor valor, es decir, menos de 10 millones de dólares. Si la resolución alternativa de conflictos ofrece una vía más eficaz para resolver estos litigios de menor valor, puede ser el vehículo preferido para conseguirlo.

17 Para más información sobre Bitrated, véase su página web (Bitrated, s.f.)

Las partes, previamente a concluir la transacción, nominan a un *trust agent* que, en caso de disputa, actuará como árbitro y dirimirá la controversia. En el momento en que todas las partes hayan consentido su participación en la transacción, el comprador procede con el pago en una *multi-signature address*[18], donde el vendedor podrá comprobar que el pago se ha realizado. Acto seguido, el pago queda bloqueado en la *multi-signature address* hasta que dos de las tres partes (comprador, vendedor y *trust agent*) acuerden liberarlo. En el caso de que todo vaya bien, el comprador y el vendedor acordarán liberar el pago, y quedará bajo el control del vendedor, sin necesidad de intervención alguna por parte del *trust agent*. En caso de surgir una disputa, el *trust agent* puede intervenir, revisar el caso y decidir qué parte tiene razón, ya sea devolviendo el pago al comprador o librándolo al vendedor.

Bitrated incluye un sistema de gestión de la reputación para ayudar a las partes a escoger al *trust agent*.

Por su lado, Confideal es un servicio que ayuda a las partes a crear *smart contracts* que integran un mecanismo de resolución de disputas, el cual permite a los usuarios resolver sus controversias sin tener que recurrir a terceros intermediarios fuera de la cadena de bloques (Gandhi *et al.*, 2020, p. 2).

Los usuarios, antes de celebrar el contrato inteligente, seleccionan al árbitro que, en su caso, conocerá de la disputa. Los árbitros se escogen de entre un listado que incluye a miembros de asociaciones, centros de arbitrajes u otras organizaciones que garanticen la experiencia de estos en arbitraje. Al igual que Bitrated, también incluye un sistema de clasificación de árbitros según criterios objetivos y subjetivos para ayudar a los usuarios a elegir (Buckle *et al.*, 2018, p. 33).

Juris[19] proporciona un sistema alternativo de resolución de disputas para los contratos inteligentes. Los usuarios pueden optar por integrar un código relativo a dicho sistema en su *smart contract*. En caso de surgir una controversia, el protocolo Juris se activa y el cumplimiento del *smart contract* queda suspendido.

Este protocolo se divide en varias etapas. En este sentido, es similar a una cláusula escalonada, a las que se conoce en inglés como *multi-tiered dispute resolution clause*. En un primer momento, el protocolo insta a las partes a lo que se llama una *SELF Mediation*. En esta primera fase, Juris proporciona a las partes el acceso a una amplia gama de herramientas y técnicas de mediación para facilitarles resolver el conflicto amistosamente.

De no ser efectiva, se pasa a la segunda fase, la llamada *SNAP (Simple Neutral Arbitrator Poll) Judgment*. En esta fase, se facilita a todos los juristas disponibles información sobre la disputa. Estos tendrán una cantidad limitada de tiempo para revisar los detalles de la controversia y dar su opinión sobre una posible solución basada en la equidad, todo ello desde la anonimidad. Las partes, tras recibir el desglose de los resultados, siguen teniendo la opción de resolver la controversia por su cuenta.

Por último, si las partes no consiguen llegar a un acuerdo amistoso satisfactorio, cualquiera de ellas puede escoger pasar a la tercera fase, llamada *Binding PANEL (Juris Peremptory Agreement for Neutral Expert Litigation) Judgment*. En esta fase, el protocolo Juris facilitará la selección de tres *high-jurists* (aquellos juristas con un alto nivel de reputación dentro del sistema Juris), clasificados según sus especialidades y cualquier otro factor incluido por las partes en el contrato inteligente. Este tribunal cuenta con un tiempo predeterminado para dirimir la controversia. Cuando el tribunal haya llegado a una decisión, el presidente tendrá la facultad de ejecutarla inmediatamente, a través de la modificación correspondiente del *smart contract*.

Por su parte, los fundadores de Kleros definen a su servicio como

> a decentralized application built on top of Ethereum that works as a decentralized third party to arbitrate disputes in every kind of contract, from very simple to highly complex ones. It relies on game theoretic incentives to have jurors rule cases correctly. The result is a dispute resolution system that renders ultimate judgments in a fast, inexpensive, reliable, and decentralized way (Ast *et al.*, 2019, p. 1)[20].

---

[18] Las *multi-signature addresses* se caracterizan por necesitar más de una llave para efectuar una transacción.

[19] Para más información, véase Juris (2018).

[20] Traducción libre :

> Una aplicación descentralizada construida sobre Ethereum que funciona como una tercera parte descentralizada para arbitrar disputas en todo tipo de contratos, desde los más simples hasta los más complejos. Se basa en incentivos de la teoría del juego para que los jurados resuelvan los casos correctamente. El resultado es un sistema de resolución de conflictos que dicta sentencias definitivas de forma rápida, económica, fiable y descentralizada.

Esta iniciativa fue la ganadora del Blockchains for Social Good Prize de la Unión Europea en 2020.

Las partes de un contrato inteligente tienen que designar a Kleros como su árbitro. Cuando optan por Kleros, esta elige cuántos miembros tendrá el jurado y qué corte dentro del sistema Kleros será la que conozca de la controversia (por ejemplo, aquella especializada en seguros, *e-commerce* o transporte).

Kleros opera a través del *crowdsourcing* de jurados anónimos. Estos se proponen a sí mismos usando *tokens* (también llamados *pinakion*). Cuantos más *tokens* apuesten, más posibilidades tienen de ser elegidos. Los que resulten elegidos revisarán las pruebas disponibles y, posteriormente, tomarán una decisión. Los jurados que emiten una decisión coherente con la decisión mayoritaria son recompensados, mientras que los que deciden en contra de la mayoría son penalizados con la pérdida de *tokens*, que son transferidos a los que votaron 'correctamente' (Gandhi *et al.*, 2020, p. 2).

Una particularidad de Kleros es que admite apelaciones. En el caso de que una de las partes no esté conforme con la decisión del jurado, puede apelar. Cada nueva apelación será revisada por el doble de miembros en el jurado más uno. Por ello, tanto los honorarios por la gestión del arbitraje como los del jurado aumentan exponencialmente con cada apelación.

V. ¿QUÉ VENTAJAS PUEDE BRINDAR LA TECNOLOGÍA *BLOCKCHAIN* AL ARBITRAJE?

Independientemente del arbitraje en el *blockchain*, la tecnología de cadenas de bloques puede ser beneficiosa para el arbitraje 'tradicional', ayudando a mitigar los riesgos de ataques cibernéticos, a preservar la confidencialidad del procedimiento arbitral y a hacerlo, además, más eficiente.

A. Ciberseguridad

La transformación digital, además de sus innumerables beneficios, también acarrea peligros. El número de ciberataques a plataformas móviles y a la nube, según un informe de Check Point Software Technologies Ltd., aumentó en 2019 con respecto a años anteriores (2020). Además, se vaticina que la vulnerabilidad de las redes aumentará con el despliegue de la tecnología 5G, entre otras razones, por el aumento de dispositivos conectados.

Los despachos de abogados no son ajenos a estos peligros. Uno de los casos más sonados en su día fue la fuga de los Papeles de Panamá, donde millones de documentos confidenciales de una firma de abogados panameña se filtraron[21].

Más recientemente, en mayo de 2020, una firma de abogados americana, especializada en asesoramiento legal a artistas y medios de comunicación, reconoció haber sufrido un ciberataque. A cambio de no publicar la información obtenida, los *hackers* pedían 21 millones de dólares. Para ejercer presión, los *hackers* llegaron a filtrar información que involucraba a la conocida artista Madonna[22].

En esa línea, las cortes y procedimientos arbitrales no son ajenos a los ciberataques. Por ejemplo, en el caso *Libananco Holdings Co. Limited c. Turquía* (2008), el demandante informó al tribunal arbitral de que había tenido conocimiento de

> [t]urkish court orders requested and obtained by Respondent in 2007 and 2008, expressly to conduct intercept of emails and MSN instant messages not only sent by and to persons associated with Claimant but also approximately 1,000 privileged, private, and confidential emails sent by, to and between Claimant's counsel of record in connection with this arbitration over the past year (citado en *Araque Moreno et al.*, 2020, p. 549)[23].

Este no es un caso aislado, la Corte Permanente de la Haya sufrió un ciberataque en 2015 mientras se celebraba la audiencia de prueba sobre la disputa territorial por el mar de la China meridional entre Filipinas y China. En el tercer día de audiencia, el sitio web de la Corte fue infectado por *malware*, por lo que tuvo que ser desconectado.

Durante los últimos años, para mitigar los riesgos de ciberseguridad, se han promulgado diferentes normas *soft law* con el objetivo de informar a los usuarios de un procedimiento arbitral sobre la importancia de la ciberseguridad, proporcionándoles al tiempo útiles directrices a seguir en estos casos.

[21] Para más información sobre el caso, véase a Reuters Staff (2018).

[22] Para más información sobre el caso, véase a El País (2020).

[23] Traducción libre:

> La corte turca ordenó y obtuvo del demandado en el 2007 y 2008, la interceptación de correos electrónicos y mensajes instantáneos de MSN enviados no solo por y a personas asociadas con el demandante, sino también aproximadamente 1000 correos electrónicos privilegiados, privados y confidenciales enviados por, a y entre el demandante y sus abogados respecto del proceso arbitral que se llevaba a cabo en ese año.

Un ejemplo es el Protocol on Cybersecurity in International Arbitration[24], elaborado en 2020 por la International Council for Commercial Arbitration (ICCA), la New York City Bar Association (NYC Bar) y el International Institute for Conflict Prevention & Resolution (CPR).

Los ciberataques sufridos tanto por cortes arbitrales como por usuarios del arbitraje no quieren decir que estos sean especialmente vulnerables, sino que no son inmunes. Nadie es completamente inmune, grandes multinacionales como Sony Pictures, Yahoo, eBay y Facebook también han sido víctimas de ciberataques.

Pues, precisamente, uno de los múltiples posibles beneficios que puede aportar la transformación tecnológica al arbitraje, a través de la tecnología *blockchain*, es la ciberseguridad.

Según Forbes,

> la *blockchain* o cadena de bloques se presenta como una opción viable para hacer frente a los ciberataques y estafas, al ser un libro de registros perfecto e infalsificable que permite la transferencia de datos con una codificación muy sofisticada y segura (Riveroll, 2018).

Las cualidades anteriormente mencionadas de las cadenas de bloques privadas, esto es, su inmutabilidad y seguridad, convierten a esta tecnología en la perfecta aliada de los usuarios del arbitraje en su preocupación por mitigar los riesgos de ciberseguridad inherentes a la transformación digital que vivimos.

La inmutabilidad del *blockchain* ayudaría a mejorar la ciberseguridad al facilitar la detección de actividades fraudulentas, a través de mecanismos de consenso y de cualquier alteración de los datos.

Aunque las cadenas de bloques, por lo general –por su carácter descentralizado–, no tienen un único punto de falla, las cadenas de bloques privadas, al contar con un menor número de nodos, tendrán que asegurarse de que su red está suficientemente distribuida y sea resistente en todos sus puntos para garantizar un funcionamiento continuo incluso en caso de ciberataque (Kumar, 2018). Así, aunque gran parte de la red esté sufriendo un ciberataque, el *blockchain* seguiría operativo.

A pesar de las características que revisten las cadenas de bloques, sería ingenuo creer que son totalmente impenetrables. Como sostiene Cillian Leonowicz, alto directivo de Deloitte en Irlanda,

> blockchain's characteristics do not provide an impenetrable panacea to all cyber ills, to think the same would be naïve at best, instead as with other technologies blockchain implementations and roll outs must include typical system and network cyber security controls, due diligence, practice, and procedures (citado en *Dalton et al.*, 2017, p. 4)[25].

B. Confidencialidad

Por otra parte, la tecnología *blockchain* también podrá ayudar a los usuarios del arbitraje a mantener la confidencialidad del procedimiento arbitral.

En otra encuesta llevada a cabo en este caso por White & Case y la Queen Mary University of London, el 87% de los encuestados señalaron que la confidencialidad es importante o muy importante en un procedimiento arbitral y que debería ser "an opt-out, rather than an opt-in feature" (2018, p. 3)[26]. Además, el 35% de los encuestados escogieron la confidencialidad y privacidad como una de las características más valiosas del arbitraje internacional.

Las cadenas de bloques privadas, y en concreto las no permisionadas, al tener una entidad central controlando los permisos de acceso de los diferentes usuarios a la información, podrían ser un elemento adicional que contribuiría sustancialmente a preservar la confidencialidad del procedimiento arbitral y de sus documentos.

C. Eficiencia

Asimismo, más de la mitad de los encuestados en ese mismo sondeo de opinión declararon que "increased efficiency, including through technology, is the factor that is most likely to have a significant impact on the future evolution of international

[24] Para más información sobre el protocolo de ciberseguridad, véase a International Council for Commercial Arbitration (2019).

[25] Traducción libre:

> Las características del *blockchain* no ofrecen una panacea impenetrable contra todos los males cibernéticos, creer ello sería ingenuo, en su lugar, como otras tecnologías, las implementaciones y uso de *blockchain* debe incluir los controles de seguridad, diligencia, práctica y procedimiento de sistemas y redes típicos.

[26] Traducción libre: "una característica que se escoja no tener, en vez de una que se escoja tener".

arbitration" (Queen Mary University of London & White & Case, 2018, p. 3)[27].

Según IBM, algunos de los beneficios de la tecnología de cadena de bloques para la solución de controversias incluyen: (i) una resolución más rápida de controversias; (ii) un ahorro de costes laborales; (iii) un menor riesgo de que las controversias no se reconcilien adecuadamente; y (iv) menos dinero paralizado a esperas de la resolución de la disputa (Dickinson, 2020).

Por los costes asociados que ello conlleva y, como ya destaqué anteriormente, es incontrovertible que en muchas ocasiones no merece la pena que las partes inicien un procedimiento arbitral para dar solución a las diferencias que les separan. En algunos casos, principalmente en transacciones *online* que entrañen un monto económico no elevado, pues, como vulgarmente se dice, 'el remedio puede ser peor que la enfermedad'. En cambio, si esas transacciones se realizan a través de *smart contracts* en una cadena de bloques, la solución de la controversia podrá conseguirse a través de algunas de las iniciativas que están surgiendo de una manera menos costosa y, además, mucho más eficiente.

VI. CONCLUSIONES

En los últimos tiempos, vivíamos en un mundo en continua transformación digital. Este proceso de cambio era relativamente pausado hasta la pandemia del COVID-19, que ha acelerado exponencialmente el proceso, ahora realmente vertiginoso. Antes, celebrar una audiencia de prueba de manera virtual era inusual. Hoy en día, no hay corte de arbitraje que no haya publicado una guía sobre cómo celebrarlas por la sencilla razón de que la excepción se ha convertido en regla y la regla en excepción.

Las cadenas de bloques, aunque se encuentren en su fase embrionaria de desarrollo, van mostrando avances significativos y se acercan, no hay duda, a su despliegue a gran escala.

Sus propiedades intrínsecas podrían ayudar al correcto desarrollo de un procedimiento arbitral, tanto en aquello relacionado con la ciberseguridad como con la confidencialidad y la eficiencia misma del procedimiento.

El arbitraje en el *blockchain* puede aprovechar el nicho de mercado de las controversias de pequeña cuantía, mientras que la tecnología *blockchain* tiene múltiples aplicaciones prácticas en el mundo del arbitraje aún por desarrollar.

Por ello, tanto los usuarios del arbitraje en el *blockchain* como la comunidad arbitral deben prepararse para adaptarse tanto a las aplicaciones ya desarrolladas como a aquellas otras que a buen seguro se desarrollarán en un futuro no tan lejano como algunos creen. Como afirman desde Pinsent Masons y la Queen Mary University of London,

> [w]hilst it may be some time before technologies such as blockchain and augmented reality are used as a matter of course in construction arbitrations, it is incumbent upon the arbitration community to engage with the technology industry and, in line with its clients, make the transition to the digital environment (2019, p. 41)[28].

REFERENCIAS

Araque Moreno, Y., Fernández-Samaniego, J., & Hierro Viéitez, G. (2020). Ciberseguridad y arbitraje internacional: el Protocolo de Ciberseguridad en Arbitraje Internacional del ICCA, el NYC Bar y el CPR (Edición 2020). *THĒMIS-Revista De Derecho*, (77), 547-557. https://doi.org/10.18800/themis.202001.031

Ast, F. (24 de diciembre de 2020). Oráculos: Conectando los Smart Contracts con el Mundo. *Astec*. https://medium.com/astec/or%C3%A1culos-conectando-los-smart-contracts-con-el-mundo-9bcfda4ebffb

Ast, F., George, W., & Lesaege, C. (2019). *Kleros* (Short Paper v1.0.7). https://kleros.io/whitepaper.pdf

Benítez Martínez, F. (2021). *Un modelo de gobernabilidad para procesos de eDemocracia basados en una red neuronal de blockchain* (tesis doctoral). Universidad de Granada, Granada, España.

Bitrated. (s.f.). Frequently Asked Questions. https://www.bitrated.com/faq

[27] Traducción libre: "El aumento de la eficiencia, incluso a través de la tecnología, es el factor que más probablemente tendrá un impacto significativo en la evolución futura del arbitraje internacional".

[28] Traducción libre:

> Aunque puede pasar algún tiempo antes de que tecnologías como el *blockchain* y la realidad aumentada se utilicen de forma habitual en los arbitrajes de construcción, corresponde a la comunidad arbitral comprometerse con la industria tecnológica y, en consonancia con sus clientes, hacer la transición al entorno digital.

Buckle, M., Dowling, C., & Rogers, J. (2019). Energy, technology and arbitration: The latest buzz. *Norton Rose Fulbright's International Arbitration Report*, (11), 30-34.

Buhl, H., Fridgen, G., Keller, R., & Sedlmeir, J. (2020). The Energy Consumption of Blockchain Technology: Beyond Myth. *Business & Information Systems Engineering*, (62), 599- 608. https://doi.org/10.1007/s12599-020-00656-x

Campos Mínguez, F. (2019). *Blockchain: Aplicaciones a la administración pública* (trabajo de fin de grado). Universidad Politécnica de Valencia, Valencia, España.

Centro Internacional de Arbitraje de Madrid (2020). *Nota sobre organización de audiencias virtuales*. https://madridarb.com/wp-content/uploads/2020/10/NOTA-SOBRE-AUDIENCIA-VIRTUAL-ES-v1.pdf

Check Point Software Technologies Ltd. (2020). *Cyber Security Report 2020*. https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf

Compound (s.f.). Compound. https://compound.finance

Conejero, M., & Porxas, N. (2018). Tecnología Blockchain: funcionamiento, aplicaciones y retos jurídicos relacionados. *Actualidad Jurídica Uría Menéndez*, (48), 24-36.

Cordero Valdavida, M. (2019). Blockchain en el sector público, una perspectiva internacional. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, (16), 16-34.

Dalton, D., Kehoe, L., & Piscini, E. (2017). *Blockchain & Cyber Security*. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/Blockchain-and-Cyber.pdf

De Filippi, P., & Wright, A. (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. Social Science Research Network. http://dx.doi.org/10.2139/ssrn.2580664

Deloitte (2020). *Deloitte's 2020 Global Blockchain Survey*. https://www2.deloitte.com/content/dam/insights/us/articles/6608_2020-global-blockchain-survey/DI_CIR%202020%20global%20blockchain%20survey.pdf

Dickinson, A. (16 de noviembre de 2020). Blockchain for invoice reconciliation and dispute resolution. https://www.ibm.com/blogs/blockchain/2020/11/blockchain-for-invoice-reconciliation-and-dispute-resolution/

Diem (s.f.). Welcome to the Diem project. https://www.diem.com/en-us/

Digital Connecting Europe (s.f.). Experience the future with the European Blockchain Services Infrastructure (EBSI). https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi

El País (13 de mayo de 2020). "Hackeado" el desapacho de abogados de las estrellas de Hollywood. *El País*. https://elpais.com/gente/2020-05-13/hackeado-el-despacho-de-abogados-de-las-estrellas-de-hollywood.html

eToro (21 de noviembre de 2017). Guía sencilla y rápida de eToro sobre la cadena de bloques (blockchain). https://www.etoro.com/es/news-and-analysis/trading/guia-sencilla-y-rapida-de-etoro-sobre-la-cadena-de-bloques-blockchain/

Fundación del Español Urgente (22 de febrero de 2017). Cadena de bloques, mejor que el blockchain. *Fundéu*. https://www.fundeu.es/recomendacion/cadena-de-bloques-mejor-que-blockchain/

Gandhi, K., Potter, M., Trust, B., & Whitman, V. (2020). *Using blockchain to open up new possibilities for resolving disputes*. CMS Legal. https://cms.law/en/gbr/publication/future-facing-disputes-using-blockchain-to-open-up-new-possibilities

Gárate Rivera, L. (18 de marzo de 2021). El blockchain para la transferencia de acciones y la organización de libros sociales. *Adefinitivas*. https://adefinitivas.com/arbol-del-derecho/el-blockchain-para-la-transferencia-de-acciones-y-la-organizacion-de-libros-sociales-a-cargo-de-luisa-garate-rivera/

Gil, D. (14 de enero de 2020). The Story Behind IBM's 2019 Patent Leadership. *IBM*. https://www.ibm.com/blogs/research/2020/01/ibm-patent-leadership-2019/

Hanshi, D., Chong, Y., Karuppayah, S., Kwangman, K., & Zubaydi, H. (2019). A Review on the Role of Blockchain Technology in the Healthcare Domain. *Electronics*, *6*(8). https://doi.org/10.3390/electronics8060679

Hyperledger (s.f.). Hyperledger. https://www.hyperledger.org/

International Business Machine [IBM] (s.f. a). ¿Qué es la tecnología blockchain? https://www.ibm.com/es-es/topics/what-is-blockchaink

(s.f. b). IBM Food Trust: A new era in the world's food supply. https://www.ibm.com/blockchain/solutions/food-trust

International Council for Commercial Arbitration (2019). *ICCA-NYC Bar-CPR Protocol on Cybersecurity in International Arbitration (2020 Edition)* (The ICCA Reports No. 6). https://cdn.arbitration-icca.org/s3fs-public/document/media_document/icca-nyc_bar-cpr_cybersecurity_protocol_for_international_arbitration_-_print_version.pdf

International Court of Arbitration (2020). *Nota de orientación de la CCI sobre Posibles Medidas Destinadas a Mitigar los Efectos de la Pandemia del COVID-19*. Cámara de Comercio Internacional. https://iccwbo.org/content/uploads/sites/3/2020/05/guidance-note-possible-measures-mitigating-effects-covid-19-spanish.pdf

Juris (2018). *White Paper Version 2.0*. https://getjuris.com/publications/#whitepaper

Kumar, S. (25 de julio de 2018). How emerging technologies such as blockchain, IoT and RPA are making an impact on cyber security. *Express Computer.* https://www.expresscomputer.in/magazine/how-emerging-technologies-such-as-blockchain-iot-and-rpa-are-making-an-impact-on-cyber-security/23688/

Lis Data Solutions (s.f.). Blockchain: Contratos Inteligentes - Smart Contracts I. https://www.lisdatasolutions.com/blog/blockchain_contratos_inteligentes/

Merck (4 de mayo de 2020). Merck, IBM, KPMG and Walmart successfully complete FDA pilot program to evaluate the use of blockchain to help protect pharmaceutical product integrity. https://www.merck.com/stories/merck-ibm-kpmg-and-walmart-successfully-complete-fda-pilot-program

Pinsent Masons & Queen Mary University of London (2019). *International Arbitration Survey – Driving Efficiency in International Construction Disputes.* https://www.pinsentmasons.com/thinking/special-reports/international-arbitration-survey?pageNumber=1

R3 (s.f.). Digital trust, delivered. https://www.r3.com

Reuters Staff (14 de marzo de 2018). Panama Papers law firm Mossack Fonseca to shut down after tax scandal. *Reuters. https://www.reuters.com/article/us-panama-corruption-idUSKCN1GQ34R*

Riveroll, E. (31 de julio de 2018). La blockchain, una opción contra ciberataques. *Forbes*. https://www.forbes.com.mx/la-blockchain-una-opcion-contra-ciberataques/

Santander (12 de septiembre de 2019). Santander launches the first end-to-end blockchain bond. https://www.santander.com/en/press-room/press-releases/santander-launches-the-first-end-to-end-blockchain-bond

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. *Extropy: Journal of Transhumanist Thought*, (16), 1-10.

White & Case & Queen Mary University of London (2018). *2018 International Arbitration Survey: The Evolution of International Arbitration.* http://www.arbitration.qmul.ac.uk/media/arbitration/docs/2018-International-Arbitration-Survey---The-Evolution-of-International-Arbitration-(2).PDF

Zelada, S. (31 de julio de 2020). COVID-19, un acelerador de la transformación digital. *Deloitte.* https://www2.deloitte.com/pe/es/pages/technology/articles/COVID19-un-acelerador-de-la-transformacion-digital.html

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Reglas de CIMA para las audiencias de pruebas testificales y periciales por medios audiovisuales, Corte Civil y Mercantil de Arbitraje, de 8 de junio de 2020 (Esp.).

Libananco Holdings Co. Limited c. República de Turquía, Caso CIADI ARB/06/8, Decisión sobre cuestiones preliminares 23 de junio de 2008. https://www.italaw.com/cases/626

Hugo Sologuren Calmet

Abogado - Arbitro

Adjudicador

10.18800/themis.202101.017

DERECHO E INTELIGENCIA ARTIFICIAL EN EL MUNDO DE HOY: ESCENARIOS INTERNACIONALES Y LOS DESAFÍOS QUE REPRESENTAN PARA EL PERÚ

LAW AND ARTIFICIAL INTELLIGENCE IN TODAY'S WORLD: INTERNATIONAL SCENARIOS AND THE CHALLENGES THAT THEY REPRESENT FOR PERU

Christian Dennis Valero Quispe*
Universidad Nacional del Altiplano

There is a tendency to digitalize human activities, as evidenced by computers and the internet. In addition to this trend, there are intelligent machines capable of simulating human behavior known as artificial intelligence, whose development has caused a radical change in the application of the different branches of knowledge, including Law.

In this article, the author analyzes the irruption of intelligent systems developed in the field of Law at a national and international level, and also raises the main challenges they represent for the legal world. In addition, he argues that the mechanical part of Law will be carried out by machines, and the practical part by people; in view of which, it is no longer enough to be trained only in legal issues, it is now necessary to be trained also in technology issues, and to give greater emphasis to the subjects of argumentation and litigation. In this way, the author concludes that judges of first instance will probably be replaced by robots, but for the higher instances the decision-makers will be people (by virtue of the ideal of justice).

Keywords: Rights; challenges; artificial intelligence; international; technology.

Existe una tendencia por digitalizar las actividades del ser humano, prueba de ello son el ordenador y el internet. A esta tendencia se le suman las máquinas inteligentes capaces de simular comportamientos humanos conocidos como inteligencia artificial, cuyo desarrollo ha provocado un cambio radical en la aplicación de las distintas ramas del conocimiento, incluido el Derecho.

En el presente artículo, el autor analiza la irrupción de los sistemas inteligentes desarrollados en el campo del Derecho a nivel nacional e internacional, a su vez que plantea los principales desafíos que representan para el mundo jurídico. Adicionalmente, sostiene que la parte mecánica del Derecho será realizada por las máquinas y la parte práctica por las personas; en atención a lo cual, ya no basta solo con formarse en temas jurídicos, ahora es necesario formarse también en temas de tecnología y darle mayor énfasis a las asignaturas de argumentación y litigación. De este modo, el autor concluye que los jueces de primera instancia probablemente sean reemplazados por los robots, mas para las instancias superiores quienes deberán tomar las decisiones son las personas (en virtud del ideal de justicia).

Palabras clave: Derechos; retos; inteligencia artificial; internacional; tecnología.

* Estudiante de la Facultad de Ciencias Jurídicas y Políticas de la Universidad Nacional del Altiplano (Puno, Perú). Contador Público por la Universidad Nacional del Altiplano. Contacto: vale.peru13@gmail.com

Este artículo obtuvo el tercer puesto del Concurso de Artículos Jurídicos de Historial.pe organizado por Hiperderecho, con el apoyo de la Asociación Civil THĒMIS.

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 24 de febrero de 2021, y aceptado por el mismo el 4 de mayo de 2021.

I. INTRODUCCIÓN

El avance de la tecnología en todos los ámbitos de nuestra sociedad ha dado como resultado inventos que hacen la vida del ser humano cada día más sencilla y, a medida que pasa el tiempo, estos inventos son mejorados para realizar cada vez más funciones. Sin embargo, cuando nos ponemos a pensar en robots inteligentes capaces de realizar actividades como si fueran humanos, lo asociamos con un tema del futuro, pero lo cierto es que en la actualidad ya se han desarrollado sistemas inteligentes que simulan el comportamiento humano, los mismos que destacamos en el presente artículo.

A pesar de que la inteligencia artificial se ha desarrollado con mayor énfasis en el campo de las ciencias médicas, el Derecho no es ajeno a esta realidad, razón por la que nos vamos a centrar en los sistemas inteligentes que han sido desarrollados exclusivamente para realizar funciones en el mundo jurídico y vamos a plantear los desafíos que representan el uso de estos sistemas en el Derecho. Además, nos vamos a enfocar en áreas como los gestores normativos, desarrollo del proceso judicial, la forma de administrar justicia y la formación profesional.

Por las razones descritas, en el artículo se destaca las revoluciones industriales, a su vez que se realiza una aproximación al término inteligencia artificial y la relación que tiene con el Derecho. Asimismo, se detallan los sistemas inteligentes desarrollados a nivel internacional y los desafíos que representan en el mundo jurídico. Finalmente, se plantean escenarios para debatir sobre una posible responsabilidad en caso de que fallen los sistemas inteligentes y se formula la pregunta: ¿podrían los robots sustituir a los abogados?, dando apertura al debate jurídico sobre la materia.

II. LA CUARTA REVOLUCIÓN INDUSTRIAL

La constante evolución del ser humano lo ha llevado a desarrollar nuevas estructuras tecnológicas que van desde la invención de máquinas de vapor hasta la creación de máquinas inteligentes. No cabe duda de que estos acontecimientos han provocado cambios substanciales en la vida diaria, siendo así que, el término revolución implica un cambio radical en las esferas propias de la vida humana[1]. Según Castells, en nuestra historia se han suscitado por lo menos dos revoluciones:

> La primera comenzó en el último tercio del siglo XVIII, se caracterizó por las nuevas tecnologías como la máquina de vapor […] la segunda, unos cien años después, ofreció el desarrollo de la electricidad, el motor de combustión interna, la química basada en la ciencia, la fundición de acero eficiente y el comienzo de las tecnologías de la comunicación, con la difusión del telégrafo y la invención del teléfono (1996/2000, p. 64).

La necesidad del ser humano de hacer su vida cada vez más sencilla dio como resultado la tercera revolución industrial que, para Schwab:

> Se inició en la década de 1960. Generalmente se la conoce como la revolución digital o del ordenador, porque fue catalizada por el desarrollo de los semiconductores, la computación, la informática personal e Internet […] hoy estamos en los albores de una cuarta revolución industrial. Esta comenzó a principios de este siglo y se basa en la revolución digital. Se caracteriza por un Internet más ubicuo y móvil, por sensores más pequeños y potentes que son cada vez más baratos, por la inteligencia artificial y el aprendizaje de la máquina (2016, pp. 12-13).

A pesar de que no existe una clara diferencia entre la tercera y cuarta revolución[2], estos sucesos evidencian que la inteligencia artificial no es un tema del futuro, es un tema actual. A la par con los sistemas inteligentes, también se vienen desarrollando otros campos como la genética, nanotecnología, energías renovables, computación cuántica, algoritmos, comercio electrónico, etc. Prácticamente estamos atravesando un cambio trascendental y no podemos ser ajenos a esta realidad, siendo inevitable no preguntarse sobre los nuevos desafíos del Derecho en esta cuarta revolución.

III. INTELIGENCIA ARTIFICIAL

Las capacidades mentales del ser humano le permiten razonar, inventar, crear, aprender y todo ello como una característica propia del razonamiento. Con la cuarta revolución industrial se habla de la inteligencia artificial que, para Malpica Velasco:

> [E]s la rama de las Ciencias de la Computación que estudia el software y hardware necesarios

[1] Las revoluciones son el resultado de nuevas tecnologías, lo que ha desencadenado cambios en los sistemas económicos y estructuras sociales (Schwab, 2016, p. 12).

[2] Hablar de una tercera y una cuarta revolución resulta todavía desconcertante cuando no es muy clara la separación entre ellas y por la confusión que podría suscitarse de las concepciones o descripciones de cada autor (Beraud Martínez, 2018, p. 50).

> para simular el comportamiento y comprensión humana. El objetivo último de la IA es simular la inteligencia humana en una máquina creando robots que sean conscientes y con sentimientos reales, similares a los humanos (s.f., p. 1).

De lo anterior se entiende es que la inteligencia artificial es la creación de *hardware* y *software*[3] que simulan la comprensión humana por medio de máquinas inteligentes o concebidas como máquinas con mentes[4]. El estudio de estos procesos se realiza mediante modelos computacionales que les permite procesar, razonar, decidir y resolver como verdaderos agentes inteligentes.

De forma similar, Rusell y Norvig (2004) señalan que:

> El campo de la inteligencia artificial, o IA, va más allá: no sólo intenta comprender, sino que también se esfuerza en construir entidades inteligentes. La IA es una de las ciencias más recientes. El trabajo comenzó poco después de la Segunda Guerra Mundial, y el nombre se acuñó en 1956 […]. La IA sintetiza y automatiza tareas intelectuales y es, por lo tanto, potencialmente relevante para cualquier ámbito de la actividad intelectual humana. En este sentido, es un campo genuinamente universal (p. 1).

De ahí se desprende que la inteligencia artificial es la rama de las ciencias de la computación, que se desarrolla sobre la base de procesos y permite a la máquina realizar un razonamiento[5] para llegar a posibles decisiones como si fuera el resultado del razonamiento humano.

En la misma línea, Rich señala que "la inteligencia artificial es el estudio de cómo conseguir que las computadoras hagan las cosas que, por el momento, las personas hacen mejor" (citado en Beekman, 2005, p. 558). Es decir, la inteligencia artificial vendría a ser una máquina que, al procesar la información, podría replicar las acciones humanas y ofrecer posibles soluciones en campos económicos o sociales[6], razón por la cual el Derecho no puede ser ajeno al uso de estos sistemas inteligentes. En ese sentido, es válido plantearse la pregunta: ¿qué desafíos debe afrontar el Derecho con la llegada de la inteligencia artificial? Esta será la pregunta que se responderá en el desarrollo del artículo.

IV. DERECHO E INTELIGENCIA ARTIFICIAL

El desarrollo tecnológico implica que el Derecho contemple nuevas soluciones que orienten la convivencia al bien común y estas deben estar en armonía con los enfoques contemporáneos, por lo que, se necesita no solo de un tratamiento jurídico o técnico, sino también se requiere juristas con un nuevo pensamiento capaces de manejar los retos de un nuevo Derecho. Al respecto, Martínez García (2018) reflexiona en el extremo que:

> La mayoría de los estudios jurídicos sobre informática y robótica se orientan hacia una problemática técnica o instrumental, concibiendo a la máquina como una herramienta útil. O bien se centran en una problemática ética o de tratamiento jurídico: protección de datos, comercio electrónico, administración electrónica, amenazas a la libertad, acceso y control de usuarios, cancelación y rectificación de información, ciberseguridad, etc. […] Pero aquí interesa como desafío conceptual el impacto en la forma mental del jurista (p. 98).

En ese sentido, el cambio mental del jurista no se va a lograr solamente con una regulación normativa y que los operadores del Derecho apliquen esas normas. Un cambio mental implica reflexionar sobre el impacto de la inteligencia artificial en el Derecho y la forma de orientar la profesión como una verdadera ciencia multidisciplinaria.

La inteligencia artificial se aplica en el Derecho en áreas como "i) Modelos para la argumentación y la toma de decisiones; ii) Clasificación de textos legales; iii) Extracción de información y iv) Creación y planificación de un sistema legislativo" (Fernández & Boulat, 2015). Es así que, la información o planificación de un sistema legislativo busca codificar y hacer interactuar al usuario con la máquina, es decir, que la persona pueda realizar sus actividades con ayuda de un sistema y de esa forma pueda tomar mejores decisiones. Ello implica que

[3] El *hardware* viene a ser la parte física del sistema y el *software* viene a ser las instrucciones que le dicen al *hardware* lo que hay que hacer y cómo transformar un dato de entrada en un dato de salida (Beekman, 2005, p. 32).

[4] Una máquina inteligente es un agente que opera en medios desconocidos y al no usar solo sus conocimientos iniciales es capaz de aprender (Rusell & Norvig, 2004, p. 60).

[5] Un sistema es racional si hace lo correcto en función al ideal de inteligencia humana (Rusell & Norvig, 2004, p. 2).

[6] La cumbre 46 del Foro Económico Mundial (WEF, por sus siglas en inglés) abordó la Cuarta Revolución Industrial o Industria 4.0. Esta promete transformaciones asociadas al desarrollo, tasas de crecimiento y mejores condiciones de vida, pero también la falta de preparación y pérdida de puestos de trabajo (Beraud Martínez, 2018, p. 52).

los sistemas legales creados con algoritmos[7] sean capaces de almacenar información jurídica en una base de datos y superado la codificación de los algoritmos se daría paso a la creación de robots[8], y con ello el necesario análisis en áreas como el desarrollo del proceso, emisión de sentencias, elaboración de escritos, formación profesional, responsabilidad, entre otros.

V. DESAFÍO EN LOS GESTORES NORMATIVOS

Al existir en nuestro ordenamiento jurídico una gran cantidad de leyes, resulta necesario estructurar la legislación. Este aspecto ya ha sido realizado por medio del Sistema Peruano de Información Jurídica (en adelante, SPIJ) que vendría a ser:

> Una edición oficial del Ministerio de Justicia que contiene los textos de la legislación nacional e información jurídica debidamente sistematizada, concordada, actualizada y con herramientas de búsqueda y recuperación de información idóneas. Permite ubicar en forma rápida, los textos de normas legales a través de palabras, frases, número de norma, fecha de publicación, entre otros (Ministerio de Justicia y Derechos Humanos [MINJUS], s.f., p. 6).

Por medio del SPIJ, nuestro ordenamiento jurídico peruano se viene estructurando en una base de datos. De forma similar, la base jurisprudencial de Hiperderecho vendría a ser otra base de datos[9] que almacena casos, resoluciones y sentencias, lo que prácticamente muestra que las normas se vienen organizando por medio de sistemas.

En otras palabras, en el Perú se está trabajando con gestores que ayudan a organizar y sistematizar las normas del ordenamiento; sin embargo, cuando se pretende estudiar el Derecho comparado, se advierte que no existe un sistema único que reúna la normativa concordada y actualizada de los diferentes países. Es en este punto donde la inteligencia artificial puede desarrollar un sistema único, ya que, con el refinamiento de datos al introducir la normativa nacional e internacional, los algoritmos podrían transformar una simple base de datos a un sistema que pueda procesar consultas e identificar normas con la sola búsqueda de palabras claves. En otras palabras, crearía un sistema inteligente[10], logrando así una contribución al estudio del Derecho comparado con ayuda de la inteligencia artificial.

VI. DESAFÍO EN EL PROCESO JUDICIAL

Según San Martín Castro (2015), el proceso se define:

> Como el instrumento de carácter esencial que ostenta la jurisdicción, el Poder Judicial a través de sus órganos: juzgados y salas para la resolución definitiva e irrevocable de los conflictos intersubjetivos y sociales […]. El proceso presenta una estructura básica: existen actos de alegación y actos probatorios a cargo de las partes, necesarios para que el juez pueda juzgar y aplicar el derecho objetivo a los casos concretos, esto es, preservar el ordenamiento jurídico, tutelando efectivamente los derechos e intereses de todos, lo que revela su pleno carácter instrumental (pp. 38-39).

En otras palabras, el proceso es el instrumento mediante el cual el juez puede aplicar el Derecho y mediante una sentencia logra resolver los conflictos. No obstante, para ello se requiere que previamente las partes realicen actos de alegación y actos probatorios, siendo así que este modelo se caracteriza por el predominio de la palabra hablada en virtud del principio de oralidad.

Ahora bien, para garantizar que las partes tomen conocimiento de las distintas actuaciones procesales, el desarrollo del proceso se orientó al uso de las tecnologías como la aplicación de sistemas informáticos para el seguimiento de las resoluciones, las notificaciones electrónicas, portales interactivos. En la actualidad, producto de la pandemia del COVID-19, las audiencias se llevan a cabo de manera virtual. Por ejemplo, ahora el proceso se viene desarrollando con los medios informáticos de notificación, portales de consulta de expedientes y videoconferencias.

Es por esta razón que el desafío posterior al uso de medios informáticos va a implicar un cambio integral en la reingeniería procesal, lo que significa una

---

7 Un algoritmo es un lenguaje informático que permite transformar un problema a un programa mediante un proceso de refinamiento de datos desde las ideas principales hasta los detalles concretos, el resultado de la programación es un algoritmo (Beekman, 2005, p. 516).

8 Los robots son agentes físicos que realizan tareas mediante la manipulación física. Para realizar sus actividades están equipados de piernas, ruedas, pinzas y sensores como cámaras y giroscopios (Rusell & Norvig, 2004, p. 1023).

9 Una base de datos es un sistema de archivo electrónico donde la información está almacenada y organizada en un programa de tal forma que se pueda recobrar, actualizar, insertar y borrar la información (Gutiérrez Díaz, 2010, p. 10).

10 Entendido como un soporte de inteligencia donde el razonamiento no está en las personas sino en los componentes constitutivos del sistema (Martínez García, 2018, p. 108).

transformación de los actuales modelos procesales a un modelo inteligente donde se pueda llevar a cabo actividades como las que Corvalán (2019) plantea:

> Apenas ingresa un escrito que acredita personería junto a la copia digital de un poder, el sistema en pocos segundos podría detectar y elaborar un despacho que tenga por acreditada la personería [...] dialogar con el presentante, a fin de advertirle acerca de posibles errores existentes. Por ejemplo, que adjuntó un poder en donde no figura la persona que afirma ser apoderada [...] segmentar y clasificar por trámites más urgentes [...] sugerirle al operador judicial un orden de prioridad de los expedientes pendientes de control y firma [...] automatizar sin intervención humana, resoluciones judiciales simples como vistas, traslados, pases y notificaciones (pp. 10-11).

Las actividades que plantea Corvalán no es solo doctrina. A nivel internacional, el Ministerio Público Fiscal de Buenos Aires ha desarrollado PROMETEA, un sistema capaz de elaborar 1000 dictámenes jurídicos en solo 45 días, tiempo el cual hubiese aumentado a 174 si no se hubiese empleado el sistema. Para el caso de ejecuciones fiscales, en un mes se puede realizar 225 resoluciones; no obstante, con PROMETEA se podría alcanzar 1440 en el mismo periodo. Asimismo, en el Registro Civil de Buenos Aires ingresan al año 6000 rectificaciones partidarias, con PROMETEA se atendieron estas rectificaciones en dos meses, cuando antes demoraban ocho. Cabe resaltar que con la intervención humana el sistema inteligente fue capaz de leer, analizar, detectar y sugerir casos prioritarios sobre derecho a la salud en menos de dos minutos, algo que para una persona humana le hubiera llevado 96 días hábiles de trabajo (Abogados.com.ar, 2019).

PROMETEA no es el único caso. En Alemania, en las universidades de Heidelberg y Darmstadt, se ha desarrollado JUDITH, un sistema experto[11] capaz de aplicar el Código Civil alemán. Este sistema experto jurídico[12] es entendido por Martínez Bahena (2013) como:

> [U]n sistema computacional que puede plantear posibles soluciones a determinados asuntos jurídicos aplicando el conocimiento experto en la materia [...] o puede ser usado como herramienta de apoyo para los operadores jurídicos en contextos tales como la asesoría, asistencia legal o la función jurisdiccional (p. 833).

El caso de JUDITH evidencia que el uso de sistemas expertos en el Derecho es una realidad. En ese sentido, el desafío en el desarrollo del proceso judicial implica hacer uso de estos sistemas inteligentes como PROMETEA, de tal manera que se logre transformar el clásico modelo, en donde se advierte una alta carga procesal, a un sistema secuencial, rápido, estructurado y sobre todo dinámico.

VII. DESAFÍO EN LA ADMINISTRACIÓN DE JUSTICIA

En la actualidad quien emite una sentencia es un ser humano que ostenta la función de magistrado, sin embargo, debemos preguntarnos: ¿puede la inteligencia artificial emitir sentencias? Para responder esta pregunta, planteamos un caso internacional de un sistema experto de sentencias, en el cual su creadora (la doctora María del Socorro Téllez Silva) diseñó un sistema de apoyo a los jueces de familia. En este, el sistema inteligente relaciona la lógica y el razonamiento jurídico, y es capaz de emitir una posible sentencia como si fuera un operador de justicia. Sobre este sistema experto en sentencias, Martínez Bahena (2013) destaca que:

> Para probar la estabilidad del sistema se presentó este prototipo ante dos jueces de lo familiar para que emitieran su opinión en dos rubros. El primero se refiere a la facilidad de operar el sistema y, el segundo, a si el sistema emitió una solución similar a la que ellos emitirían sin ayuda del programa. Como respuesta a la primera pregunta recomendaron la elaboración de un manual de usuario. Por lo que se refiere a la segunda pregunta, manifestaron que no se presentó mayor complicación para resolver lo que en derecho corresponda; sin embargo, consideraron que deben idearse programas combinados debido a que los litigantes, generalmente, ejercitan más de una pretensión (pp. 844-845).

Respecto a la primera pregunta que se refiere a la facilidad para operar el sistema, los jueces recomendaron la elaboración de un manual de usua-

[11] Es un conjunto de procedimientos lógicos de inteligencia artificial que permite a la computadora analizar situaciones y adoptar posibles decisiones (De Trazegnies Granda, 2013, p. 116).

[12] Nos referimos a programas de computación que actúan como consultores o asistentes inteligentes en la búsqueda de una solución a un problema legal (De Trazegnies Granda, 2013, p. 122).

rio[13]. Ello debe hacernos reflexionar en el extremo de que el Derecho no es solo normas, sino es una ciencia multidisciplinaria, y como tal la preparación de los estudiantes y juristas ahora deben darle mayor énfasis al manejo de programas, sistemas y algoritmos inteligentes. En otras palabras, el desafío para los próximos magistrados, además de formarse en la ciencia jurídica, es ahora una formación en el manejo de sistemas computacionales, pues de lo contrario va a resultar complicado operar sistemas expertos, aun con la ayuda de un manual de usuario.

Con relación a la segunda pregunta sobre la emisión de la resolución, debemos precisar que la sentencia emitida por el sistema fue similar a la que los jueces hubiesen emitido. Ello implica que las pruebas piloto en la administración de justicia ya se están llevando a cabo mediante sistemas inteligentes. El perfeccionamiento de estos sistemas expertos en sentencias implicaría su presencia en los distintos juzgados. En todo caso, la preparación en temas de inteligencia artificial son desafíos a los que debemos responder desde la formación universitaria.

VIII. DESAFÍO EN LA FORMACIÓN PROFESIONAL

El Derecho demanda formación, experiencia y adoctrinamiento en la justicia, y esto no se manifiesta solo con el ordenamiento jurídico, sino que exige una preparación en todas las ramas. Al respecto, el maestro Couture (s.f.) indica que "estudia: el Derecho se transforma constantemente. Si no sigues sus pasos, serás cada día un poco menos abogado". Este primer mandamiento del abogado exige una constante actualización, ya que al Derecho cada día se le suman leyes, resoluciones, doctrina, jurisprudencia y ahora temas de tecnología.

Un Derecho cada vez más inteligente exige que la sociedad esté en permanente contacto con la inteligencia artificial. En esa línea, Ocaña, Valenzuela y Garro-Aburto (2019) señalan que:

> En la formación universitaria se pone énfasis en el diseño de perfiles profesionales que se enmarquen al trabajo y la generación de conocimiento [...] pero bien ¿hay una vertiente diáfana en los contextos de la educación superior que se enfoquen a los cambios que se suscitan en los nuevos retos sustentados en la educación digital?; ¿cuál es el perfil, y que competencias deberá de desarrollar el estudiante inmerso en el mundo virtual? (pp. 542-543).

Sin duda la respuesta a estas preguntas es la oralidad; debido a que, con un sistema capaz de tomar decisiones como si fuera una inteligencia humana, los escritos y las actuaciones procesales se van a realizar de forma mecánica y la parte práctica por el jurista.

A nivel internacional, según explica De Trazegnies Granda, "la Universidad de Harvard implementó un curso sobre la aplicación de la inteligencia artificial al Derecho, a fin de reclutar futuros investigadores" (2013, p. 122). Este escenario muestra que los estudiantes del Derecho ya se vienen formando desde la universidad en inteligencia artificial y si a ello le sumamos los sistemas expertos en sentencias, nos damos cuenta de que aprender Derecho ya no va a consistir en aprender contenidos, sino va a significar un aprendizaje en argumentación.

Así, la parte teórica va a ser realizada por las máquinas inteligentes y la parte filosófica por los juristas. En virtud de lo cual, las actuales facultades de Derecho del país deben cambiar su estructura curricular e incluir temas de tecnología, sistemas computacionales e inteligencia artificial, así como darle énfasis a las asignaturas de argumentación y litigación jurídica.

IX. ROBOT ROSS

Los sistemas inteligentes aplicables al Derecho no se están discutiendo en nuestro país o, por lo menos, no en la medida que se debería. No cabe duda de que esta situación debe cambiar, ya que la inteligencia artificial no es un tema del futuro que va a ocurrir de aquí a unos años, sino es una situación actual. Por ejemplo, en Estado Unidos se ha contratado la inteligencia artificial ROSS, el cual es considerado el primer abogado robot, puesto que es un sistema capaz de absolver consultas y emitir una respuesta más rápida que un abogado humano.

Según explica Chuquicallata Reategui (2018):

> Este software fue creado por una startup[14] canadiense de la Universidad de Toronto. Los investigadores utilizaron la tecnología del superordenador Watson, desarrollado por la International Business Machines Corporation (IBM)" (2018).

[13] El manual de usuario es un documento que explica cómo hacer determinadas tareas (Rusell & Norvig, 2004, p. 744).

[14] *Startup* es una empresa que comercializa productos y/o servicios a través del uso de las Tecnologías de la Información y la Comunicación (TIC) (Fernández, s.f.).

ROSS es capaz de responder preguntas legales en tiempo real y no solo ofrece respuestas acertadas, sino que además puede analizar sentencias y advertir riesgos o ventajas ante una posible estrategia legal. Tales son las ventajas que ofrece este abogado robot que ya ha sido contratado por despachos jurídicos, tal como destaca Chuquicallata Reategui (2018):

> En 2016, la prestigiosa firma estadounidense, Baker & Hostetler, contrató a ROSS para que forme parte del Departamento de Gestión de Quiebras, junto a un numeroso equipo de 50 abogados humanos. Según aseguran sus fundadores, la compañía decidió contratar a esta inteligencia artificial como abogado para formular hipótesis y fundamentarlas con citas de leyes o precedentes legales. Los responsables de la firma explicaron que no son los únicos en haber contratado los servicios de este abogado artificial.

A pesar de que ROSS Intelligence[15] cerró sus operaciones el 31 de enero de 2021[16], el hecho de que una inteligencia artificial como ROSS haya sido contratado en despachos de abogados para que pueda participar del mundo jurídico, mediante la formulación de una opinión legal, debe hacernos reflexionar sobre el futuro de la profesión y, sobre todo, cambiar el pensamiento de un Derecho clásico por el de un Derecho inteligente.

ROSS no es el único sistema inteligente capaz de adentrarse al mundo legal. Otro caso a nivel internacional es RAVN, el cual es un sistema de inteligencia artificial que ha logrado destapar un presunto fraude de sobornos en Reino Unido. En esa línea, Hernández (2019) señala que:

> Ross, de IBM está programado para procesar y utilizar el lenguaje natural y también es capaz de formular hipótesis para responder a las preguntas planteadas, utilizando la jurisprudencia. Algo similar hace RAVN, famoso por haber contribuido a destapar un fraude en una conocida marca de automóviles, al haber sido capaz de analizar 600,000 documentos al día. Es prácticamente impensable lo que le habría costado analizar a una persona esa cantidad de documentos (p. 807).

Casos como los de ROSS y RAVN evidencian que la inteligencia artificial ha logrado optimizar los recursos y la productividad. Ambos sistemas inteligentes son capaces de emplear conocimientos jurídicos y ofrecer una asistencia al abogado; por lo cual, el desafío para los próximos profesionales del Derecho debe ser formarse en inteligencia artificial y no esperar a que estos robots inteligentes cambien el Derecho como lo conocemos.

X. REALIDAD INTERNACIONAL

A nivel internacional existen otros sistemas inteligentes que ya se usan en el mundo jurídico. En España, por ejemplo, se tienen sistemas inteligentes como Vlex Analytics, que es un sistema que ayuda a predecir los casos en litigio, lo cual se logra mediante un análisis de los juzgados y tribunales; Jurimetría, que es un programa inteligente que reúne millones de resoluciones judiciales y, sobre la base de los fundamentos expresados en las resoluciones, permite tomar decisiones; Legal Data, sistema inteligente que está diseñado para introducir datos del proceso y es capaz de predecir los resultados de los litigios; o como el sistema Tirant Analytics, que analiza los hechos y es capaz de ofrecer posibles estrategias legales, así como el porcentaje de éxito de cada una de ellas (Noticias Jurídicas, 2016).

Por otro lado, en Estados Unidos el Consejo de la Abogacía Norteamericana (ABA por sus siglas en inglés) aprobó una reforma en sus modelos de normas de conducta profesional, estableciendo que los abogados deben ser competentes no solo en conocimientos legales, sino también en tecnología. Asimismo, el Colegio de Nuevo Hampshire, en materia de *cloud computing*[17], ha establecido que los abogados tengan conocimientos básicos en tecnología. En forma similar, el Colegio de California, en su Formal Opinion 2015-193, concluye que la carencia de conocimientos tecnológicos puede convertir a un abogado en éticamente incompetente (Noticias Jurídicas, 2016). En otras palabras, hasta cierto punto, se puede afirmar que en Estados Unidos indirectamente se obliga a los abogados a formarse y ser competentes en temas de tecnología.

En España se usan los *smart contracts*[18] –que se ejecutan sobre la plataforma de los Ethereum, la cual se basa en *blockchain–,* estos son contratos inteligentes que se llevan a cabo de manera automática, previo acuerdo de los términos y condicio-

[15] Traducido al español como inteligencia.

[16] En el 2020 Thomson Reuters y Westlaw presentaron una demanda contra ROSS. Los costosos litigios ocasionaron que sea difícil soportar el proceso, lo que a su vez no ha hecho posible recaudar financiación para seguir impulsando el proyecto (ROSS, 2020).

[17] Traducido al español como computación en la nube.

[18] Traducido al español como contratos inteligentes.

nes de las partes. Adicionalmente, se tienen los *ChatBot* Jurídicos, que son programas informáticos usados en estudios de abogados con los cuales se puede mantener una conversación como si fuera el propio abogado del despacho quien atiende a las preguntas formuladas por el usuario.

En Francia, se ha desarrollado CARAF, sistema que supervisa y trata de armonizar la acción de las cajas regionales de asignaciones familiares. En Gran Bretaña, existe ACCI de la Universidad de Manchester, que proporciona medios para interpretar la legislación en materia de impuestos. En Italia, se encuentran PROVA y CONSULENZA de la Universidad de Milán, sistemas que facilitan la aplicación de la ley por medios interactivos. En Noruega, se utiliza SARA para ayudar en las decisiones discrecionales. Finalmente, en Alemania, en la Universidad de Tubinga se trabaja en el sistema experto relativo al Código Penal alemán para proyectar la resolución de casos (Britos, Sierra & García, 2004).

Estos casos internacionales muestran que la inteligencia artificial ya se está aplicando en el mundo jurídico, siendo un desafío para el Perú su análisis y la implementación de las medidas pertinentes para hacer frente a estos cambios.

XI. DEBATE SOBRE LA RESPONSABILIDAD EN EL USO DE SISTEMAS INTELIGENTES

Con el acelerado desarrollo de la robótica y los sistemas inteligentes resulta necesario iniciar un debate sobre la legislación específica en inteligencia artificial. En el Perú, no existe una normativa que regule estos asuntos. Quizá porque aún los sistemas inteligentes no han provocado cambios en nuestros modelos de vida, ni en el Derecho peruano, pero, con los casos internacionales citados en los apartados precedentes, es necesario plantear escenarios donde se vea involucrado el ser humano y un robot.

Estos escenarios deben abordarse desde dos aristas: primero, plantear un razonamiento sobre quién tendría la responsabilidad en el caso de que se lesione o se ponga en peligro un bien jurídico tutelado por la ley; y segundo, evidenciar la necesidad de una legislación específica respecto de máquinas inteligentes.

La robótica[19] da apertura a un mundo inteligente, clasificando a los robots por niveles: en el primer peldaño, se ubican los sistemas programados, que son sistemas que ayudan en la realización de tareas automatizadas; seguido de los robots no autónomos, que a nivel de construcción son robots pero realizan tareas simples sin asistencia humana; en el tercer nivel, se ubican los robots autónomos, quienes tienen capacidad autónoma para realizar tareas complejas y en el último nivel se ubica la inteligencia artificial, que son máquinas que perciben el ambiente externo sin necesidad de órdenes programadas (Torres Manrique, 2017, pp. 213-214).

Los sistemas programados actualmente se utilizan en nuestro país. Prueba de ello es el Derecho informático que ha resuelto controversias con ayuda de una página web[20]. Con relación a los robots no autónomos, este tipo de robots son los que realizan actividades sencillas y están representados por los actuales sistemas tecnológicos de asistencia en el hogar o robots que se dedican a la limpieza. Sin embargo, los dos últimos niveles, es decir, los robots autónomos y la inteligencia artificial son los sistemas que merecen un análisis minucioso debido a que un error en el sistema inteligente podría provocar lesiones o posibles afectaciones a bienes jurídicos y daría lugar a un debate sobre responsabilidades.

Respecto del tercer nivel, el término robots autónomos es entendido por Torres Manrique (2017) como:

> [A]quellos que tienen capacidad de desarrollar tareas encomendadas complejas, listando las mismas, priorizando, tomando o creando sus propias decisiones con libertad dentro de su ámbito de trabajo [...] sin necesidad de asistencia humana, con suficiente autonomía para que con base en una orden dada por un operador humano realice las tareas según lo considere más adecuado o efectivo para el cumplimiento de dicho objetivo (pp. 213-214).

Este tipo de robots que toman decisiones sin necesidad de asistencia humana, en la actualidad están representados por los automóviles autónomos. Estos son vehículos configurados para tomar el control de la conducción, es decir, la persona puede viajar y es el sistema del vehículo quien lleva a cabo el manejo, particularmente es el robot el que está configurado para operar las funciones del vehículo. Precisamente, esta autonomía constituye la base para debatir sobre la responsabilidad y el dilema en caso de que el sistema informático falle.

[19] Es una disciplina que se ocupa del diseño de robots, basado en tres categorías: robots manipuladores, móviles y humanoides (Rusell & Norvig, 2004, pp. 1023-1024).

[20] Véase el siguiente caso que se resolvió con ayuda de una página web (Resolución 1898-2014/SPC-INDECOPI, 2014).

Por ejemplo, en Arizona un volvo operado por un sistema informático presentó fallas en sus algoritmos y, producto de ello, perdió la vida un peatón (Iglesias, 2018). Por otro lado, también hubo otros casos como el del sistema de asistencia de piloto automático de Tesla, ocurrido en California, en el cual el conductor murió en un accidente de tráfico por las decisiones autónomas del sistema de manejo de autopiloto, pues el sistema había errado en su interpretación de las líneas de separación de carriles (Merino, 2019). Caso similar al ocurrido en Florida, donde el vehículo en conducción automática se impactó contra un camión ocasionando la muerte del conductor (El País, 2019).

Ante estos casos, surge la pregunta, ¿quién tiene la responsabilidad por lo acontecido? ¿el conductor que no tenía sus manos en el volante a pesar de estar en piloto automático? ¿el diseñador del vehículo autónomo? ¿la persona que programó el sistema para que el automóvil tome decisiones independientes? ¿el diseñador del *software*? ¿la empresa distribuidora? o nadie tiene la responsabilidad por los hechos.

Al encontrarnos frente a este dilema, consideramos que no podría haber un solo responsable. Si el piloto automático exige que el conductor esté atento en todo momento, ello implicaría que la responsabilidad es del conductor. No obstante, si hay una falla técnica en el *software*, existiría una responsabilidad por quienes programaron el sistema. Por otro lado, si el piloto automático funciona de manera independiente con un *software* que opera de forma autónoma o si depende de un usuario la configuración de los algoritmos, además de una responsabilidad penal, estaríamos frente a una responsabilidad civil. En otro extremo, si el resultado de la muerte fue producto de la intervención de un tercero quien manipuló o provocó intencionalmente la falla en el sistema, la responsabilidad sería de este tercero.

Así pues, es necesario precisar que solo con el tema de los vehículos autónomos surge todo un dilema en el mundo jurídico. Entonces, si solo con el tercer nivel encontramos estas dificultades, con mayor razón resulta necesario analizar responsabilidades en el uso de la inteligencia artificial.

Con relación al último nivel de la robótica, para Torres Manrique, la inteligencia artificial "son aquellos sistemas mecánicos que perciben el ambiente externo por sí mismos sin necesidad de órdenes pre programadas externas, con capacidad para discernir diferentes circunstancias que acontezcan a su alrededor y con capacidad para moverse de forma voluntaria" (2017, p. 214). En ese sentido, aquellos sistemas que puedan discernir circunstancias y actuar de forma autónoma serán considerados inteligencia artificial.

El dilema jurídico surge en posibles fallas que puedan resultar producto de los procedimientos que realizan los sistemas inteligentes. Por ejemplo, en Reino Unido se creó el sistema Digital Surgery[21], que está diseñado para salas de cirugía por medio de una directriz en los procedimientos con el objetivo de realizar una cirugía más segura. No obstante, en el supuesto de que fallen los algoritmos y la cirugía produzca la muerte de una persona, ¿quién tendría la responsabilidad por los hechos? ¿el médico que confió en el sistema inteligente? ¿la persona que programó el sistema? ¿el director del hospital por contratar la inteligencia artificial? ¿el proveedor del servicio? ¿el diseñador del software?

Ante estas interrogantes, no hay una respuesta jurídica. Probablemente, el razonamiento sería similar al de los robots autónomos, pero, a diferencia del tercer nivel, debemos tomar en cuenta que la inteligencia artificial es el último nivel de la robótica donde los sistemas inteligentes son capaces de simular el actuar humano, lo que evidencia aún más la necesidad de una regulación específica. En todo caso, aunque parezca prematuro discutir sobre una legislación específica en inteligencia artificial, es necesario abordar con prontitud estos dilemas jurídicos.

Los casos de robots autónomos y máquinas inteligentes evidencian que el Perú no está preparado normativamente para hacer frente a estos sistemas inteligentes. En efecto, con la normativa actual de nuestro país, para determinar un perjuicio tendríamos que remitirnos a las reglas de los daños en materia civil o a las responsabilidades en materia penal. Por tanto, resulta necesario contar con una normativa específica sobre la materia. Las máquinas inteligentes no son temas del futuro, son cambios que ya están ocurriendo y van a ocurrir aún más, lo que va a representar un desafío para los legisladores, juristas, estudiantes del Derecho y demás profesionales.

XII. ¿PODRÍAN LOS ROBOTS SUSTITUIR A LOS ABOGADOS?

El internet[22] y el ordenador dejaron obsoletos los trabajos manuales y ahora, con la cuarta revolu-

[21] Traducido al español como cirugía digital.

[22] El internet es un sistema de redes de alcance global. En 1969 se construyó la red experimental ARPANET que más adelante dio vida a internet (Beekman, 2005, p. 42).

ción industrial por medio de los sistemas inteligentes, la probabilidad de que puestos de trabajo sean reemplazados por los robots es cada vez mayor. En todo caso, ¿qué puestos de trabajo podrían ser reemplazados en el campo del Derecho?

A pesar del avance de la inteligencia artificial como los casos analizados en el desarrollo del artículo, consideramos que no se podría reemplazar todo el aparato jurídico, pero existe la posibilidad de reemplazar puestos de trabajo como el de los analistas de jurisprudencia, asistentes judiciales, notificadores y quizá jueces en primera instancia.

De Trazegnies Granda (2013) reflexiona sobre el reemplazo de jueces e indica que:

> [P]odríamos imaginar un sistema experto que, por sí sólo, sin participación de juez alguno, emitiera una sentencia debidamente fundamentada en primera instancia. En una gran parte de los casos, esta opción adoptada por la inteligencia artificial sería difícilmente discutible [...] sin embargo, a nivel de las instancias superiores, las resoluciones en apelación o casación corresponderían necesariamente a jueces (p. 129).

Coincidimos con De Trazegnies Granda, ya que un sistema experto, en este caso uno experto en sentencias, como el analizado en apartados anteriores, sería el reemplazo de los jueces. Sin embargo, por mucho que este sistema alivie la carga procesal y pueda emitir sentencias fundamentadas, el ser humano como portador del ideal de la justicia siempre debe salvaguardar las decisiones en última instancia a través de su razonamiento, no para evitar el reemplazo de los jueces, sino más bien, porque la justicia va más allá del desarrollo de algoritmos.

Asimismo, añade De Trazegnies Granda (2013) que:

> [L]as sentencias IA (inteligencia artificial) emitidas en primera instancia llegarían al nivel superior con un razonamiento muy trabajado por la computadora, facilitando la comprensión del problema. De otro lado, el juez del segundo nivel tendría a su vez la ayuda de un sistema experto, no para emitir la sentencia sino para facilitarle al tribunal toda la información precisa que requiere en materia de doctrina, legislación, etcétera y también para hacerle ver los diferentes caminos entre los que puede optar (p. 130).

Por otro lado, Dans (2018) afirma que:

> Resulta fuera de toda duda que muchas de las tareas que hoy lleva a cabo un abogado serán desempeñadas en el futuro por algún tipo de aplicación de la inteligencia artificial [...] No nos planteemos si la tecnología nos va a dejar o no sin trabajo: planteémonos cómo podemos mejorar nuestro trabajo con ella. Y de paso, cómo podemos mejorar la sociedad (p. 16).

Esta última reflexión debe ser la nueva mentalidad de los abogados. No hay que preocuparse por los trabajos que puedan ser reemplazados por los robots; mejor preocupémonos en cómo mejorar nuestra vida, el Derecho, la convivencia y, sobre todo, el bien común con ayuda de la inteligencia artificial.

Guardiola Salmerón (2018) añade que "la lejana posibilidad de atribuir derechos o incluso personalidad a entidades no humanas será un complejo debate, y un largo camino por recorrer, pero sin duda supondrá un auténtico desafío jurídico hasta ahora inimaginable" (p. 12).

Nuestra profesión y el país deben enfrentar estos desafíos ahora y no esperar un cambio abrupto en los modelos clásicos del ejercicio del Derecho. Plantear estos postulados no implica reemplazar a los abogados, se trata de complementar el Derecho con la inteligencia artificial para así reforzar el sistema jurídico. Finalmente, será el abogado quien tome las decisiones que los sistemas inteligentes puedan ofrecer. Definitivamente la evolución de la justicia a una inteligente va a cambiar nuestra profesión y la percepción que tenemos del Derecho. Será un largo debate y un auténtico desafío jurídico.

XIII. CONCLUSIONES

La inteligencia artificial es la rama de las ciencias de la computación que estudia el *hardware* y *software* con el objetivo de simular la comprensión humana. Para ello, crea máquinas inteligentes que son capaces de procesar información, replicar las acciones humanas sin necesidad de órdenes preprogramadas externas, discernir ante circunstancias que ocurren a su alrededor y actuar en forma voluntaria. Con la cuarta revolución industrial, nuestra forma de entender, aplicar y ejercer el Derecho debe cambiar para adaptarnos a los desafíos que exige la llegada de los sistemas inteligentes.

El ordenamiento jurídico se ha organizado y estructurado a través de las bases de datos donde la información normativa está almacenada en un programa como es el caso del SPIJ; sin embargo, con la inteligencia artificial el desafío implicaría desarrollar un sistema único donde se almacene la normativa nacional e internacional para transformar una simple base de datos a un sistema inteligente que contribuya al estudio del Derecho comparado.

Respecto al desarrollo del proceso, el sistema inteligente PROMETEA, que es capaz de elaborar dictámenes jurídicos, ejecuciones fiscales y analizar documentación en tiempos inferiores a los que podría realizar una persona, contribuiría en la reducción de la carga procesal. Con relación a la administración de justicia, el sistema experto JUDITH, que es capaz de aplicar el Código Civil alemán, o el sistema experto en sentencias de la doctora María del Socorro Téllez Silva brindarían un apoyo a los magistrados, lo que implicaría como desafío además de formarse en temas jurídicos ahora es necesario una formación en inteligencia artificial para poder operar estos sistemas inteligentes.

Por otro lado, en la Universidad de Harvard se implementó el curso de aplicación de la inteligencia artificial al Derecho con el objetivo de reclutar futuros investigadores, lo que evidencia que, a nivel internacional, los estudiantes ya se vienen formando en inteligencia artificial.

Ahora bien, PROMETEA y JUDITH evidencian que la parte mecánica del Derecho va a ser realizada por las máquinas y la parte práctica por las personas, siendo el desafío modificar las mallas curriculares y formarse desde la universidad en sistemas inteligentes y darles énfasis a las asignaturas de argumentación y litigación jurídica.

A nivel internacional el Derecho ya está trabajando con sistemas inteligentes, prueba de ello es que en Estados Unidos se contrató en los despachos a ROSS, considerado el primer abogado robot y en Reino Unido, RAVN ha logrado destapar presuntos sobornos. Asimismo, existe en España Vlex Analytics, que ayuda a predecir casos en litigio; Jurimetría, que reúne resoluciones judiciales y ayuda a tomar decisiones; Legal Data, que predice resultados de los litigios; y Tirant Analytics, que muestra el porcentaje de éxito de las estrategias legales; CARAF en Francia, que opera en las cajas regionales de asignaciones familiares; y ACCI en Gran Bretaña, que interpreta la legislación de impuestos, ello por nombrar algunos ejemplos.

El debate sobre la responsabilidad en el caso de que fallen los sistemas inteligentes da apertura a un dilema para determinar quién tendría la responsabilidad por los hechos fallidos. Esto, sin lugar a dudas, evidencia la necesidad de contar con una legislación específica en inteligencia artificial. A pesar de que pueda parecer prematuro en el Perú plantear normas al respecto, los escenarios internacionales muestran que la aplicación en el Derecho está cambiando y teniendo en cuenta el acelerado desarrollo de sistemas inteligentes es necesario contar con normas específicas sobre la materia.

Con el desarrollo de sistemas expertos en sentencias, probablemente el magistrado de la primera instancia sea reemplazado por un robot. Sin embargo, para las instancias superiores quien debe tomar las decisiones debe ser la persona, puesto que con el apoyo del sistema inteligente se tendría mayor comprensión del caso y se necesitaría el razonamiento humano, no para evitar el reemplazo de los magistrados, sino más bien, porque la justicia va más allá del desarrollo de algoritmos.

REFERENCIAS

Abogados.com.ar (27 de mayo de 2019). PROMETEA: el primer sistema de inteligencia artificial predictivo de la justicia se presenta en "Mundial de Inteligencia artificial". *Abogados.com.ar.* https://abogados.com.ar/prometea-el-primer-sistema-de-inteligencia-artificial-predictivo-de-la-justicia-se-presenta-en-el-mundial-de-inteligencia-artificial/23523

Beekman, G. (2005). *Introducción a la Informática.* Pearson Educación.

Beraud Martínez, I. (2018). Cuarta revolución industrial - Impacto de la inteligencia artificial en el modo de producción actual. *Revista Conjeturas Sociológicas*, *6*(16), 43-57.

Britos, P., Sierra, A., & García Martínez, R. (2004). Sistema de asistencia legal en riesgos de trabajo. *Journal Informática y Sociedad*, *1*(1), 34-49.

Castells, M. (2000). *La era de la información: economía, sociedad y cultura* (C. Martínez & J. Alborés, trad.). Alianza Editorial. (Obra original publicada en 1996).

Chuquicallata Reategui, F. (5 de setiembre de 2018). Ross, el primer abogado robot que litiga usando inteligencia artificial. *LP Pasión por el Derecho*. https://lpderecho.pe/ross-primer-abogado-robot-litiga-usando-inteligencia-artificial/

Corvalán, J. (9 de septiembre de 2019). El impacto de la IA en el Derecho Procesal. *DPI Cuántico*. https://dpicuantico.com/2019/09/09/el-impacto-de-la-ia-en-el-derecho-procesal/

Couture, E. (s.f.). *Los mandatos del abogado.* http://www.justiciayderecho.org.pe/revista2/articulos/LOS%20MANDAMIENTOS%20DEL%20ABOGADO%20eduardo.pdf

Dans, E. (2018). ¿Sustituirán las máquinas a los abogados? *Revista Abogacía Española*, (108), 16.

De Trazegnies Granda, F. (2013). ¿Seguirán existiendo jueces en el futuro?: El razonamiento judicial y la inteligencia artificial. *Ius et Veritas*, (47), 112-130.

El País (17 de mayo de 2019). Tesla reconoce otro accidente mortal en un vehículo que circulaba con piloto automático. https://elpais.com/tecnologia/2019/05/17/actualidad/1558075375_210626.html

Fernández, C., & Boulat, P. (10 de abril de 2015). Inteligencia Artificial y Derecho. Problemas y perspectivas. *Noticias Jurídicas*. https://noticias.juridicas.com/conocimiento/articulos-doctrinales/10061-inteligencia-artificial-y-derecho-problemas-y-perspectivas/#_Toc416175199

Fernández, H. (s.f.). ¿Qué es una startup? *Economía TIC*. https://economiatic.com/que-es-una-startup/

Guardiola Salmerón, M. (2018). Retos, desafíos y nuevas oportunidades. *Revista Abogacía Española*, (108), 10-13.

Gutiérrez Díaz, A. (2010). *Base de datos.* Centro Cultural Itaca S.C. https://www.aiu.edu/cursos/base de datos/pdf leccion 1/lección 1.pdf

Hernández, M. (2019). Inteligencia Artificial y Derecho Penal. *Actualidad Jurídica Iberoamericana*, (10), 792-843.

Iglesias, D. (19 de marzo de 2018). Primer atropello mortal de un vehículo sin conductor. *El Mundo*. https://www.elmundo.es/motor/2018/03/19/5aaff150e2704ec82e8b463f.html

Malpica Velasco, J. A. (s.f.). *Inteligencia Artificial y conciencia*. http://www3.uah.es/benito_fraile/ponencias/inteligencia-artificial.pdf

Martínez Bahena, G. C. (2013). La inteligencia artificial y su aplicación al campo del Derecho. *Alegatos-Revista Jurídica de la Universidad Autónoma Metropolitana*, *26*(82), 827-846.

Martínez García, J. I. (2018). Derecho inteligente. *Cuadernos Electrónicos de Filosofía del Derecho*, (37), 95-114. https://doi.org/10.7203/CEFD.37.11440

Merino, M. (03 de mayo de 2019). Tesla, demandada por la familia del conductor que murió en accidente de tráfico mientras viajaba con el Autopilot activado. *Xataca*. https://www.xataka.com/inteligencia-artificial/tesla-demandada-familia-conductor-que-murio-accidente-trafico-viajaba-autopilot-activado

Ministerio de Justicia y Derechos Humanos [MINJUS] (s.f.). *Manual de usuario. Sistema Peruano de Información Jurídica*. http://spij.minjus.gob.pe/manuales/ManualUsuario.pdf

Noticias Jurídicas (05 de septiembre de 2016). ¿Se pueden exigir conocimientos de tecnología a los abogados? *Noticias Jurídicas*. https://noticias.juridicas.com/actualidad/noticias/11285-iquest;se-pueden-exigir-conocimientos-de-tecnologia-a-los-abogados/

Ocaña, Y., Valenzuela, L., & Garro-Aburto, L. (2019). Inteligencia artificial y sus implicaciones en la educación superior. *Propósitos y Representaciones, 7*(2), 536-568. http://dx.doi.org/10.20511/pyr2019.v7n2.274

ROSS (11 de diciembre de 2020). Anuncio por los fundadores de ROSS. *ROSS*. https://blog.rossintelligence.com/post/announcement

Rusell, S., & Norvig, P. (2004). Inteligencia artificial. Un enfoque moderno (J. Corchado, F. Martín, J. Cadenas, L. Hernández, E. Paniagua, R. Fuentetaja, M. Robledo & R. Rizo, trad.). Pearson Educación

San Martín Castro, C. (2015). *Derecho Procesal Penal. Lecciones*. Instituto Peruano de Criminología y Ciencias Penales.

Schwab, K. (2016). *La cuarta revolución industrial*. Editorial Debate.

Torres Manrique, J. (2017). Breves consideraciones acerca del aterrizaje de la inteligencia artificial en el derecho y su influencia en la realización de los derechos fundamentales. *Pensamiento Americano*, *10(*19), 210-227. http://dx.doi.org/10.21803%2Fpenamer.10.19.480

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Sala Especializada en Protección al Consumidor del Tribunal de Defensa de la Competencia y de la Propiedad Intelectual, 11 de junio de 2014, Resolución 1898-2014/SPC-INDECOPI, Expediente 3023-2012-CPC (Perú).

10.18800/themis.202101.018

MINERÍA DE TEXTOS Y DATOS E INTELIGENCIA ARTIFICIAL: NUEVAS EXCEPCIONES AL DERECHO DE AUTOR

TEXT AND DATA MINING AND ARTIFICIAL INTELLIGENCE: NEW EXCEPTIONS TO COPYRIGHT

H. Andrés Izquierdo*
Palacio & Izquierdo

There is growing attention and discussion on how national laws or international agreements should allow or prevent the fundamental right to research through text and data mining, and artificial intelligence. This article examines how copyright laws are beginning to regulate the subject matter. The most recent legislative amendments cover the inclusion of new exceptions and limitations in the rules of reproduction, storage, and public communication of works.

The analysis indicates that the standards adopted or used to regulate text and data mining (TDM) vary in their content and purpose from one country to another, which begins to generate a varied, inadequate, and incompatible international environment for project development based in text and data mining and artificial intelligence. The article concludes with some thoughts regarding the right of research, artificial intelligence, data and text mining, and the creation of new limitations and exceptions to copyright law.

Keywords: Data mining; text mining; artificial intelligence; copyright.

Existe una creciente atención y discusión sobre cómo las leyes nacionales o los acuerdos internacionales deberían permitir o impedir el derecho fundamental a la investigación por medio de la minería de textos y datos, y la inteligencia artificial. Este artículo examina cómo las leyes de derechos de autor están empezando a regular la materia. Las más recientes modificaciones legislativas comprenden la inclusión de nuevas excepciones y limitaciones en las normas de reproducción, almacenamiento, y comunicación pública de las obras.

El análisis indica que las normas aprobadas o utilizadas para regular la minería de textos y datos (TDM) varían en su contenido y objetivo de un país a otro, lo que empieza a generar un entorno internacional variado, inadecuado e incompatible para el desarrollo de proyectos de investigación basados en minería de textos y datos e inteligencia artificial. Este artículo concluye con reflexiones centradas en el derecho a la investigación, la inteligencia artificial, la minería de textos y datos, y la creación de nuevas limitaciones y excepciones en las leyes de derechos de autor.

Palabras clave: Minería de datos; minería de textos; inteligencia artificial; derechos de autor.

* Abogado. Master of Laws (LL.M.) en Propiedad Intelectual, Derechos de Autor e Industria del Entretenimiento por la Università degli Studi di Torino. Master of Laws (LL.M.) en Propiedad Intelectual, Derechos de Autor, Derecho de Marcas y Derecho del Entretenimiento estadounidense por la American University Washington College of Law. Asesor legal en Propiedad Intelectual e investigador académico de Inteligencia Artificial, Minería de Textos y Datos, y Derecho Cibernético en American University Washington College of Law. Socio de Palacio & Izquierdo (Washington DC, Estados Unidos). Contacto: info@andresizquierdo.com

Lo expresado en este artículo es a título personal, y no representa la posición de la Universidad o la firma de abogados.

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 27 de enero de 2021, y aceptado por el mismo el 26 de abril de 2021.

I. INTRODUCCIÓN

La inteligencia artificial (en adelante, IA) y el aprendizaje automático o *machine learning* (en adelante, ML) han mostrado un progreso práctico significativo en los últimos años. Los algoritmos de IA y ML están creando una sociedad mucho más automatizada, modificando diversos aspectos de la vida actual. La confluencia única de grandes cantidades de datos (incluida la información y los datos que se pueden encontrar en internet), los nuevos algoritmos y la informática moderna abren un nuevo capítulo para el desarrollo de IA y ML. Los productos básicos y los servicios –incluidas la atención médica, la agricultura o las finanzas– ahora dependen más de los algoritmos de ML[1]. Algunos de los ejemplos más destacados de crecimiento del sector privado en la actualidad, como Amazon o Facebook[2], dependen del uso de ML para optimizar sus métodos de producción, cadenas de suministro, el *marketing* y los precios cobrados a sus consumidores.

Sin embargo, existe un problema interesante: algunos países han aprobado normas para regular el creciente desarrollo en IA al mismo tiempo en el que se establecen estándares internacionales diversos y poco armoniosos para manejar el tema[3]. A medida que muchas industrias crecen y necesitan más información para adelantar investigación en minería de textos y datos o *text and data mining* (en adelante, TDM), algunas naciones han aprobado leyes para regular esta práctica. Aun así, los resultados evidencian leyes que no son compatibles entre esos mismos países. Por ejemplo, las normas en TDM aprobadas recientemente por la Directiva del mercado único digital (2019) en Europa serán incompatibles en muchos aspectos con la reforma de derechos de autor de TDM japonesa del 2018, o con las recientes sentencias de Google o HathiTrust del Tribunal de Apelaciones del Segundo Circuito de los Estados Unidos[4]. La diversa regulación crea un entorno internacional inestable, fragmentado y complejo para los usuarios e investigadores que utilizan información protegida por las leyes de derechos de autor.

Asimismo, la mayoría de los países que aún no inician una actualización de sus leyes en materia de derechos de autor en TDM solo pueden brindar oportunidades limitadas de poner a disposición obras con derechos de autor. Si los investigadores deciden utilizar las limitaciones y excepciones (en adelante, L&E) existentes –como el derecho a la investigación, la reprografía digital, el uso privado o uso personal–, el no contar con reglas explícitas respecto a TDM se traducirá en altos niveles de incertidumbre con motivo de los nuevos y constantes desarrollos tecnológicos de la IA para explorar la información. Además, los países que cuentan con interpretaciones muy restrictivas en L&E (por ejemplo, Argentina), sin duda harán casi imposible el desarrollo de cualquier proyecto de TDM en que se utilicen copias impresas o digitales de obras protegidas por derechos de autor. Los debates sobre IA y TDM crecen en todo el mundo en diversos escenarios, incluidos la Organización para la Cooperación y el Desarrollo Económicos (en adelante, OCDE) y la Organización Mundial de la Propiedad Intelectual (en adelante, OMPI)[5]. No obstante, a la fecha, no ha surgido ningún modelo de consenso al respecto.

Este artículo adoptará una perspectiva interdisciplinaria. La sección II abordará los conceptos de IA, ML y TDM sobre la base de las investigaciones gubernamentales, científicas y tecnológicas más recientes. La sección III revisará y analizará los aspectos legales con referencia a los contextos regionales y nacionales en TDM y derechos de autor. Se plantearán preguntas sobre la capacidad de las excepciones y limitaciones actuales en las leyes regionales o nacionales para promover el acceso a los datos bajo la perspectiva de los investigadores y los usuarios. La sección IV proporcionará recomendaciones para facilitar el diálogo entre los derechos de autor, la IA y la TDM, al tiempo que mostrará posibles soluciones para futuros cambios de políticas en este campo del derecho.

II. TRANSFORMACIÓN DIGITAL HACIA LA INTELIGENCIA ARTIFICIAL Y EL APRENDIZAJE AUTOMÁTICO

A. Inteligencia artificial

Nadie podría haber imaginado que la pregunta de Alan Turing en 1950 "¿pueden las máquinas pen-

1 Véase MIT SMR (2020)

2 Véase Congressional Research Service (2017); Davis (2020), Metz (2020).

3 Vease Flynn *et al.* (2020); también, Flynn *et al.* (2021). En Europa ver Geiger *et al.*(2018a); Hugenholtz (2019); Quintais (2020); para TDM en los Estados Unidos ver Sag (2019); Sag (2009); Carroll (2019); ver en forma general Okediji (2017); Litman (1994).

4 Ver *infra* Sección II.

5 Véase Organización Mundial de Propiedad Intelectual (2020).

sar?" sería el futuro del desarrollo tecnológico en la humanidad[6]. Este matemático británico es una de las muchas personas que abrieron el camino a décadas de trabajo sobre la capacidad de una máquina para mostrar un comportamiento inteligente. En la década de 1950, la investigación de la IA se centró, principalmente, en los juegos; en la década de 1960, en algoritmos de búsqueda y resolución de problemas generales (GPS); durante la década de 1970, la IA también exploró la comprensión del lenguaje natural y la representación del conocimiento (Zhongzhi, 2011). No obstante, en la década de 1980, a pesar de que se habían puesto en marcha muchos aspectos diferentes de la IA, su campo aún carecía de éxitos prácticos significativos, una situación que llevó a los conocidos "inviernos de la IA", en los que disminuyó substancialmente la financiación en Investigación y Desarrollo (MIT Lincoln Laboratory [MIT LL], 2019).

A finales de 1990 y principios del 2000, aquella resurgió con algunos éxitos prácticos. En los últimos años, la IA y el Aprendizaje Automático (ML) han mostrado un progreso práctico significativo. La nueva confluencia de grandes cantidades de datos (incluida la información y los datos que se pueden encontrar en internet), algoritmos y computación moderna está abriendo un nuevo capítulo para la historia de la IA[7]. Las estimaciones indican que el 90% de todos los datos se han creado en los últimos dos años. Hay una mayor capacidad para entrenar los algoritmos existentes con grandes cantidades de muestras de datos. Además, el uso de la computación moderna, particularmente las unidades de procesamiento de gráficos (GPU) y la capacidad de almacenamiento, han permitido que la IA emerja en la última década como no fue posible durante sus primeros 70 años de desarrollo. La combinación de estos elementos ha traído consigo avances dramáticos en IA en redes neuronales o métodos de "aprendizaje profundo" (Congressional Research Service [CRS], 2017)[8].

Como respuesta a estos avances, varios países y regiones de todo el mundo ya han elaborado informes sobre cómo alistarse para los próximos desafíos. En la carrera por ser pioneros en esta tecnología, la Oficina de Política de Ciencia y Tecnología de la Casa Blanca (OSTP), el Comité de Asuntos Legales del Parlamento Europeo, el Comité de Ciencia y Tecnología de la Cámara de los Comunes en el Reino Unido, el Consejo de Estado chino y el Center for Security and Emerging Technology de la Federación rusa han publicado estrategias para liderar en el campo de la IA. Paralelamente a la acción del gobierno, los comités de expertos también han elaborado diversos documentos de políticas públicas[9], así como el sector privado y las universidades a través de numerosos estudios y documentos de investigación sobre el tema[10].

1. Inteligencia artificial y *machine learning*

Definir a la IA es de suma importancia, especialmente cuando el tema está pendiente de legislación en todo el mundo. Esta tarea plantea un gran desafío, puesto que se encuentra en una evolución constante, por lo que trae nuevos desarrollos y aplicaciones de forma periódica. Los gobiernos han dado diversas definiciones, algunas amplias, otras más limitadas, pero, en general, no existe una comúnmente aceptada, en parte debido a los diversos enfoques de investigación en el campo[11]. Esta falta de acuerdo traerá problemas en los futuros procesos legislativos a nivel internacional, regional y nacional. No obstante, la falta de una definición precisa y universalmente aceptada de la IA, probablemente, también ha contribuido a que el campo crezca y avance a un ritmo cada vez más acelerado.

Por otra parte, ML es el nombre de una familia integral de técnicas utilizadas para nuevas formas de análisis de datos en IA (Lehr & Ohm, 2017). Hoy en día existe una mayor capacidad para entrenar los

6 Véase Turing (1950).

7 Ver definición de Inteligencia artificial en la siguiente sección

8 Véase también Davis (2020) y Metz (2020). La Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) ha identificado tres "olas" de desarrollo de la IA: La primera ola se centró en el conocimiento artesanal que permitió el razonamiento habilitado por el sistema en situaciones limitadas, aunque carecía de la capacidad de aprender o abordar la incertidumbre, como con muchos sistemas basados en reglas desde la década de 1980. La segunda ola, desde aproximadamente la década de 2000 hasta el presente, se ha centrado en los avances en las redes neuronales y el aprendizaje automático (por ejemplo, reconocimiento de imágenes, traducción de idiomas) utilizando modelos estadísticos y conjuntos de grandes datos. La tercera ola se centrará en la adaptación contextual, el aprendizaje y el razonamiento a medida que el sistema encuentra nuevas tareas, avanzando hacia la IA general.

9 Ver, por ejemplo, el Grupo de expertos de alto nivel en inteligencia artificial designado por la Comisión Europea, el grupo de expertos en IA en la sociedad de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), o el comité selecto sobre inteligencia artificial del Reino Unido, House of Lords.

10 Ver, por ejemplo, el Max Planck Institute for Innovation and Competition; Center for International Intellectual Property Studies (CEIPI) en Strasbourg University; PIJIP, American University, Washington College of Law.

11 Para Estados Unidos ver el reporte de la Select Committee on Artificial Intelligence of the National Science & Technology Council (2019); para Europa ver EPRS (2020); para China ver New America (2017).

algoritmos existentes con grandes cantidades de muestras de datos, convirtiéndolos en herramientas esenciales para la predicción y la toma de decisiones (Lehr & Ohm, 2017). Como se precisó anteriormente, con el uso de la informática moderna, en particular las unidades de procesamiento de gráficos (GPU) y la capacidad de almacenamiento, la IA ha crecido mucho respecto a sus primeras décadas de desarrollo.

Actualmente, la IA tiene aplicaciones en sectores como transporte, atención médica, agricultura, finanzas, derecho, ciberseguridad, y defensa[12]. Además, muchos productos y servicios, incluidos los filtros de correo no deseado, los diagnósticos médicos, el *marketing* de productos y los vehículos autónomos, dependen ahora de los algoritmos de ML (Coglianese & Lehr, 2017). Algunos de los ejemplos más destacados de crecimiento del sector privado en la actualidad, como Amazon o Zillow, dependen en su utilización para optimizar los métodos de producción, los precios, el *marketing* y las cadenas de suministro (Coglianese & Lehr, 2017, p. 1151). También, el ML ha incursionado en la seguridad nacional y la defensa mundial, una de las principales razones por las que los gobiernos también están buscando avances este campo[13].

Normalmente, el *machine learning* se analiza desde tres enfoques: aprendizaje supervisado, aprendizaje por refuerzo y aprendizaje no supervisado. En el primero, la máquina 'aprende' mediante la supervisión o la enseñanza. Más precisamente, recibe un conjunto de entrenamiento que le permitirá encontrar la respuesta correcta (Carroll, 2019). Bajo este sistema, el científico de datos actúa como un guía para enseñarle al algoritmo las respuestas correctas, pues requiere que "las posibles respuestas del algoritmo ya sean conocidas y que los datos utilizados para entrenar el algoritmo ya estén etiquetados con respuestas correctas" (Castle, 2017) [traducción libre][14]. Este tipo de aprendizaje se encuentra en sistemas diseñados para reconocer objetos (como el reconocimiento facial), sistemas de traducción automática, sistemas de apoyo a la toma de decisiones clínicas (como síntomas y diagnóstico), sistemas para evaluar las solicitudes de préstamos (también para seguros) y sistemas de recomendación de clientes (compras en línea)[15].

El aprendizaje por refuerzo es muy similar, ya que ambos sistemas requieren capacitación a través de ejemplos. No obstante, este último cambia el enfoque del aprendizaje automático del reconocimiento de patrones a la "toma de decisiones secuencial impulsada por la experiencia" (Hassabis *et al.*, 2017, p. 246-247) [traducción libre][16]. Este enfoque de aprendizaje automático generalmente implica la creación de metodologías de capacitación que permitan a un sistema explorar de forma independiente, realizar múltiples pruebas en tareas y aprender de estas experiencias. Como se explicó en una audiencia del Senado de los Estados Unidos en 2016:

> [El aprendizaje por refuerzo] explora los desafíos de permitir que los sistemas realicen una

[12] Véase Congressional Research Service (2017). Ver tambien Davis, (2020), Metz (2020).

[13] El último enfoque de operaciones cibernéticas mediante el uso de *machine learning* (ML) puede mejorar las "herramientas y capacidades de misión crítica", ya que los modelos de aprendizaje más recientes pueden detectar cambios de tráfico de distribución, patrones de comportamiento de red anómalos y ataques creativos a medida que se originan (Guerra & Tamburello, 2018). Más precisamente, ML puede ayudar a identificar *malware*, anomalías de red, detección de intrusiones, clasificación de agregación de información, inspección profunda de paquetes y detección de amenazas cibernéticas. En los últimos años, las operaciones cibernéticas reales van desde la piratería en redes gubernamentales o militares hasta ataques cibernéticos a corporaciones y cuentas personales. Los ejemplos más notables incluyen: el incidente de Titan Rain en 2003, cuando las instalaciones del Departamento de Defensa de EE. UU., los laboratorios de la NASA, Lockheed Martin y otros sistemas fueron pirateados y perdieron muchos terabytes de información; los incidentes cibernéticos dirigidos contra Estonia y Georgia, que provocaron graves trastornos en los medios de comunicación, el gobierno y los sistemas bancarios; la lucha de Estados Unidos contra el Estado Islámico de Irak y Siria (en adelante, ISIS); o el ciberataque de 2014 a Sony Pictures Entertainment por parte del grupo Guardianes de la paz, que roba datos y deshabilita sistemas informáticos. Nótese el contraste entre la guerra tradicional, que generalmente dependía de la participación de las fuerzas armadas de un Estado o de un grupo capaz de realizar operaciones militares estándar y los nuevos ciberataques. Ver también Myers (2007).

[14] Texto original: "[…] requires that the algorithm's possible outputs are already known and that the data used to train the algorithm is already labeled with correct answers". También puede verse Mokhtarian (2018).

[15] Para dar un ejemplo, un algoritmo binario pudo clasificar 1600 sentencias judiciales de cortes en Estados Unidos en temas de sociedades. En este caso, el algoritmo fue capaz de examinar las palabras de cada sentencia y determinar la probabilidad de sentencia a favor o en contra. Otro ejemplo se puede ver con el algoritmo COMPASS, un software de evaluación de riesgos que se utiliza para pronosticar qué delincuentes tienen más probabilidades de reincidir. Este sistema contiene información sobre delincuentes diseñada específicamente para determinar sus riesgos y necesidades e informar planes dinámicos de casos "que guiarán al delincuente a lo largo de su ciclo de vida en el sistema de justicia penal". Sin embargo, es relevante mencionar que se ha cuestionado la equidad en este tipo de algoritmos, ya que podría presentar sesgos con los sistemas automatizados de toma de decisiones (ADM). Ver Fagan (2015); Spielkamp (2017); ver también *NJCM et al./Países Bajos* (2018), sentencia por medio de la cual se le prohibió al gobierno holandés el uso de SyRI, una tecnología utilizada para detectar posibles fraudes a la asistencia social).

[16] Texto original: "sequential decision making driven by experience".

> exploración activa en mundos simulados y reales, que tienen como objetivo dotar a los sistemas con la capacidad de hacer predicciones y realizar acciones físicas con éxito (U.S. Senate, Subcommittee On Space, Science, And Competitiveness, Committee On Commerce, Science, And Transportation, 2016, p. 13) [traducción libre][17][18].

Un tercer sistema de aprendizaje automático relevante es el aprendizaje no supervisado. A diferencia del aprendizaje supervisado o por refuerzo, el aprendizaje no supervisado funciona sin recibir instrucciones externas, un aprendizaje sin etiquetas de autoría humana. Bajo este sistema, la máquina funciona mediante agrupamiento y reducción de dimensionalidad mientras busca identificar la estructura entre los datos no etiquetados[19]. Ejemplos comunes de algoritmos de aprendizaje no supervisados son la investigación de segmentación de audiencia, investigación de clientes, reconocimiento de patrones, o detección de anomalías (operaciones cibernéticas). El aprendizaje no supervisado se caracteriza a menudo como aprendizaje supervisado con un resultado desconocido, ya que muchas veces es difícil generar un criterio objetivo para clasificar los resultados como fallidos o exitosos (Hinton & Sejnowski, 1999). El hecho de que una máquina pueda identificar y resolver problemas de procesamiento de forma independiente nos acerca a la pregunta original de "¿pueden pensar las máquinas?" formulada por Alan Turing en la década de 1950.

2. TDM e IA

La minería de textos y datos se está convirtiendo en una práctica cada vez más común. Se refiere a la capacidad de la IA para interpretar grandes cantidades de datos sin procesar, para, precisamente, ser procesados mediante la identificación de patrones[20]. Como se ha advertido, la TDM puede ubicarse como aprendizaje por refuerzo o como aprendizaje no supervisado, toda vez que se permite a un sistema explorar de forma independiente, realizar múltiples pruebas en tareas y aprender de estas experiencias, y –algunas veces– la máquina funciona mediante el agrupamiento y reducción de dimensionalidad mientras busca identificar la estructura entre los datos no etiquetados.

Así, a medida que aumenta la escala de la información procesada, la TDM utiliza algoritmos para analizar grandes volúmenes de contenido en busca de patrones e información en períodos de tiempo mucho más reducidos en comparación con un lector humano, al mismo tiempo que aporta nuevos conocimientos y comprensión en diversos campos del saber humano (Geiger *et al.*, 2019, p. 24). Sin que las conexiones se identifiquen o mencionen explícitamente en los artículos, por ejemplo, la TDM se puede utilizar en lingüística para analizar grandes volúmenes de texto y extraer patrones sintácticos o gramaticales (Hugenholtz, 2019); en medicina, para encontrar asociaciones entre un gen y una enfermedad, o entre un fármaco y un evento adverso (Borghi, 2016); y, en general, la TDM es una práctica estándar en la actualidad para diversos temas de investigación –incluida la investigación farmacéutica, periodismo, recuperación de información, e información al consumidor (Hugenholtz, 2019)–. En la siguiente sección, examinaremos el enfoque legal adoptado por diferentes países a medida que las normas TDM se están volviendo desiguales, fragmentadas y complejas para las bibliotecas, los investigadores y los usuarios de la información (Caspers *et al.*, 2017).

III. MINERÍA DE TEXTOS Y DATOS, Y LAS NUEVAS EXCEPCIONES EN DERECHOS DE AUTOR

Como se examinó anteriormente, la minería de textos y datos amplía sustancialmente las capacidades de investigación en la literatura científica y académica. Aun así, para funcionar de manera efectiva, necesita acceso completo a los datos de materiales de texto y bases de datos. Actualmente, existen dos posibilidades para el acceso a estos: la

---

17 Texto original:

> Research efforts have been underway on the challenges of enabling systems to do active exploration in simulated and real worlds that are aimed at endowing the systems with the ability to make predictions and to perform physical actions successfully.

18 Bajo este sistema, la máquina aprende a través de recompensas o penalizaciones que están vinculadas a los resultados de tales acciones. Los ejemplos incluyen sistemas de ML que aprenden a jugar un juego mediante recompensas vinculadas a las victorias y con las penalizaciones vinculadas a las derrotas; o sistemas de inversión donde las recompensas están vinculadas a las ganancias financieras, y las sanciones a las pérdidas. Cuando este sistema está funcionando a su máximo potencial, las aplicaciones de IA pueden tomar acciones independientes en el mundo real. Ver también U.S. Senate, Subcommittee On Space, Science, And Competitiveness, Committee On Commerce, Science, And Transportation (2016).

19 Ver Castaneda *et al.* (2020); ver generalmente Hinton & Sejnowski (1999); Barlow (1989); Le *et al.* (2012).

20 La Directiva 2019/790, en su artículo 2.2, define la minería de textos y datos como: "toda técnica analítica automatizada destinada a analizar textos y datos en formato digital a fin de generar información que incluye, sin carácter exhaustivo, pautas, tendencias o correlaciones" (2019). Véase también Eskevich & Bosch (2016).

primera opción es obtener materiales de acceso abierto que generalmente se encuentran disponibles gratuitamente para su descarga y reutilización; la segunda, es utilizar materiales protegidos por el derecho de autor con reglas de permiso específicas para el acceso y la manipulación.

Bajo la primera opción, comúnmente, los contenidos están disponibles para su descarga bajo una licencia Creative Commons o similar que permite una redistribución y reutilización más abierta que una obra protegida exclusivamente por los derechos de autor. Las publicaciones de acceso abierto van en aumento con bases de datos como PubMed Central con más de 2,75 millones de artículos de texto completo para TDM y otros tipos de reutilización[21]. La segunda opción de acceso a contenidos son las revistas basadas en suscripción, que restringen el acceso a sus publicaciones bajo la legislación de derechos de autor aplicable o a los tipos de contratos suscritos. Algunas colaboraciones entre editores brindan acceso a contenidos basados en suscripción, pero no parecen brindar a los investigadores un acceso completo a la literatura publicada para realizar investigaciones de TDM (Carroll, 2019).

Cuando los derechos de autor son la limitación para el acceso a los contenidos, cada país ostenta un conjunto diferente de reglas para permitir, limitar o, posiblemente, prohibir las actividades de TDM. Algunos países como Japón[22], Reino Unido[23] y Alemania[24] han desarrollado reglas específicas para el uso de TDM. A nivel regional, la Unión Europea aprobó, en 2019, la Directiva sobre el mercado único digital que incluye explícitamente las actividades de investigación de TDM (Directiva 2019/790, 2019). En Estados Unidos, las cortes han permitido actividades específicas de TDM a través del uso justo de los derechos de autor[25]. Los países que no han abordado la TDM a través de leyes o fallos judiciales podrían permitir la investigación de TDM por medio de excepciones y limitaciones de derechos de autor: el derecho a la investigación, la reprografía, el uso privado o personal, el almacenamiento digital o las medidas técnicas de protección podrían ser una solución para las investigaciones basadas en TDM. Hay otros ejemplos de países en donde la legislación nacional sobre derechos de autor cuenta con una interpretación restrictiva que bloquea cualquier posibilidad para la investigación de este tipo[26].

La legislación integral sobre TDM se presenta como una herramienta esencial para los investigadores, ya que pueden permitir el acceso legal a materiales y bases de datos, realizar reproducciones, almacenar la información y, en algunos casos, compartir los resultados sin violaciones de derechos de autor (Francoise, 2020). Como se verá en esta sección, los países muestran diversas regulaciones sobre la realización de la TDM.

A. Legislación en minería de textos y datos

Las regulaciones sobre TDM, generalmente, son una excepción al régimen actual de derechos de autor, lo que permite a los usuarios extraer obras a las que tienen acceso lícito. La excepción permite a los investigadores y otros usuarios legítimos realizar actividades del tema sobre grandes cantidades de datos. Esta excepción, usualmente, incluye el acceso a contenidos –en el sitio (como la biblioteca o archivo) y de forma remota– y el derecho a la reproducción de las obras. En otros casos, la excepción también garantiza el derecho a retener copias para su almacenamiento y estudio posterior. En contadas ocasiones, también incluye el derecho de comunicación a fin de poder compartir el *corpus* o los resultados de la investigación con terceras personas, fuera del círculo de trabajo. En las siguientes secciones, se examinarán las limitaciones y excepciones de derechos de autor aprobadas recientemente por la Unión Europea, Reino Unido, Japón y Estados Unidos.

1. Unión Europea

La Unión Europea (en adelante, UE) se encuentra en proceso de modernización respecto a sus normas de derechos de autor para los nuevos y cambiantes entornos digitales (European Comission, 2020b). En 2017, se aprobó un reglamento sobre la portabilidad transfronteriza de los servicios de contenido en línea para permitir a los consumidores que compran o se suscriben a películas, retransmisiones deportivas, música, libros electrónicos y juegos a fin de acceder a los contenidos

[21] Véase la página web PubMed Central (PMC) (s/f).

[22] Véase Ley de Derechos de Autor de Japón (Act 48, 1970).

[23] Véase *Copyright, Designs and Patents Act 1988* (modificado 2017).

[24] Véase *Urheberrechtsgesetz* (1965).

[25] Véase sentencias judiciales: *Authors Guild, Inc. c. Google, Inc.* (2015) y *Authors Guild, Inc. c. HathiTrust* (2014).

[26] Véase Flynn *et al.* (2020). Argentina es un ejemplo de interpretación restrictiva de las excepciones y limitaciones de su ley de derechos de autor. El articulo 10 de la Ley 11.723 de 1933, solo permite reproducir breves fragmentos no superiores a 1000 palabras, lo cual hace casi imposible la investigación por medio de TDM.

mientras viajan por países de la UE. En el mismo año, por medio de una Directiva y un Reglamento, se implementó el Tratado de Marrakech para permitir el acceso de contenidos protegido por derechos de autor a las personas ciegas, con discapacidad visual o con alguna otra discapacidad[27]. En el 2019, la Directiva del mercado único digital (en adelante, Directiva MUD) adoptó nuevas excepciones y limitaciones de derechos de autor que se centran en la disponibilidad en línea de los contenidos en toda la UE, incluidas las excepciones del artículo 3 y 4 sobre TDM[28].

Los artículos 3 y 4 de la Directiva MUD tienen como objetivo proporcionar un entorno armonizado para los investigadores de toda Europa. En primer lugar, la Directiva MUD crea excepciones y limitaciones obligatorias para los investigadores que llevan a cabo proyectos en TDM, lo que garantiza una implementación más uniforme en todo el continente. En segundo lugar, las L&E cubren usos comerciales y no comerciales, generando que la investigación se encuentre disponible para materiales a los que se accede legalmente. Finalmente, las disposiciones contractuales creadas por los titulares de derechos no pueden anular los usos no comerciales garantizados en el artículo (*Geiger et al.*, 2018a). Sin embargo, las dos excepciones no son igualmente sólidas, ya que el uso comercial del artículo 4 puede estar restringido por acuerdos privados (Hugenholtz, 2019), como veremos en la sección siguiente.

a. *Artículo 3, Directiva MUD*

El artículo 3 de la Directiva MUD (Directiva 2019/790, 2019) crea una excepción de derechos de autor obligatoria para la investigación científica no comercial realizada con TDM. Cualquier disposición contractual contraria a la excepción en TDM será inaplicable y el proyecto en TDM solo puede ser promovido por organismos de investigación e instituciones responsables del patrimonio cultural. La excepción incluye reproducciones, extracciones y almacenamiento de obras; no obstante, el usuario requiere un acceso lícito. Para comprender plenamente el alcance de este artículo, es necesario revisar los beneficiarios de la excepción –organizaciones de investigación, instituciones de patrimonio cultural–; las condiciones de uso, como el acceso lícito y las medidas técnicas de protección (en adelante, TPM); así como las limitaciones que encontrará la disposición en TDM de la Directiva MUD en comparación con otras legislaciones nacionales.

i. *Beneficiarios de la excepción*

Según la Directiva MUD, el primer grupo de beneficiarios de la excepción son los organismos de investigación (Directiva 2019/790, 2019). Este tipo de organizaciones cubren una amplia variedad de entidades cuyo objetivo principal es realizar investigación científica o realizarla junto con servicios educativos (Directiva 2019/790, 2019, considerando 12). La descripción de las organizaciones de investigación incluye universidades –y sus bibliotecas–, institutos de investigación o cualquier otra entidad, como hospitales, que realice esta clase de labor. La Directiva MUD limita la organización de investigación exigiendo que trabaje sin fines de lucro o reinvirtiendo todos los beneficios en su investigación científica, o trabajando bajo una misión de interés público reconocida por un Estado miembro europeo[29]. Es necesario tener en cuenta que el considerando 11 de la Directiva MUD permite a las organizaciones de investigación beneficiarse de la excepción cuando sus actividades de investigación se llevan a cabo en el marco de asociaciones público-privadas, pero organizaciones en las que las empresas comerciales tienen una influencia decisiva en el proyecto de investigación –como accionistas o miembros que podrían obtener acceso preferencial a los resultados de la investigación–, no se consideran organizaciones de investigación para tal directiva (Hugenholtz, 2019).

El segundo grupo de beneficiarios de las excepciones de la TDM son las instituciones responsables del patrimonio cultural. La Directiva MUD las define como cualquier biblioteca o museo de acceso público, un archivo o una institución de patrimonio cinematográfico o sonoro (Directiva 2019/790, 2019, considerando 13 & art. 2.3). La definición incluye bibliotecas y museos de acceso público, independientemente del tipo de obras que guarden en sus colecciones y archivos permanentes, películas o audio. La descripción también incluye bibliotecas y archivos nacionales, y cualquier archivo y biblioteca de acceso público de establecimientos educativos, organizaciones de investigación u organizaciones de radiodifusión del sector público.

[27] Véase Reglamento 2017/1563 (2017) y Directiva 2017/1564 (2017).

[28] Véase Directiva 2019/790 (2019), Directiva 96/9/CE (1996) y Directiva 2001/29/CE (2001). Asimismo, ver de forma general Geiger *et al.* (2018a, pp. 4-15).

[29] Dicha norma menciona en su considerando 12 que "dicha misión podrá quedar reflejada, por ejemplo, a través de la financiación pública o de disposiciones de la legislación nacional o de los contratos públicos" (Directiva 2019/790, 2019). Asímismo véase Quintais (2020).

Dado que la definición es tan amplia, algunas instituciones del patrimonio cultural también podrían clasificarse como organizaciones de investigación. Es importante mencionar que la excepción no incluye a personas o investigadores no afiliados, claramente excluidos del MUD[30].

ii. *Acceso lícito*

En cuanto a las condiciones de uso, el acceso lícito es un actor importante en el proceso de TDM. Este incluye el contenido basado en una política de acceso abierto y el obtenido mediante acuerdos contractuales entre los titulares de derechos y los beneficiarios de la excepción (organizaciones de investigación o instituciones de patrimonio cultural) (Directiva 2019/790, 2019, considerando 14). La política de acceso abierto se refiere "[…] a la información científica que es gratuita para el usuario y que es reutilizable" (European Comission, 2020b) [traducción libre][31 32], mientras que el contenido sujeto a un acuerdo contractual cubre todas las suscripciones y el contenido que está disponible en línea. El considerando 14 establece que "en el caso de las suscripciones realizadas por organismos de investigación o instituciones responsables del patrimonio cultural, se considera que las personas vinculadas a ellas y amparadas por esas suscripciones también tienen acceso lícito" (Directiva 2019/790, 2019). Así, el acceso lícito se divide entre servicios gratuitos y servicios pagos.

Sin embargo, las limitaciones al acceso legal no vienen con los contenidos de acceso abierto, sino con los contenidos que requieren un pago por suscripción. Cuando el acceso legal está vinculado a los pagos de los servicios de suscripción, la capacidad presupuestaria de la organización pasa a desempeñar un rol fundamental. Geiger, Frosio y Bulayenko afirman que "solo pocas organizaciones de investigación podrán adquirir licencias para todas las bases de datos que sean relevantes para un proyecto de investigación en TDM" (2018c, p. 29) [traducción libre][33]. Como resultado, solo un número limitado de organizaciones de investigación podrá adelantar proyectos de TDM. Si la capacidad de financiamiento de cada institución determina los resultados de la investigación en dicho campo, el acceso lícito aumentará las diferencias entre las instituciones. Además, podría aumentar la brecha científica y de innovación entre las naciones europeas desarrolladas y las menos desarrolladas.

El acceso lícito tiene una capa adicional de control, ya que el artículo 3 inciso 3 permite a los titulares de derechos aplicar medidas técnicas de protección (TPM) "para garantizar la seguridad e integridad de las redes y bases de datos en que estén almacenadas las obras u otras prestaciones. Dichas medidas no irán más allá de lo necesario para lograr ese objetivo" (Directiva 2019/790, 2019)[34]. El considerando 16 va más allá para explicar el razonamiento detrás de la disposición, ya que enmarca la solicitud en un número potencialmente elevado de solicitudes de acceso y descargas de obras. Por lo tanto, los titulares de derechos pueden hacer uso de medidas técnicas de protección en casos en los que la seguridad e integridad de sus sistemas o bases de datos pueda verse comprometida. No obstante, la Directiva MUD también establece un equilibrio recomendado entre las TPM y los riesgos de seguridad, ya que ambos "no deben exceder de lo necesario para alcanzar el objetivo de garantizar la seguridad e integridad de la red y no han de menoscabar la aplicación efectiva de la excepción" (Directiva 2019/790, 2019, considerando 16).

Sin embargo, el alcance de la excepción del artículo 3 inciso 3 genera varias preguntas, ya que podría ubicar a la UE en una posición de desventaja para la investigación en IA[35]. Si bien la UE divide el régimen de TDM entre uso no comercial y co-

30 Ver más adelante en la sección del Reino Unido, en la que se incluyen los investigadores no afiliados en la excepción TDM de *la Copyright, Designs and Patents Act* (1988, § 29A).

31 Texto original: "[…] access to scientific information that is free of charge to the user and is reusable".

32 Véanse también los proyectos Open Access Infrastructure for Research in Europe (OpenAIRE), Open Science Policy Platform, Horizon 2020, European Open Science Cloud (EOSC) para programas y grupos de expertos enfocados en el acceso a datos abiertos. Ver, en general, en los Estados Unidos el Open Access Policy de la University of California:

> Each Faculty member grants to the University of California a nonexclusive, irrevocable, worldwide license to exercise any and all rights under copyright relating to each of his or her scholarly articles, in any medium, and to authorize others to do the same, for the purpose of making their articles widely and freely available in an open access repository (Office of Scholarly Communication, 2013).

33 Texto original: "Only few research organisations will be able to acquire licences for all databases that are relevant for a TDM research project".

34 Asimismo, ver de forma general Dusollier:

> Despite the expressed intention of the European lawmaker to safeguard a balance between the rights of the copyright holders and the interests of the users and society at large, the anti-circumvention provisions give the rights owners preference: the protection is broad and surely extends beyond the boundaries of copyright; the exceptions are overridden, albeit the empty promise of the article 6(4) (2003, p. 478).

35 Véase Samuelson (2018), Hilty (2016) y Ducato & Strowel (2019).

mercial, otros países como Estados Unidos y Japón han evitado ese enfoque, permitiendo la TDM sin importar el propósito comercial o el tipo de usuario[36]. Como se evidenciará en las siguientes secciones, las recientes sentencias judiciales de TDM en los Estados Unidos –*Authors Guild, Inc. c. Google* (2015) y *Authors Guild, Inc. c. HathiTrust* (2014)– han permitido el uso comercial de la investigación de TDM bajo la excepción de uso justo en la ley de derecho de autor. Asimismo, Japón, el primer país en aprobar una disposición de derechos de autor en TDM, no distingue entre uso comercial y no comercial; el análisis de la información no debe realizarse necesariamente con fines de investigación científica, y TDM está abierto a todos los usuarios (*Act 48*, 1970). En consecuencia, dadas las limitaciones entre usos comerciales y no comerciales en la UE, las empresas de este continente podrían enviar al exterior sus proyectos de investigación en TDM, a lugares con una legislación menos restrictiva o, de la misma forma, las empresas fuera del continente podrían evitar el mercado europeo debido a las restricciones de la Directiva MUD (Samuelson, 2018).

b. *Artículo 4, Directiva MUD*

Contrario al artículo 3, el artículo 4 crea una excepción que no tiene ninguna restricción sobre el tipo de usuario o el propósito comercial; aun así, la excepción puede ser anulada por acuerdos contractuales o una declaración unilateral (Quintais, 2020). Esta excepción de TDM incluye todo tipo de usuarios sin importar su afiliación: cualquier organización, corporación o investigador individual puede hacer uso de la excepción en TDM. Además, la actividad TDM es aplicable a cualquier reproducción y extracción de obras legalmente accesibles, ya sea para uso comercial o no comercial (Directiva 2019/790, 2019, art. 4.1 & 4.2). No obstante, la excepción o limitación es aplicable solo a condición de que los titulares de los derechos no se hayan reservado expresamente el uso de las obras, ya que les da una opción de exclusión voluntaria (Directiva 2019/790, 2019, art. 4.3).

A todos los efectos, el artículo 4 es una disposición que permite a cualquier persona u organización participar en proyectos de TDM siempre que el titular del derecho consienta el uso. El artículo 4 inciso 3 y el considerando 18 dan a los titulares de derechos la opción de reservar sus derechos mediante "la utilización de medios de lectura mecánica, incluidos los metadatos y las condiciones de un sitio web o un servicio" (Directiva 2019/790, 2019). Sin embargo, también pueden reservarse los derechos por otros medios, "como acuerdos contractuales o una declaración unilateral" (Directiva 2019/790, 2019, art. 4.3). Entonces, en la práctica, un editor puede controlar el acceso que tenga la intención de uso comercial; ostenta la libertad de otorgar licencias mediante acuerdos contractuales, o puede bloquear o prohibir unilateralmente cualquier uso de sus obras. El riesgo surge, como afirma Hugenholtz, en que los editores podrán "ofrecer el acceso pago a TDM, y se mostrarán reacios a otorgar licencias TDM a terceros" (2019). Como resultado, el artículo 4 podría, efectivamente, crear y legitimar un 'mercado derivado' para las actividades de TDM, a través de contratos, licencias e incluso, exclusividad sobre obras y contenidos.

Este artículo también podría ubicar a la UE en una posición de desventaja, ya que la opción de exclusión voluntaria en la Directiva MUD no coincide con las disposiciones de TDM menos restrictivas de otras jurisdicciones. A la vanguardia de las regulaciones abiertas de TDM, Japón puede permitir cualquier uso de TDM, incluida la investigación comercial, sin ninguna compensación al titular de los derechos. La legislación de Japón también puede permitir que un usuario de TDM esté libre de la retribución económica de un titular de derechos cuando accede a datos o información, y realiza copias electrónicas incidentales de las obras o durante la búsqueda de bases de datos (*Act 48*, 1970). Además, como se verá en el caso de Google TDM de Estados Unidos, las empresas pueden participar en proyectos de TDM sin ninguna compensación al titular de los derechos si cumplen las condiciones de uso justo requeridas[37]. Asimismo, algunos países que carecen de disposiciones específicas para limitar el uso de TDM, como Belice o Barbados, pueden permitir la libre explotación en virtud del trato justo o del artículo 9, numeral 2, del Convenio de Berna (1886)[38]. Estos mercados alternativos podrían alentar a los investigadores, organizaciones y corporaciones a explorar países con menos limitaciones legales para los proyectos de TDM.

2. Reino Unido

La excepción de derechos de autor de TDM del Reino Unido se aprobó en 2014, pero se limita a

[36] Ello se comentará en secciones posteriores del presente trabajo.

[37] Véase *Copyright Act of 1976* (U.S. Code, 2012, título 17, § 107), Limitaciones a los derechos exclusivos: Uso justo.

[38] Véase Ley de Derechos de Autor de Bélice (2000, cap. 252) y Ley de Derechos de Autor de Barbados (1998, cap. 300).

un propósito no comercial[39]. El texto del artículo 29A del *Copyright, Designs and Patents Act* señala lo siguiente: "una persona que tenga acceso lícito a la obra puede realizar un análisis computacional de todo lo registrado en la obra con el único fin de realizar una investigación con fines no comerciales" (1988, art. 29A(1)(a)) [traducción libre][40]. El alcance de esta excepción se enmarca en el artículo 5.3 (a) de la Directiva InfoSoc, norma que requiere un fin de investigación científica con carácter no comercial (Directiva 2001/29/CE, 2001)[41]. Aunque el artículo 5.3 no es una excepción obligatoria para los miembros de la UE, al introducir la excepción al *Copyright, Designs and Patents Act* (2014), el gobierno buscaba permitir la investigación sin "socavar el control de los editores sobre los sistemas de TI o la explotación comercial" (HM Government, 2012, p. 37) [traducción libre][42]. Según lo expresado por la Oficina de Propiedad Intelectual del Reino Unido, la creación de la excepción no significa que los investigadores tendrán acceso gratuito, ya que "los investigadores o sus instituciones todavía tienen que comprar el acceso al contenido si ese es el modelo de negocio del editor" (UK Intellectual Property Office, 2014, p. 8) [traducción libre][43]. No obstante, no existen restricciones sobre cómo o dónde se pueden publicar los resultados de la investigación en TDM, siempre y cuando el propósito original de la investigación no sea comercial.

No obstante, el uso no comercial no es la única restricción relevante a la excepción del Reino Unido. Existe una segunda restricción significativa respecto a la excepción de derechos de autor: el requerimiento de acceso lícito a las obras que se utilizan (Geiger *et al.*, 2018b, p. 17). El artículo 29A (1) requiere el acceso lícito para realizar la copia de la obra que se utilizará para realizar el análisis computacional. La Oficina de Propiedad Intelectual del Reino Unido define el acceso lícito como el derecho de "los investigadores para leer una obra protegida por derechos de autor" (UK Intellectual Property Office, 2014, p. 7) [traducción libre][44]. Sin embargo, como se vio anteriormente con la Directiva MUD, las limitaciones al acceso lícito no se instituyen con los contenidos de acceso abierto, sino con los contenidos que requieren una suscripción paga. Cuando el acceso lícito está vinculado a los pagos de los servicios de suscripción, la capacidad presupuestaria del investigador llega a jugar un papel esencial, por lo que puede aumentar la brecha científica y de innovación entre los investigadores en el interior del Reino Unido.

La tercera limitación significativa proviene del artículo 29A (2), ya que la excepción solo se aplica a las reproducciones, pero no a la comunicación de la obra. A diferencia de otras excepciones de TDM que permiten la reproducción y el intercambio del trabajo, el artículo 29A (2) (a) no permite al investigador "compartir la información de investigación de TDM con ninguna otra persona" (*Copyright, Designs and Patents Act,* 1988) [traducción libre][45], excepto cuando la transferencia esté autorizada por el propietario de los derechos de autor. La Oficina de Propiedad Intelectual del Reino Unido es clara en esta restricción, ya que las obras "no se compartirán, venderán o pondrán a disposición del público de ninguna manera y cualquiera que lo haga podría ser demandado por infracción de derechos de autor" (UK Intellectual Property Office, 2014, p. 7) [traducción libre][46]. Asimismo, aunque el artículo 5(3) de la Directiva InfoSoc (Directiva 2001/29/CE, 2001), que inspiró el artículo 29A, permite las excepciones tanto para la reproducción como para la comunicación, la ley de derechos de autor del Reino Unido decidió excluir la opción de comunicación. En un proceso de TDM, compartir información es una segunda parte importante del proceso, lo que permite que otros investigadores colaboren o incluso desarrollen nuevos proyectos de investigación a partir de la misma información. Compartir ayuda a un mayor desarrollo del conocimiento, la misma función que tiene un libro cuando se imprime y se publica para el público en general.

Como resultado, la excepción de derechos de autor de TDM del Reino Unido podría estar pendiente de revisión. Dado que la excepción se formuló antes del Brexit (2014) y se inspiró parcialmente en el artículo 5(3) de la Directiva InfoSoc (Direc-

39 Véase Geiger *et al.* (2018b, p. 17) y Margoni & Dore (2016).

40 Texto original: "a person who has lawful access to the work may carry out a computational analysis of anything recorded in the work for the sole purpose of research for a non-commercial purpose".

41 Ver de forma general Rosati (2019).

42 Texto original: "[…] without undermining publishers' control over IT systems or commercial exploitation".

43 Texto original: "[…] researchers or their institutions still have to buy access to content if that is the business model of the publisher".

44 Texto original: "researchers have the legal right to access a copyright work to read it".

45 Texto original: "the copy is transferred to any other person".

46 Texto original: "They can't be shared, sold, or made publically available in any way and anyone doing so could be sued for copyright infringement".

tiva 2001/29/CE, 2001), el Reino Unido podría estar *ad portas* de nuevas reglas en TDM que alineen más los enfoques internacionales actuales o, incluso, con la Directiva MUD. Sin embargo, a pesar de que la Directiva MUD de la UE podría ser un punto de partida para una reforma, incluir un uso comercial obligatorio –como se ve en Japón o Estados Unidos–, podría traer mejores resultados competitivos para los investigadores del Reino Unido. Enmarcar excepciones que pueden estar a la par con los países más progresistas también podría traer proyectos internacionales al territorio del Reino Unido.

3. Japón

Japón fue el primer país en modificar su Ley de derechos de autor en 2009 para incluir una excepción de TDM, posteriormente modificada por una enmienda de 2018 que amplió el alcance de la excepción.

La disposición TDM de 2009 se introdujo para permitir el análisis de información por computadora, autorizando la reproducción y adaptación de obras utilizadas para proyectos TDM[47]. La excepción incluía una definición amplia de análisis informativo[48], no tenía restricciones de uso comercial y no era necesario que los proyectos TDM se llevarán a cabo exclusivamente con fines de investigación científica (SYNYO GmbH, 2015). Sin embargo, la excepción también contaba con algunas limitaciones relevantes: todas las tareas de TDM debían realizarse exclusivamente con un ordenador, lo que generó dudas sobre la aplicabilidad futura si entraran en juego nuevas tecnologías (Borgui & Karapapa, 2013). La excepción también parecía excluir los datos sin procesar, así como las bases de datos (Triaille *et al.*, 2014). Estas limitaciones e incertidumbres en la norma crearon la necesidad de una enmienda a la excepción de derechos de autor de TDM de 2009 (Caspers & Guibault, 2016).

La enmienda de 2018 introduce disposiciones adicionales en TDM, al tiempo que ofrece un alcance más amplio para las tecnologías involucradas[49]. El artículo 30, numeral 4 (*Act 48 de 1970*, 2018), amplía el alcance de las obras para uso en TDM, al tiempo que introduce los tipos de explotación que se pueden realizar. El artículo permite la explotación de cualquier obra protegida por derechos de autor que no esté destinada a disfrutar o hacer que otra persona disfrute de las ideas o emociones expresadas en dicha obra[50]. La definición de 'disfrutar' surge como un elemento clave para fijar el alcance de esta limitación. Para la Oficina Japonesa de Derechos de Autor (en adelante, JCO por sus siglas en inglés), el valor económico de una obra surge cuando una "[p]ersona que ve o escucha la obra, paga una compensación por dicha obra para disfrutar de las ideas o emociones expresadas en la obra, satisfaciendo los intereses intelectuales o emocionales de dicho usuario" (Japan Copyright Office, 2019, p. 12) [traducción libre][51]. Por tanto, para la JCO los actos realizados sin el propósito de disfrutar de las ideas o emociones expresadas en una obra no perjudicarán los intereses del titular de los derechos de autor. El artículo 30, numeral 4, inciso (iii), proporciona ejemplos de obras no destinadas para 'disfrute', siendo estas obras utilizadas en el procesamiento de datos informáticos y que no involucran su percepción por medio de los sentidos humanos.

El artículo 30, numeral 4, inciso (ii), da un alcance aún más amplio a la excepción, ya que ofrece una lista completa de los pasos previsibles en un proyecto de TDM. Según la Ley de Derechos de Autor japonesa, está permitido explotar el trabajo "de cualquier forma y en la medida que se considere necesario" (*Act 48 de 1970*, 2018, art. 30-4) [traducción libre][52]. Esto incluye acciones como la "extracción, comparación, clasificación u otro análisis estadístico de datos de lenguaje, sonido o imagen, u otros elementos de los que se componga una gran cantidad de obras o un gran volumen

[47] Véase el artículo 47-7, de la Ley de Derechos de Autor de Japón (*Act 48 de 1970*, 2018):

> For the purpose of information analysis [...] by using a computer, it shall be permissible to make recording on a memory, or to make adaptation (including a recording of a derivative work created by such adaptation), of a work, to the extent deemed necessary. However, an exception is made of database works which are made for the use by a person who makes an information analysis.

[48] Véase el artículo 47-7, de la Ley de Derechos de Autor de Japón (*Act 48 de 1970*, 2018):

> '[I]nformation analysis' means to extract information, concerned with languages, sounds, images or other elements constituting such information, from many works or other such information, and to make a comparison, a classification or other statistical analysis of such information; the same shall apply hereinafter in this Article (versión del 2009).

[49] Véase de forma general Ueno (2021).

[50] Véase de forma general Ueno (2021).

[51] Texto original: "[P]erson who views or listens to the work pays compensation for such work in order to enjoy the ideas or emotions expressed in a work and satisfies the person's intellectual or emotional desires".

[52] Texto original: "in any way and to the extent considered necessary,".

de datos" (*Act 48 de 1970*, 2018, art. 30-4(ii)) [traducción libre][53]. El artículo da derecho a extraer todos los trabajos requeridos, clasificarlos y compararlos, ejecutar cualquier proceso en TDM, así como procesar análisis estadísticos de todo tipo y tamaño de trabajos, eliminando así cualquier posibilidad de restringir el procesamiento de datos.

Las excepciones de TDM de derechos de autor de Japón muestran la legislación más abierta para el uso de TDM. Contrariamente a las excepciones de la Directiva europea MUD, o el Reino Unido, Japón ofrece una excepción lo suficientemente flexible como para ofrecer un entorno abierto para la investigación y exploración de un amplio espectro de proyectos en TDM.

B. TDM basado en decisiones judiciales

1. Estados Unidos de América

Existen diversos casos que deben ser considerados para determinar la legalidad de TDM en los Estados Unidos, toda vez que esta área del derecho no está codificada en la ley. Como se verá en esta sección, casos como *Authors Guild, Inc. c. Google, Inc.* (2015) y *Authors Guild, Inc. c. Hathitrust* (2014) han construido un sólido precedente legal para permitir TDM en Estados Unidos (Sag, 2009). Esta sección se concentra en explicar el estatuto de uso justo y nombrar los casos clave para ella en este país.

a. *Ley de uso justo*

La doctrina del uso justo de los derechos de autor fue desarrollada inicialmente por los tribunales de los Estados Unidos para permitir la copia no autorizada de obras protegidas por derechos de autor[54]. Los tribunales desarrollaron el uso justo para promover el artículo 1 de la Constitución de los Estados Unidos (en específico el inciso octavo de la octava sección) con el propósito de fomentar el "progreso de la ciencia y las artes útiles" (U.S. Const., 1791, art. 1 § 8) [traducción libre][55]. Si bien los autores son uno de los beneficiarios previstos por el derecho de autor el beneficiario primario y final es el público, cuyo acceso a las obras busca avanzar el conocimiento, mientras que se proporciona una compensación a los autores por su trabajo (U.S. Const., 1791, art. 1 § 8). Es así que los tribunales han reconocido que el objetivo final del derecho de autor es "ampliar el conocimiento y la comprensión del público", al tiempo que otorga a los creadores el monopolio de sus obras (U.S. Const., 1791, art. 1 § 8). El uso justo de los derechos de autor surge como un desarrollo de las prioridades dadas en la Constitución de los Estados Unidos, pero también funciona como una válvula de seguridad para la Primera Enmienda (Cunard *et al.*, 2020)[56].

El uso legítimo se codificó con la sección 107 de la Ley de derechos de autor de 1976 (U.S. Code, título 17, § 107). La sección 107 formalizó el uso justo en un estatuto que incluye cuatro factores que se deben analizar a fin de determinar si existe un uso justo de una obra protegida por el derecho de autor[57]. Los cuatro factores son los siguientes: (i) el propósito y el carácter del uso; (ii) la naturaleza del trabajo protegido por derechos de autor; (iii) la cantidad y sustancialidad de la parte utilizada en relación con la obra protegida por derechos de autor en su conjunto; y (iv) el efecto del uso sobre el mercado potencial o el valor de la obra protegida por derechos de autor (U.S. Code, 2012, título 17, § 107). Cada uno de los cuatro factores debe examinarse de forma independiente y luego ponderarse entre sí[58]. Los cuatro factores de la sección 107 no deben "tratarse de forma aislada [...]

[53] Texto original: "extraction, comparison, classification, or other statistical analysis of language, sound, or image data, or other elements of which a large number of works or a large volume of data is composed;".

[54] Véase sentencia *Folsom c. Marsh* (1841) (denominado como el primer caso de uso justo); asimismo, véase de forma general Samuelson (2017).

[55] Véase el texto original: "progress of science and useful arts,".

[56] Véase también las sentencias relacionadas: *Eldred c. Ashcroft* (2003); *Harper & Row Publishers, Inc. c. Nation Enters*. (1985); y *Nat'l Rifle Ass'n of Am. c. Handgun Control Fed'n of Ohio*, (1994).

[57] Ver sección 107 del título 17 del Código de los Estados Unidos:

> Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include— (1)the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2)the nature of the copyrighted work; (3)the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4)the effect of the use upon the potential market for or value of the copyrighted work (U.S. Code, 2012, título 17, § 107).

[58] El uso legítimo ha sido un concepto en constante evolución. Para el profesor Jaszi, desde la década de 1960 hasta la de 1990, el uso legítimo se había entendido como una excepción que sólo podía utilizarse "si sus actividades no invaden el mercado del titular de los derechos de autor de ninguna manera" (Aufderheide & Jaszi, 2018, p. 88). En 1990, el Juez Federal de Primera Instancia Leval cuestionó la forma en que los tribunales habían entendido –o administrado

[todos] deben explorarse, y los resultados deben sopesarse a la luz de los propósitos del derecho de autor" (*Dr. Seuss Enters., L.P. c. Penguin Books*, 1997, p. 1399) [traducción libre][59]. Cada factor es parte de la pregunta sobre

> cómo definir el límite de los derechos exclusivos del autor original con el fin de servir mejor a los objetivos generales de la ley de derechos de autor de expandir el aprendizaje público mientras se protegen los incentivos de los autores para crear para el bien público[60] (*Folsom c. Marsh*, 1841) [traducción libre].

Bajo el primer factor, la corte considera hasta qué punto la nueva obra es 'transformadora'[61], ya que la obra debe agregar "algo nuevo, con otro propósito o carácter diferente, alterando el primero con nueva expresión, significado o mensaje" (*Campbell c. Acuff-Rose Music, Inc.*, 1994, p. 579) [traducción libre][62]. Bajo el segundo factor, el tribunal considera si la obra protegida por derechos de autor es "del tipo creativo o instructivo que las leyes de derechos de autor valoran y buscan fomentar" (Leval, 1990, p. 1117) [traducción libre][63]. El tercer factor "pregunta si la cantidad y la sustancialidad de la parte utilizada en relación con la obra protegida por derechos de autor en su conjunto son razonables en relación con el propósito de la copia" (*Dr. Seuss Enters., L.P. c. Penguin Books*, 1997, p. 1402) [traducción libre][64]. Finalmente, bajo el cuarto factor, los tribunales deben cuestionar

> si el daño real al mercado resultó del uso del acusado […] y si una conducta generalizada e irrestricta del tipo que lleva a cabo el acusado... resultaría en un impacto sustancialmente adverso en el potencial mercado para el original o sus derivados (*Campbell c. Acuff-Rose Music, Inc.*, 1994, p. 590) [traducción libre][65].

En la práctica, los tribunales tienden a dar más peso a los factores uno y cuatro; pero, si el uso es de naturaleza transformadora, el primer análisis factorial debe preguntar cuál es el propósito del trabajo. Si el propósito es transformador, no debería importar si el uso es comercial o no, y se debe reconocer un uso justo[66].

C. Casos sobre uso justo y minería de textos y datos (TDM)

Actualmente, dos fallos judiciales en Estados Unidos permiten el uso de TDM: el caso *Authors*

---

intuitivamente– el uso justo, y abogó por una interpretación más centrada en el propósito transformador que en el efecto del uso en el mercado potencial o el valor del producto o trabajo protegido por derechos de autor ("Judges do not share a consensus on the meaning of fair use [...]. The opinions reflect widely differing notions [...] [d]ecisions are not governed by consistent principles, but seem to result from intuitive reactions to individual fact patterns") (Leval, 1990, pp. 1106-1107). Asimismo, ver el caso *Campbell c. Acuff–Rose Music, Inc.*, (1994), en el que se sostiene que un propósito transformador hace que el primer factor sea más probable que favorezca el uso justo. Desde Campbell, la lectura del uso legítimo se ha ampliado para dar más peso al elemento transformador –el primer factor–, enfoque comúnmente seguido por la Corte de Apelaciones del Segundo Circuito de los Estados Unidos.

59 Texto original: "The four fair use factors 'are to be weighed together, in light of the objectives of copyright to promote the progress of science and the useful arts'".

60 Véase la sentencia *Folsom c. Marsh* (1841) (denominado como el primer caso de uso justo); asimismo, véase de forma general Samuelson (2017).

61 Véase *Mattel, Inc. c. Walking Mountain Prods*. (2003).

62 Texto original: "something new, with a further purpose or different character, altering the first with new expression, meaning, or message".

63 Texto original: "consider whether the protected writing is of the creative or instructive type that the copyright laws value and seek to foster". Este factor rara vez juega un papel importante en la determinación de una disputa por uso justo. Véase también Patry (2015).

64 Texto original: "whether the amount and substantiality of the portion used in relation to the copyrighted work as a whole was reasonable to the purpose of the copying".

65 Texto original:

> market harm caused by the particular actions of the alleged infringer, but also "whether unrestricted and widespread conduct of the sort engaged in by the defendant... would result in a substantially adverse impact on the potential market" for the original.

66 Con el caso *Campbell c. Acuff-Rose Music*, *Inc.* (1994) los tribunales comenzaron a dar más peso al elemento transformador en sus consideraciones de uso justo, véase *Authors Guild, Inc. c. Google, Inc*. (2015, p. 15):

> Notwithstanding fair use's long common-law history, not until the Campbell ruling in 1994 did courts undertake to explain the standards for finding fair use […]. The Campbell Court undertook a comprehensive analysis of fair use's requirements, discussing every segment of § 107 [...]. [T]he Court made clear that they are ''illustrative and not limitative'' and ''provide only general guidance about the sorts of copying that courts and Congress most commonly ha[ve] found to be fair uses.''[…].The statute ''calls for case-by-case analysis'' and ''is not to be simplified with bright-line rules.

Ver también *Castle Rock Entm't, Inc. c. Carol Pub. Grp., Inc*. (1998) y *Cariou c. Prince* (2013). Asimismo, ver Samberg & Hennesy (2018).

Guild, Inc. c. HathiTrust (2014) y *Authors Guild, Inc. c. Google* (2015)[67]. En este último, el Tribunal permitió que realizara una digitalización no autorizada de obras protegidas por derechos de autor, la creación de una función de búsqueda y la visualización de fragmentos de esas obras en los motores de búsqueda de Google (*Authors Guild, Inc. c. Google*, 2015) . En el *Authors Guild, Inc. c. HathiTrust* (2014), la Corte permitió que las bibliotecas del proyecto Hathitrust digitalizarán obras protegidas por derechos de autor con el fin de permitir búsquedas de texto completo. También autorizó a las bibliotecas miembros del proyecto proporcionar a los usuarios con discapacidades el acceso a las obras de texto completo, y que las bibliotecas conservarán los libros protegidos por derechos de autor en formato digital.

Ambos casos fueron decididos en apelación por el Tribunal Federal de Apelaciones del Segundo Circuito y los usos se consideraron lo suficientemente transformadores como para estar cubiertos por la excepción de uso justo de los derechos de autor. En *Authors Guild, Inc. c. HathiTrust*, la Corte concluyó que la creación de una base de datos de búsqueda de texto completo es un uso transformador: cuando se realiza una búsqueda de palabras, el resultado es diferente en "propósito, carácter, expresión, significado y mensaje de la página (y el libro) de la que se extrae" (2014, p. 18) [traducción libre][68]. Por lo tanto, hay poca o ninguna semejanza entre el trabajo original y los resultados de la búsqueda de texto completo de la Biblioteca digital HathiTrust.

En el caso Google, el Tribunal también determinó que la creación por parte de la empresa de una copia digital de los libros de los demandantes con fines de búsqueda es transformadora: "[e]l propósito de permitir una búsqueda para la identificación de libros que contienen un término de interés para el buscador implica un propósito altamente transformador" (*Authors Guild, Inc. c. Google*, Inc., 2015, p. 21) [traducción libre][69]. El propósito de Google era poner a disposición información significativa sobre los libros de obras copiados, lo que permitía a los buscadores encontrar las obras que contenían una palabra de interés; además, la función 'ngrams' permitió a los lectores conocer la frecuencia de uso en el *corpus* agregado de libros publicados para diferentes períodos históricos. Esas dos funciones demostraron ser lo suficientemente transformadoras como para favorecer el uso justo de las obras protegidas por derecho de autor.

Es importante señalar que los casos de HathiTrust y Google muestran cómo se permite el uso comercial y no comercial de TDM en los Estados Unidos: HathiTrust era una entidad educativa sin fines de lucro, mientras que Google es una corporación comercial con fines de lucro[70]. En ambos casos, se permitió la minería de textos y datos (TDM) después de que se cumplieron los requisitos de transformación de uso justo. En este sentido, si el nuevo trabajo agrega algo nuevo con un propósito adicional o carácter diferente –alterando el primero con una nueva expresión, significado o mensaje–, o si el trabajo cumple con los requisitos transformado-

[67] Ver de forma general a Carroll (2019); ver también el caso *Williams & Wilkins Co. c. Estados Unidos* (1973). Este es el primer caso relevante sobre copias no autorizadas institucionales y sistemáticas con fines de investigación. En el caso *Williams & Wilkins Co. c. Estados Unidos*, un editor de revistas médicas demandó a un instituto de investigación médica del gobierno y a su biblioteca por infracción de derechos de autor. El Departamento de Salud, Educación y Bienestar, a través de los Institutos Nacionales de Salud (NIH) y la Biblioteca Nacional de Medicina (NLM), hizo fotocopias no autorizadas de algunos de los artículos de las revistas científicas de la editorial Medicine, Journal of Immunology, Gastroenterology y Revisiones farmacológicas. Así pues, los investigadores médicos que solicitaron las fotocopias eran investigadores científicos y profesionales que necesitaban los artículos para uso personal en su trabajo científico, y no había intención de duplicarlos para la venta u otra distribución general. Las instituciones también restringieron la copia única de un solo artículo con una extensión limitada de cincuenta páginas. Sobre la base del tipo y contexto de uso, el Tribunal no encontró ninguna infracción, ya que el uso impugnado se consideró como uso legítimo. Así, el razonamiento del tribunal utilizó principalmente el cuarto factor del uso legítimo para llegar a su decisión. El demandante no pudo probar su presunción de perjuicio económico, en el pasado o potencialmente para el futuro. Como señaló el Tribunal, "[the] record simply does not show a serious adverse impact, either on plaintiff or on medical publishers generally, from the photocopying practices of the type of NIH and NLM" (*Williams & Wilkins Co. c. Estados Unidos*, 1973, p. 1359). Por lo tanto, el editor no demostró como un hecho probado la hipótesis hipotética de pérdida de mercado. Pero el Tribunal consideró que se podría causar un perjuicio a la investigación médica y científica si se consideraba ilegal la fotocopia de este tipo. Así, el Tribunal falló a favor de los acusados. Por todo esto, este caso cobró relevancia, ya que se autorizó a las bibliotecas a realizar copias con fines de investigación.

Véanse también otros casos de copia sistemática e institucional de imágenes con fines transformadores cuando las copias cumplían una función diferente a la original: *Kelly c. Arriba Soft Corp.* (2003); *Perfect 10, Inc. c. Amazon.com* (2007); *A.V. ex rel. Vanderhye c. iParadigms, LLC* (2009).

[68] Texto original: "purpose, character, expression, meaning, and message from the page (and the book) from which it is drawn".

[69] Texto original: "[the] purpose of enabling a search for identification of books containing a term of interest to the searcher involves a highly transformative purpose".

[70] Véase *Authors Guild, Inc. c. Google*, Inc. (2015) y *Authors Guild, Inc. c. HathiTrust* (2014).

res del primer factor de uso justo, menor será la importancia de otros factores a fin de determinar si existe un uso legítimo[71].

Aunque los casos actuales permiten el uso comercial y no comercial de TDM, aún quedan preguntas sin resolver (Sag, 2019). No existe una respuesta específica sobre cómo abordar los problemas que surgen en virtud del derecho contractual, las leyes que prohíben la elusión de las medidas de protección tecnológica o los problemas transfronterizos de derechos de autor ¿Qué sucede cuando se desarrolla un proyecto de investigación TDM con catálogos de bibliotecas en diferentes países? ¿Pueden los investigadores desarrollar proyectos TDM sin acceso legal a los datos o la información? ¿Es posible participar en proyectos internacionales y compartir los resultados de los contenidos? ¿Pueden los bibliotecarios negociar para eliminar o reducir las restricciones contractuales sobre los derechos de los investigadores para participar en TDM? A medida que avanza la tecnología, seguirán surgiendo más preguntas sobre cómo nivelar las leyes de derechos de autor con el acceso de los usuarios y la innovación.

IV. FUTURO DEL DESARROLLO DE POLÍTICAS LEGISLATIVAS EN MINERÍA DE TEXTOS Y DATOS

Una legislación integral en TDM se presenta como una herramienta esencial para los investigadores, ya que puede permitir el acceso legal a materiales y bases de datos, así como el derecho de reproducción, almacenamiento y comunicación al público sin que se presenten posibles vulneraciones a los derechos de autor (Francoise, 2020). Una excepción en TDM adecuadamente estructurada puede permitir a los investigadores desarrollar proyectos sobre esta con materiales de acceso abierto y contenidos basados en suscripción; puede permitir TDM para uso comercial y no comercial; y construir análisis y proyectos de TDM no limitados a propósitos de investigación científica[72]. Asimismo, una excepción abierta al respecto debería permitir el almacenamiento del *corpus* o las copias generadas con TDM, además de tener la opción de compartir los resultados del proyecto con terceras personas y sin limitarlo a un círculo privado de contactos. En general, una excepción en TDM puede brindar acceso abierto a todo tipo de usuarios, incluidos, entre otros, investigadores, académicos, organizaciones sin fines de lucro o con fines de lucro.

No obstante, como se vio en las secciones anteriores, las leyes regionales o nacionales aprobadas en TDM carecen de muchas de las características descritas anteriormente. Por ejemplo, los artículos de TDM aprobados en la Directiva europea del mercado único digital (Directiva 2019/790, 2019) serán incompatibles en algunas partes con la reforma de derechos de autor de TDM japonesa de 2018 o las recientes sentencias de Google o HathiTrust del Tribunal de Apelaciones del Segundo Circuito de los Estados Unidos. Mientras que Europa y el Reino Unido distinguen el uso comercial y no comercial, Japón y Estados Unidos no. Además, mientras que Alemania limita el intercambio a un grupo cercano de investigadores, Japón permite el intercambio gratuito sin restricciones. Si bien el uso comercial en Europa puede excluirse mediante contratos, en el Reino Unido, el uso comercial ni siquiera forma parte de las excepciones de TDM.

Asimismo, la mayoría de los países en desarrollo no han iniciado el proceso de actualización de sus leyes de derecho de autor para incluir excepciones que permitan la TDM. La única alternativa con la que cuentan los países sin una legislación dedicada sobre este punto es la adopción de interpretaciones flexibles y abiertas sobre las L&E existentes como el derecho a la investigación, la reprografía digital o el uso privado o personal. Colombia posiblemente podría contar con flexibilidades en su legislación para el uso privado (Ley 23, 1982, art. 37), pero otras legislaciones, como la de Perú (Decreto Legislativo 822, 1996, art. 43 & 48) o Nicaragua (Ley 312, 1999, art. 31), contarían con restricciones sobre la cantidad de uso que se puede hacer sobre una obra. Igualmente, no tener reglas explícitas al respecto incrementa los niveles de incertidumbre dados los nuevos y constantes desarrollos tecnológicos de IA para explorar y explotar la información. Además, los países con una interpretación restrictiva de L&E, como Argentina (Ley 11.723, 1933, art. 10), sin duda prohibirán a los investigadores permitir cualquier TDM sobre obras protegidas por el derecho de autor.

Como lo menciona Okediji (2017), existen beneficios relevantes para la armonización de las leyes básicas de derechos de autor, en este caso, para permitir el flujo transfronterizo de información. La TDM requiere un entorno internacional integral de derechos legales para crecer como una fuente mundial de conocimiento. Al revisar las posibles disposiciones legales de derechos de autor invo-

[71] Ver *Campbell c. Acuff-Rose Music*, *Inc.* (1994) y también *Authors Guild, Inc. c. Google, Inc*. (2015).

[72] Véase Flynn *et al.*: "TDM need not come at the expense of right holders. These reproductions do not compromise the core interests of exclusive rights, which is to prohibit unauthorised reproductions that can substitute for the work of the author" (2020, p. 4).

lucradas en el proceso de aprendizaje automático, las siguientes consideraciones están disponibles.

En primer lugar, una política legislativa debe cuestionar si el acceso lícito debe ser un requisito para la TDM. El acceso legal cubre el contenido basado en una política de acceso abierto, o mediante acuerdos contractuales entre los titulares de derechos y los beneficiarios de la excepción. La política de acceso abierto se refiere "a la información científica que es gratuita para el usuario y que es reutilizable" (European Commission, 2020b) [traducción libre][73], mientras que el contenido del acuerdo contractual cubre todas las suscripciones y el contenido que está disponible gratuitamente en línea. No obstante, las limitaciones al acceso legal no vienen con los contenidos de acceso abierto, sino con los contenidos que requieren una suscripción paga. Cuando el acceso legal está vinculado a los pagos de los servicios de suscripción, la capacidad presupuestaria de la organización pasa a jugar un papel fundamental. Un posible resultado es que solo unas pocas organizaciones de investigación podrán adquirir licencias para todas las bases de datos que son relevantes para un proyecto de investigación en TDM, lo que a cambio limitará el desarrollo de TDM para un número relevante de organizaciones de investigación. Si la capacidad de financiamiento de cada institución determina los resultados de la investigación en TDM, el acceso lícito puede aumentar las diferencias entre las instituciones, poniendo a muchas de ellas en condiciones menos favorables.

En segundo lugar, una política legislativa debe cuestionar si es necesario eliminar la división entre uso comercial y no comercial. Si bien la UE divide el régimen TDM entre uso no comercial y comercial, otros países como Estados Unidos y Japón han evitado ese enfoque, permitiendo TDM sin importar el propósito comercial o el tipo de usuario. Los fallos judiciales de TDM de los Estados Unidos, *Authors Guild, Inc. c. Google, Inc*. (2015) y *Authors Guild, Inc. c. HathiTrust* (2014), han permitido el uso comercial de la investigación de TDM bajo excepciones de uso justo. Japón no distingue entre uso comercial y no comercial. El análisis de la información no tiene que realizarse necesariamente con fines de investigación científica y la TDM está abierta a todos los usuarios. Este enfoque sigue el objetivo de Japón de promover el desarrollo de las industrias de IA y el *big data*. En consecuencia, legislaciones que restringen la TDM en sus territorios al uso no comercial, eventualmente podrían ver una fuga de proyectos comerciales a otros países donde ese tipo de uso sí esté permitido.

En tercer lugar, una política legislativa debe incluir el almacenamiento, la comunicación y distribución de datos. En un proyecto TDM, compartir información es una segunda parte importante del proceso, ya que permite que otros investigadores colaboren o incluso desarrollen nuevos proyectos de investigación a partir de la misma información. Compartir ayuda a un mayor desarrollo del conocimiento, la misma función que tiene un libro cuando se imprime.

V. CONCLUSIONES

El panorama ofrece un escenario muy desigual, dividido e incierto para los investigadores de todo el mundo. Como cada investigador depende de sus leyes de derechos de autor nacionales o regionales, los resultados del acceso a los materiales siguen siendo restringidos. De no contar con instrumentos armoniosos, estos colocarán a los investigadores y usuarios en posiciones desfavorables, ya que la investigación de TDM en diferentes campos del conocimiento seguirá dependiendo de las restricciones de las variables de derechos de autor. Además, la falta de una legislación uniforme podría aumentar la brecha científica y de innovación entre las naciones desarrolladas y las menos desarrolladas.

Japón y Estados Unidos son un ejemplo interesante sobre cómo legislar en TDM. No obstante, aun así, para que la TDM fomente la innovación, los países seguramente tendrán que eliminar barreras como el acceso lícito, la división entre uso comercial y no comercial, la limitación para compartir los datos, el *corpus*, la investigación o los resultados de los proyectos de TDM, así como cualquier limitación para compartir y comunicar la información recogida y obtenida a partir de los proyectos en TDM.

La mayoría de los países en desarrollo no han iniciado el proceso de actualización de sus leyes de derecho de autor para incluir excepciones que permitan la TDM. La única alternativa con la que cuentan los países sin una legislación dedicada sobre este punto es la adopción de interpretaciones flexibles y abiertas sobre las L&E existentes, como el derecho a la investigación, la reprografía digital o el uso privado o personal.

Asimismo, no tener reglas explícitas al respecto incrementa los niveles de incertidumbre dados los nuevos y constantes desarrollos tecnológicos de IA para explorar y explotar la información. Los países con una interpretación restrictiva en sus excepciones y limitaciones, sin duda alguna, prohibirán a los investigadores permitir cualquier TDM sobre obras protegidas por el derecho de autor.

[73] Texto original: "scientific information that is free of charge to the user and is reusable".

REFERENCIAS

Aufderheide, P., & Jaszi, P. (2018). *Reclaiming Fair Use* (2da ed.). University of Chicago Press.

Barlow, H. B. (1989). Unsupervised learning. *Neural Computation, 1*(3), 295-311. https://doi.org/10.1162/neco.1989.1.3.295

Borghi, M. (2016). *Text and Data Mining*. https://www.copyrightuser.org/understand/exceptions/text-data-mining/

Borghi, M., & Karapapa, S. (2013). *Copyright and Mass Digitization: A Cross-Jurisdictional Perspective*. Oxford University Press.

Carroll, M. (2019). Copyright and the Progress of Science: Why Text and Data Mining Is Lawful. *UC Davis Law Review*, *53*(2), 893-964.

Caspers, M., Guibault, L., McNeice, K., Piperidis, S., Pouli, K., Eskevich, M., & Gavrilidou, M. (2017). *Baseline report of policies and barriers of TDM in Europe (extended version).* FutureTDM project report. https://www.futuretdm.eu/wp-content/uploads/FutureTDM_D3.3-Baseline-Report-ofPolicies-and-Barriers-of-TDM-in-Europe.pdf

Caspers, M., & Guibault, L. (2016). *Deliverable 3.3+ Baseline report of policies and barriers of TDM in Europe*. https://project.futuretdm.eu/wp-content/uploads/2017/05/FutureTDM_D3.3-Baseline-Report-of-Policies-and-Barriers-of-TDM-in-Europe.pdf

Castaneda, R., Arroyo, P., & Loza, L. (2020). Assessing Countries Sustainability: A Group Multicriteria Decision Making Methodology Approach. *Journal of Management and Sustainability*, *10*(1), 174-188.

Castle, N. (13 de julio de 2017). Supervised vs. Unsupervised Machine Learning [Entrada de blog]. https://www.datascience.com/blog/supervised-and-unsupervised-machine-learning-algorithms

Coglianese, C., & Lehr, D. (2017). Regulating by Robot: Administrative Decision Making in the Machine-Learning Era. *The Georgetown Law Journal, 105*, 1147-1223.

Congressional Research Service [CRS] (2017). *Laurie A. Harris, Overview of Artificial Intelligence*. https://crsreports.congress.gov/product/pdf/IF/IF10608/3.

Cunard, J. P., Keller, B., & Potenza, M. (2020). *Copyright Fair Use. Copyright*. Thomsons Reuters Practical Law.

Davis, J. (14 de octubre de 2020). Zillow uses Analytics, Machine Learning to Disrupt with Data. *Information Week*. http://www.informationweek.com/big-data/zillow-uses-analytics-machine-learning-to-disrupt-with-data/d/d-id/1327175

Ducato, R., & Strowel, A. (19 de marzo de 2019). Limitations to Text and Data Mining and Consumer Empowerment. Making the Case for a Right to 'Machine Legibility'. [Entrada de blog]. http://copyrightblog.kluweriplaw.com/2019/03/19/limitations-to-text-and-data-mining-and-consumer-empowerment-making-the-case-for-a-right-to-machine-legibility/

Dusollier, S. (2003). Tipping the Scale in Favor of the Right Holders: The European Anti-Circumvention Provisions. En E. Becker, W. Buhse, D. Günnewig & N. Rump (eds.), *Digital Rights Management* (pp. 462-478). Springer.

Eskevich, M., & Van Den Bosch, A. (2016). *Deliverable D3.1: Research Report on TDM Landscape in Europe*. https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5a5c961d0&appId=PPGMS

European Parliamentary Research Service [EPRS] (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

European Commission (2020a). *Shaping Europe's digital future*. https://ec.europa.eu/digital-single-market/en/copyright

(2020b). *Open Access*. https://ec.europa.eu/info/research-and-innovation/strategy/strategy-2020-2024/our-digital-future/open-science/open-access_en

Fagan, F. (2015). From Policy Confusion to Doctrinal Clarity: Successor Liability from the Perspective of Big Data. *Virginia Law & Business Review*, *9*(3), 391-451.

Flynn, S., Geiger, C., Quintais, J., Margoni, T., Sag, M., Guibault, L., & Carroll, M. (2020). Implementing User Rights for Research in the Field of Artificial Intelligence: A Call for In-

ternational Action. *European Intellectual Property Review*, (7), 1-12. https://dx.doi.org/10.2139/ssrn.3578819

Flynn, S., Izquierdo, H.A., & Palmedo, M. (2021). *Research for Text and Data Mining in Comparative Copyright Law*. Program on Information Justice and Intellectual Property, Forthcoming.

Francoise, C. (10 de Junio de 2020). Text and Data Mining: (Articles 3 and 4 of the EU-DSM) by REBIUN's Copyright working group [Entrada de blog]. https://blogs.ifla.org/lpa/2020/06/10/text-and-data-mining-articles-3-and-4-of-the-eu-dsm/

Geiger, C. Frosio, G., & Bulayenko, O. (2018a). The EU Commission's Proposal to Reform Copyright Limitations: A Good but Far Too Timid Step in the Right Direction. *European Intellectual Property Review*, *40*(1), 4-15.

(2018b). Text and Data Mining in the Proposed Copyright Reform: Making the EU Ready for an Age of Big Data?. *International Review Intellectual Property and Competition Law*, *49*(7), 814-844.

(2018c). *The Exception for Text and Data Mining (TDM) in the Proposed Directive on Copyright in the Digital Single Market - Legal Aspects* (Centre for International Intellectual Property Studies (CEIPI) Research Paper No. 2018-02). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3160586 .

(2019). Text and Data Mining: Articles 3 and 4 of the Directive 2019/790/EU. En C. Saiz García & R. Evangelio Llorca (eds.), *Propiedad Intelectual y Mercado Único Europeo* (pp. 23-64). Tirant lo Blanch.

Guerra, P., & Tamburello, P. (2018). *Modernizing Cybersecurity Operations with Machine Intelligence, Advanced Threat Detection, Hunting, and Analysis*. O' Reilly Media Inc. https://www.oreilly.com/library/view/modernizing-cybersecurity-operations/9781492035992/

Hassabis, D., Kumaran, D., Summerfield, C., & Botvinick, M., (2017). Neuroscience-inspired artificial intelligence. *Neuron, 95*(2), 245-258. https://doi.org/10.1016/j.neuron.2017.06.011

Hilty, R., Harhoff, D., & Drexl, J. (2016). *Position Statement of the Max Planck Institute for Innovation and Competition on the Proposed Modernisation of European Copyright Rules*. https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/MPI_Position_Statement_Part_B_Chapter_1_Update23022017.pdf

Hinton, G. E., & Sejnowski, T. J. (eds.) (1999). *Unsupervised learning: Foundations of neural computation in Unsupervised learning: Foundation computation*. MIT Press.

HM Government (2012). *Modernising Copyright: A modern, robust and flexible framework, Government response to consultation on copyright exceptions and clarifying copyright law*. https://www.mpaonline.org.uk/wp-content/uploads/2017/09/Modernising_Copyright_-_a_modern_robust_and_flexible_framework_-_Government_response.pdf.

Hugenholtz, B. (24 de julio de 2019). The New Copyright Directive: Text and Data Mining (Articles 3 and 4) [Entrada de blog]. http://copyrightblog.kluweriplaw.com/2019/07/24/the-new-copyright-directive-text-and-data-mining-articles-3-and-4/

Japan Copyright Office [JCO] (2019). *Outline of the Amendments to the Copyright Act in 2018*.

Le, Q. V., Ranzato, M., Monga, R., Devin, M., Chen, K., Corrado, G., Dean, J., & Ng, A.Y. (2012). *Building High-level Features Using Large Scale Unsupervised Learning*. Trabajo presentado en 29th International Conference on Machine Learning, Edimburgo, Escocia. https://static.googleusercontent.com/media/research.google.com/en//archive/unsupervised_icml2012.pdf

Lehr, D., & Ohm, P. (2017). Playing with the Data: What Legal Scholars Should Learn About Machine Learning. *UC Davis Law Review*, *51*(2), 653-717.

Leval, P. N. (1990). Toward a Fair Use Standard. *Harvard Law Review*, *103*(5), 1105-1136.

Litman, J. (1994). The Exclusive Right to Read. *Cardozo Arts & Entertainment Law Journal*, *13*(29), 34-43.

Margoni T., & Dore, G. (2016). *Why We Need a Text and Data Mining Exception (But it is Not Enough.* Trabajo presentado en Language Resources and Evaluation Conference (LREC 2016, 10th ed.), Portorož, Slovenia. https://doi.org/10.5281/zenodo.248048

Metz, C. (4 de setiembre de 2020). Now Anyone Can Tap the AI Behind Amazon's Recommendations. *WIRED*. http://www.wired.com/2015/04/now-anyone-can-tap-ai-behind-amazons-recommendations/

MIT Lincoln Laboratory [MIT LL] (2019). *Artificial Intelligence: Short History, Present Developments, and Future Outlook*. https://www.ll.mit.edu/r-d/publications/artificial-intelligence-short-history-present-developments-and-future-outlook-0

MIT Sloan Management Review [MIT SMR] (2020). *Connections Custom Research Report, How AI Changes the Rules: New Imperatives for the Intelligent Organization, SAS*. https://sloanreview.mit.edu/sponsors-content/how-ai-changes-the-rules-new-imperatives-for-the-intelligent-organization/

Mokhtarian, E. (2018). The Bot Legal Code: Developing a Legally Compliant Artificial Intelligence. *Vanderbilt Journal of Entertainment and Technology Law*, *21*(1), 145-207.

Myers, S. (27 de abril de 2007). Estonia removes Soviet-era war memorial after a night of violence. *New York Times*. https://www.nytimes.com/2007/04/27/world/europe/27iht-estonia.4.5477141.html

New America (2017). *Full Translation: China State Council, A Next Generation Artificial Intelligence Development Plan*. https://www.newamerica.org/documents/1959/translation-fulltext-8.1.17.pdf

Office of Scholarly Communication (2013). *UC Systemwide Academic Senate Open Access Policy*.

Okediji, R. (ed.) (2017). *Copyright Law in an Age of Exceptions and Limitations*. Cambridge University Press.

Organización Mundial de Propiedad Intelectual (2020). *WIPO Conversation on Intellectual Property and Artificial Intelligence*. https://www.wipo.int/about-ip/en/artificial_intelligence/policy.html#:~:text=The%20WIPO%20Conversation%20on%20IP,that%20policymakers%20need%20to%20ask.

PubMed Central (PMC) (s/f). *US National Library of Medicine National Institutes of Health*. https://www.ncbi.nlm.nih.gov/pmc/about/intro/

Quintais, J. (2020). The New Copyright in the Digital Single Market Directive: A Critical Look. *European Intellectual Property Review*, (1), 1-23. https://dx.doi.org/10.2139/ssrn.3424770

Rosati, E. (2019). *Copyright and the Court of Justice of the European Union*. Oxford University Press.

Sag, M. (2009). Copyright and Copy-Reliant Technology. *Northwestern University Law Review*, *103*(4), 1607-1682.

(2019). The New Legal Landscape for Text Mining and Machine Learning. *Journal of the Copyright Society of the USA*, *66*, 1-64.

Samberg, R., & Hennesy, C. (2018). Law & Literacy In Non-consumptive Text Mining: Guiding Researchers Through The Landscape Of Computational Text Analysis. En S. Benson (ed.), *Copyright Conversation: Rights Literacy, in A Digital World* (pp. 289-315). UC Berkeley Previously Published Works.

Samuelson, P. (2017). Justifications for Copyright Limitations & Exceptions. En R. Okediji (ed.), *Copyright Law in an Age of Limitations and Exceptions*, 12-60. Nueva York: Cambridge University Press. https://doi.org/10.1017/9781316450901.003

(12 de julio de 2018). The EU's Controversial Digital Single Market Directive – Part II: Why the Proposed Mandatory Text- and Data-Mining Exception Is Too Restrictive [Entrada de blog]. http://copyrightblog.kluweriplaw.com/2018/07/12/eus-

Select Committee on Artificial Intelligence of the National Science & Technology Council (2019). *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update*. https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf

Spielkamp, M. (2017). Inspecting algorithms for bias. *MIT Technology Review*, *120*(4), 96-98.

SYNYO GmbH, (2015). *Reducing Barriers and Increasing Uptake of Text and Data Mining for Research Environments using a Collaborative Knowledge and Open Information Approach*. https://www.futuretdm.eu/wp-content/uploads/FutureTDM_D3.3-Baseline-Report-of-Policies-and-Barriers-of-TDM-in-Europe-1.pdf

Triaille, J., Meeûs d'Argenteuil, J., & Francquen, A. (2014). *A Study on the legal framework*

of text and data mining (TDM). https://op.europa.eu/en/publication-detail/-/publication/074ddf78-01e9-4a1d-9895-65290705e2a5/language-en

Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind*, *59*(236), 433-460.

U.S. Senate, Subcommittee On Space, Science, And Competitiveness, Committee On Commerce, Science, And Transportation (2016). *The Dawn of Artificial Intelligence: Hearing Before the Subcomm. on Space, Sci., & Transp.* (114th Congress) (pp. 114-562). https://www.govinfo.gov/content/pkg/CHRG-114shrg24175/pdf/CHRG-114shrg24175.pdf

Ueno, T. (2019). TDM Exception in Japan, Possible implication for Europe?. Trabajo presentado en Challenges of the Directive 2019/790 on Copyright and Related Rights in the Digital Single Market de la Facultad de Derecho de la Universidad Jagellónica, Cracovia, Polonia. https://ipwi.uj.edu.pl/documents/122195199/144296432/Ueno_2019_Cracow_Comment.pdf/adf57b6a-ad86-4bd6-94b0-4bbac61b049c

(2021). The Flexible Copyright Exception for "Non-Enjoyment" Purposes- Recent Amendment in Japan and its Implication. *GRUR International*, *70*(2), 145-152.

UK Intellectual Property Office (2014). *Exceptions to copyright: Research*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/375954/Research.pdf

Zhongzhi, S. (2011). Advanced Artificial Intelligence. *Series on Intelligence Science*, *1*. https://ishare.iask.sina.com.cn/f/34881213.html

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

A.V. ex rel. Vanderhye c. iParadigms, LLC, 562 F.3d 630, 640 (4th Cir. 2009).

Authors Guild, Inc. c. Google, Inc., 804 F.3d 202 (2d Cir. 2015).

Authors Guild, Inc. c. HathiTrust, 755 F.3d 87 (2d Cir. 2014).

Campbell c. Acuff–Rose Music, Inc., 510 U.S. 569 (1994).

Cariou c. Prince, 714 F.3d 694, 708 (2nd Cir. 2013).

Castle Rock Entm't, Inc. c. Carol Pub. Grp., Inc., 150 F.3d 132, 141-42 (2d Cir.1998).

Convenio de Berna para la Protección de las Obras Literarias y Artísticas, 9 de septiembre de 1886, revisado en Paris 24 de julio de 1971, 1161 U.N.T.S. 3.

Copyright Act of 1976, 17 U.S. Code § 107 (2012) (Limitaciones a los derechos exclusivos: Uso justo) (EE.UU.).

Copyright, Designs and Patents Act 1988, c. 48 (Reino Unido).

Decreto Legislativo 822, Ley sobre el Derecho de Autor, 23 de abril de 1996 (Perú).

Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos, 1996 O.J. (L 77) 20 (UE).

Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, 2001 O.J. (L 160) 10 (UE).

Directiva 2017/1564 del Parlamento Europeo y del Consejo, de 13 de setiembre de 2017, sobre ciertos usos permitidos de determinadas obras y otras prestaciones protegidas por derechos de autor y derechos afines en favor de personas ciegas, con discapacidad visual o con otras dificultades para acceder a textos impresos, y por la que se modifica la Directiva 2001/29/CE relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, 2017 O.J. (L 242) 6 (UE).

Directiva 2019/790 del Parlamento Europeo y del Consejo, de 17 de mayo de 2019, sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE (Directiva del mercado único digital), 2019 O.J. (L 130) 92 (UE).

Dr. Seuss Enters., L.P. c. Penguin Books, 109 F.3d 1394, 1399 (9th Cir.1997).

Eldred c. Ashcroft, 537 U.S. 186, 219-20 (2003).

Folsom c. Marsh, 9. F. Cas. 342 (C.C.D. Mass. 1841).

Harper & Row Publishers, Inc. c. Nation Enters., 471 U.S. 539, 560 (1985).

Kelly c. Arriba Soft Corp., 336 F.3d 811, 822 (9th Cir. 2003).

L. 23/1982, 19 de febrero de 1982, Diario Oficial [D.O.] 35.949 (Colom.).

Ley 11.723, Régimen Legal de la Propiedad Intelectual [RLPI], 30 de septiembre de 1933, , B. O. 11793 (Arg.)

Ley 312, 6 de julio de 1999, Ley de Derechos de Autor y Derechos Conexos [LDADC], La Gaceta, Diario Oficial [L.G.], 1 de setiembre de 1999 (Nicar.).

Ley 4 de 1998, Ley sobre Derechos de Autor (Cap. 300, modificada por la Ley 1 de 2006) (Barb.).

Ley de Derecho de Autor, Act 48 de 6 de mayo de 1970 (modificado por Act 72 de 13 de julio de 2018) (Japón).

Ley de Derecho de Autor [LDA], Capítulo 252 de las Leyes de Belice, 31 de diciembre de 2000 (Belice).

Mattel, Inc. c. Walking Mountain Prods., 353 F.3d 792, 800 (9th Cir.2003).

Nat'l Rifle Ass'n of Am. c. Handgun Control Fed'n of Ohio, 15 F.3d 559, 562 (6th Cir. 1994).

Perfect 10, Inc. c. Amazon.com, Inc., 508 F.3d 1146, 1169 (9th Cir. 2007).

Rb Dan Haag 5 februari 2020, NJ 2020, 368 m.nt. van E.J. Dommering (NJCM et al./Países Bajos) (Países Bajos).

Reglamento 2017/1563 del Parlamento Europeo y del Consejo, de 20 de setiembre de 2017, sobre el intercambio transfronterizo entre la Unión y terceros países de ejemplares en formato accesible de determinadas obras y otras prestaciones protegidas por derechos de autor y derechos afines en favor de personas ciegas, con discapacidad visual o con otras dificultades para acceder a textos impresos, 2017, O.J. (L 242) 1 (UE).

Urheberrechtsgesetz [UrhG] [Ley de Derechos de Autor y Derechos Conexos], 9 de septiembre de 1965, BGBl I en 1273, modificado por el artículo 1 de la Ley de 1 de septiembre de 2017 (Alemania).

Williams & Wilkins Co. c. United States, 487 F.2d 1345 (Ct. Cl. 1973), aff'd by an equally divided Court, 420 U.S. 376 (1975).

RODRÍGUEZ ANGOBALDO

ABOGADOS

RODRÍGUEZ
HEREDIA
ABANTO
PINILLOS
VARSI

10.18800/themis.202101.019

BLOCKCHAIN Y PROPIEDAD INTELECTUAL: APLICANDO UNA TECNOLOGÍA INNOVADORA EN LA GESTIÓN DE DERECHOS INTANGIBLES

BLOCKCHAIN AND INTELLECTUAL PROPERTY: APPLYING A NEW TECHNOLOGY IN THE MANAGEMENT OF INTANGIBLE RIGHTS

María del Carmen Alvarado Bayo*
Rodrigo, Elías & Medrano

Daniela Supo Calderón**
Rodrigo, Elías & Medrano

One of the emerging technologies that is gaining great relevance in recent years and that promises to revolutionize transactions between individuals is blockchain, a technology considered to be the leader of the so-called fourth industrial revolution due to its ability to manage digital assets and facilitate their transfer under a trustworthy decentralized scheme.

This article starts from the premise that the Law must keep abreast of and adapt to technological changes in the contemporary world. Specifically, this work addresses blockchain technology and its application in a specific area of Law: Intellectual Property. In that order of ideas, the authors begin by taking a historical journey of blockchain technology, from its origins, to its regulation in various countries of the world. Then, they explain the operation and characteristics of the aforementioned technology to, finally, address its application in the Intellectual Property field and the advantages that blockchain offers to this branch of Law.

Keywords: Blockchain; Bitcoin; intellectual property; smart contracts; copyright; trade secret.

Una de las nuevas tecnologías que está cobrando gran relevancia en los últimos años y que promete revolucionar las transacciones entre individuos es el blockchain*, tecnología considerada como líder de la denominada cuarta revolución industrial por su capacidad de gestionar activos digitales y facilitar su transferencia bajo un esquema descentralizado confiable.*

El presente artículo parte de la premisa de que el Derecho debe mantenerse al tanto y adaptarse a los cambios tecnológicos del mundo contemporáneo. Específicamente, este trabajo aborda la tecnología blockchain *y su aplicación en un área específica del Derecho: la Propiedad Intelectual. En ese orden de ideas, las autoras empiezan realizando un recorrido histórico de la tecnología* blockchain*, desde sus orígenes, hasta su regulación en varios países del mundo. Luego, explican el funcionamiento y las características de la mencionada tecnología para, finalmente, abordar su aplicación en el campo de la Propiedad Intelectual y las ventajas que ofrece el* blockchain *en esta rama del Derecho.*

Palabras clave: Blockchain*; Bitcoin; Propiedad Intelectual;* smart contracts*; derechos de autor; secretos empresariales.*

* Abogada. Socia en Rodrigo, Elías & Medrano Abogados (Lima, Perú). Contacto: mcalvarado@estudiorodrigo.com.

** Abogada. Asociada en Rodrigo, Elías & Medrano Abogados (Lima, Perú). Contacto: dsupo@estudiorodrigo.com.

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 25 de enero de 2021, y aceptado por el mismo el 09 de abril de 2021.

I. INTRODUCCIÓN

La última década se ha caracterizado por el desarrollo y surgimiento de nuevas tecnologías que han promovido cambios en diversos sectores y dinámicas de la sociedad. Dicho de otra forma, actualmente vivimos en una época de cambios tecnológicos disruptivos, en la que se dan avances con una velocidad que no tiene precedentes en la historia. Así, algunas de estas nuevas tecnologías proponen cambios en sectores caracterizados por su bajo nivel de adaptación e innovación, como, por ejemplo, el Derecho, disciplina en la cual muchas veces se ha demostrado cierta resistencia ante los cambios que la tecnología brinda. Sin embargo, el Derecho –incluyendo la forma de ejercerlo– tiene la obligación de mantenerse actualizado y adaptarse ante estos cambios. La experiencia nos ha enseñado que la transformación y adaptación continua se han consolidado como base de las organizaciones exitosas. La innovación, adaptación y transformación no deben ser una opción sino una constante y el Derecho no debe ser ajeno a ello.

Lo dicho no se traduce en que deba existir una regulación específica ante cada cambio o incorporación que la tecnología ofrezca, pues, en la mayoría de estos casos, el cambio se adecuará al marco regulatorio vigente. Sostener lo contrario generaría una sobrerregulación cuando a lo que idealmente se debe apuntar es a una autorregulación. Sin embargo, somos enfáticas en señalar que, en los casos en que nos encontremos ante una nueva tecnología que trae consigo un impacto que implique un potencial cambio en todo tipo de relaciones en la sociedad, las ciencias jurídicas tienen el deber de estudiarla y comprenderla con el fin de establecer el mejor mecanismo de regulación posible (Núñez Miller, 2017, p. 49).

Precisamente, una de las tecnologías que promete transformar de manera radical diversos aspectos de la sociedad es la tecnología *blockchain*. Numerosos especialistas del sector de la tecnología la han colocado a la altura de la invención de la computadora portátil (*laptop*) en 1975 y del internet en 1993, e incluso, se ha considerado que esta tecnología lidera la denominada cuarta revolución industrial que vivimos actualmente (Endemann, 2020).

El principal potencial revolucionario y transformador de la tecnología *blockchain* se encuentra en su capacidad de gestionar activos digitales y facilitar su transferencia bajo un esquema descentralizado confiable, sin la necesidad de entidades centrales que garanticen el cumplimiento de las transacciones o proporcionen confianza en el sistema a los usuarios (Preukschat, 2017). En esta línea, así como el internet significó un cambio fundamental en relación con la accesibilidad y la forma en la que compartimos la información, la tecnología *blockchain* promete revolucionar y cambiar trascendentalmente la forma en la que se realizan transacciones entre individuos, empresas o incluso, máquinas. No debemos perder de vista que uno de los grandes beneficios que trae consigo la tecnología *blockchain* es que permite disponer de un sistema que garantice la absoluta transparencia.

Si bien la tecnología *blockchain* data de hace más de diez años, su uso ha venido alcanzando un mayor grado de madurez en los últimos cinco años. Ello se ve reflejado, por ejemplo, en el incremento de solicitudes de patentes relacionadas con esta tecnología durante el periodo 2015-2017[1], o en las mayores inversiones realizadas a través de nuevos modelos de financiamiento para el ecosistema *blockchain* basados en la oferta inicial de *Initial Coin Offering* (en adelante, ICOs)[2]. Sin embargo, a pesar de estos notables avances con relación al uso de la tecnología *blockchain*, lo cierto es que muchos autores comparten la opinión de que aún faltan varios años para que la sociedad se encuentre en la capacidad de ostentar una transformación digital liderada por el *blockchain*.

En esta línea, somos conscientes de que en el Perú la tecnología *blockchain* representa un concepto lejano y desconocido por muchos, por lo que es altamente probable que nuestro marco regulatorio tarde años en regular esta tecnología. Sin embargo, debido a lo demostrado a la fecha por la tecnología *blockchain* en países del primer mundo y el indiscutible potencial que implica, consideramos que estamos ante la obligación de realizar estudios sobre cómo funciona esta tecnología y, con ello, ir familiarizándonos con ella. No debemos olvidar que en nuestro país muchas veces desaprovechamos las oportunidades que brinda el proceso evolutivo de una nueva tecnología al no entenderlo y anticiparlo adecuadamente.

De acuerdo con ello, en línea con lo señalado en los primeros párrafos, al estar frente a una tecnología que promete generar un cambio sustancial, como abogados, tenemos la obligación de aproximarnos a ella, adoptarla y difundirla. Sabemos que

[1] Véase a Tian (2017).

[2] En pocas palabras, una ICO busca la financiación de una iniciativa mediante la emisión de una moneda sobre la tecnología *blockchain*, las criptomonedas.

ello no es una tarea fácil, pues nos encontramos frente a una tecnología compleja, cuya base recae en la criptografía y en algoritmos de consenso, a lo que debe sumarse que puede tener diversas configuraciones (Herran Aguirre, 2019). Sin embargo, no cabe duda de que su eventual inclusión y regulación en nuestro ordenamiento jurídico traerá desafíos importantes.

Teniendo en cuenta lo expuesto, el propósito del presente artículo es, en primer lugar, dar algunos alcances en relación con la forma de funcionamiento y características de esta tecnología, ya que consideramos que al referirnos a aspectos claves en relación con los puntos señalados, se hará posible comprender el potencial que tiene la tecnología *blockchain*. Una vez abordado este primer punto, pasaremos a desarrollar el potencial y uso del *blockchain* en una rama específica: la Propiedad Intelectual. Es precisamente en esta rama que las características de la tecnología *blockchain* han demostrado ser de gran utilidad y sin duda alguna aportan importantes beneficios para la gestión de este tipo de derechos.

II. UN REPASO A LA EVOLUCIÓN HISTÓRICA DE LA TECNOLOGIA *BLOCKCHAIN*

La tecnología *blockchain* se empieza a concebir en el año 2008 a partir de la publicación del *white paper* Bitcoin: A Peer-to-Peer Electronic Cash System[3] publicado bajo el seudónimo Satoshi Nakamoto[4]. Así, el origen del *blockchain*, sin duda, se encuentra íntimamente ligada a Bitcoin, sin embargo, se debe tener presente que esta relación cercana no los hace sinónimos. En términos prácticos: la tecnología *blockchain* es la base sobre la cual funciona el Bitcoin y otras criptomonedas, pero no está exclusivamente asociada con estas (Swan, 2015). Así, la importancia del Bitcoin en la historia de la tecnología *blockchain* recae en que fue la primera aplicación de esta tecnología. De acuerdo con ello, el Bitcoin y otras criptomonedas representan ejemplos claros en relación con la utilidad del *blockchain* en una aplicación específica.

Es un hecho, entonces, que Bitcoin juega un papel fundamental en el camino de la tecnología *blockchain*. Sin embargo, en el presente artículo no nos enfocaremos en este, sino en la tecnología que se encuentra detrás y que permite su funcionamiento. Sin perjuicio de ello, al compartir ambos conceptos el mismo origen, también comparten la misma historia. Por ello, con el fin de abordar la historia y fundamentos de la tecnología *blockchain*, nos referiremos a dos personajes ligados a la historia del Bitcoin y cuyas ideas son el sustento de lo que hoy conocemos como *blockchain.*

En primer lugar, debemos hablar del criptógrafo David Chaum, reconocido por ser el pionero de la criptografía aplicada al medio digital y 'el padre del dinero digital'. David Chaum es el autor del *paper* denominado "Blind signatures for untraceable payments" (1982), que sería considerado el primer protocolo de dinero digital. En pocas palabras, el sistema planteado por Chaum en el referido *paper* permitía crear un sistema criptográfico de pagos digitales introduciendo por primera vez el concepto de *blind signature*[5] (Chaum, 1982). Es a través de este trabajo que el mundo conoció la primera aproximación al dinero digital mediante criptografía de firma ciega.

Posteriormente, en el año 1990, Chaum creó la empresa DigiCash Inc., la cual tuvo como objetivo crear diversos servicios de dinero electrónico. Es a través de esta empresa que desarrolla el *eCash*, que es considerado una versión avanzada de su sistema criptográfico de pagos digitales. El *eCash* se trataba de un sistema digital de transferencia de fondos de forma anónima y fue considerado pionero en criptomonedas. Su objetivo era certificar la privacidad de las personas que hacen uso del internet para realizar micropagos. En 1994, en el marco de la First International Conference on the World-Wide Web, realizada en Ginebra, Suiza, David Chaum demostró, por primera vez en el mundo, cómo a través del *eCash* era posible realizar pagos con dinero electrónico empleando solamente un *software* (Vigna & Casey, 2016). Es por ello que la prensa lo denominó como *'world's first electronic cash payment over computer network'.*

En segundo lugar, corresponde referirnos a Nick Szabo, que, al igual que David Chaum, se adelantó generaciones a su época y, desde la década de los noventa, empezó a elaborar teorías que el día de

[3] Véase a Nakamoto (2008).

[4] A la fecha, nadie conoce la identidad de Satoshi Nakamoto, no habiendo sido posible conocer si se trata de una persona, una empresa o grupo que actúa bajo ese seudónimo.

[5] Según Wikipedia (2021),

> In cryptography a **blind signature** as introduced by David Chaum is a form of digital signature in which the content of a message is disguised (blinded) before it is signed. The resulting blind signature can be publicly verified against the original, unblinded message in the manner of a regular digital signature. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties. Examples include cryptographic election systems and digital cash schemes.

hoy son los cimentos de la tecnología *blockchain*. Específicamente, a Nick Szabo se le atribuyen dos importantes hechos: (i) desarrollar el concepto de *smart contract*; y (ii) ser el creador de Bit gold, considerado el precursor del Bitcoin.

En relación con su primer aporte, en 1995, a través de una publicación denominada Smart Contract Glossary, Szabo le enseñó por primera vez al mundo los fundamentos de los denominados *smart contracts*. Un año después, publicó el *paper* "Smart Contracts: Building Blocks for Digital Markets", a través del cual estableció las bases y el funcionamiento de los contratos inteligentes desarrollados en plataformas digitales. En palabras de Nick Szabo,

> the basic idea of smart contracts is that many kinds of contractual clauses (such as liens, bonding, delineation of property rights, etc.) can be embedded in the *hardware* and *software* we deal with, in such a way as to make breach of contract expensive (if desired, sometimes prohibitively so) for the breacher (1996, p.1)[6].

Hoy en día, una de las aplicaciones más prometedoras del *blockchain* es el contrato inteligente, pues se trata de una herramienta capaz de ejecutar transacciones y acuerdos de forma automática bastando únicamente que estas transacciones se programen en un *software* determinado.

En 1998, Szabo presentó un trabajo en el que desarrolló una moneda digital, Bit gold, que poseía bastantes aspectos de la estructura fundamental que daría a luz a lo que hoy en día conocemos como Bitcoin, por lo que es considerado como 'el precursor del Bitcoin'. Este trabajo tuvo como finalidad proporcionar una moneda digital segura, descentralizada y a la que pudiese tener acceso cualquier persona. Sin perjuicio de que el proyecto nunca salió adelante, es claro que las ideas en las que se sustentó el Bit gold se adelantaron conceptualmente diez años a la creación del Bitcoin.

Finalmente, también es importante hacer referencia al *paper* denominado Formalizing and Securing Relationships on Public Networks, publicado en 1997 por Szabo. En el mismo se narraba la importancia de la era digital y el cambio radical que esta planteaba en las relaciones de trabajo y confianza. Así, hacía énfasis en que la criptografía y los *smart contracts* serían la herramienta primordial para adaptarse e insertar aquellos cambios a la vida cotidiana, en lo que acertó.

Tal como se puede apreciar, los trabajos y aportes mencionados datan de los años 1980 a 1998. En 1982, David Chaum presentó un *paper* perfectamente elaborado que demostraba la posibilidad de concebir una moneda digital transfronteriza y no emitida por un banco y, en 1996, Szabo presentó un tipo de contrato que, en pocas palabras, se ejecuta automáticamente valiéndose de un *software*. Se trata de hechos que tuvieron lugar cuando la mayoría de nosotros no podíamos imaginar ni remotamente algún tipo de dinero digital o un contrato literalmente 'inteligente'. Sin duda alguna, estamos frente a dos personajes pioneros y cuyos aportes perdurarán en la historia.

Ahora bien, puntualmente, los hechos y avances introducidos por Chaum y Szabo resultan de especial relevancia en la historia de la tecnología *blockchain*, en la medida que estos contienen las siguientes características de lo que hoy en día, entre otros aspectos, serían los cimentos de esta tecnología: (i) incorporación de una estructura descentralizada; (ii) preponderancia de la privacidad; (iii) uso esencial de la criptografía; y iv) transparencia y trazabilidad. Tal como se explicará más adelante, estas ideas son las que se recogen y predominan en la filosofía que se encuentra detrás del *blockchain*.

Ahora bien, habiendo abordado parte de los inicios de lo que hoy en día conocemos como *blockchain*, debemos también mencionar cuál es el panorama hoy en día, en el año 2021.

Con relación a la evolución de esta tecnología en el ámbito privado, debemos mencionar la creación de Hyperledger, el cual consiste en un proyecto de tecnología *blockchain* impulsado por la Linux Foundation en conjunto con grandes empresas de tecnología que buscan aplicar *blockchain* en sus sistemas operativos, y así mejorar la seguridad y la confianza de sus procesos. La Linux Foundation lanzó este proyecto en diciembre de 2015 y ya en febrero de 2016 contaba con el apoyo de varias empresas y organizaciones. El objetivo principal de Hyperledger es implementar y aprovechar la tecnología *blockchain* en diversos escenarios y promover que las empresas lo utilicen. Por ello, a la fecha, Hyperledger ha implementado importantes herramientas abiertas y libres que permiten a las

[6] Traducción libre:

> La idea básica de los contratos inteligentes es que muchos tipos de cláusulas contractuales (como gravámenes, fianzas, delimitación de derechos de propiedad, etc.) pueden integrarse en el hardware y software con los que tratamos, de tal manera que en caso se infrinja el contrato sea más caro (o si se desea, se encuentre prohibido) para el infractor.

empresas seguir el camino evolutivo de la referida tecnología, aprovechando sus ventajas y aplicándolas a sus diversos entornos de trabajo.

En esta línea, son varias las empresas que han decidido desarrollar plataformas que permitan a terceros implementar tecnología *blockchain* en sus procesos internos. Por ejemplo, IBM ha implementado la Blockchain Platform[7] , Microsoft ha creado su propia plataforma llamada Microsoft Azure[8] y Amazon ha creado el servicio Amazon Managed Blockchain[9].

Asimismo, de acuerdo con uno de los portales líderes de estadísticas en línea –Statista[10]– en el año 2020 alrededor del 36% de los altos ejecutivos entrevistados señalaron que las organizaciones que lideraban planeaban invertir más de cinco millones de dólares en tecnología *blockchain* para el año 2021 (2020). La investigación señaló, además, que los pronósticos indicarían que los ingresos de la tecnología global *blockchain* experimentarán un crecimiento masivo en los próximos años, y se espera que el mercado aumente a más de 40 mil millones de dólares para 2025.

Ahora bien, cabe preguntarnos cuál ha sido la reacción o avances brindados por los gobiernos para la apertura de un mercado basado en la tecnología *blockchain*. En tanto el uso de esta tecnología en el ámbito privado no requiere una regulación específica, el mejor indicador para medir esta apertura es a través de la legislación de las criptomonedas. En efecto, desde la perspectiva del Derecho, la primera y obvia incursión en este tema está relacionada directamente con el Bitcoin y demás criptomonedas (Herran Aguirre, 2019). Es decir, actualmente, a efectos de conocer su evolución en la legislación resulta útil usar como parámetro la regulación dada a las criptomonedas. Al respecto, la Tabla 1 grafica de manera puntual la situación en algunos de los países más desarrollados.

Tabla 1: Situación de los países más desarrollados entorno a la legislación sobre criptomonedas

País	Criptomonedas	Transacciones	Comentarios
Japón	Legales Se le da el tratamiento de un bien.	Legales Deben registrarse en la Agencia de Servicios Financieros.	Japón es considerado como uno de los países que cuenta con un clima bastante progresista en relación con las criptomonedas. Así, ha llegado a establecer al Bitcoin como moneda de curso legal y aprobó una ley a mediados de 2017 que reconoce las criptomonedas como propiedad legal.
Suiza	Legales Generalmente aceptadas como pago.	Legales Reguladas por la Swiss Finance + Technology Association (SFTA).	Suiza es considerado el país europeo con condiciones más favorables para el *blockchain* y las criptomonedas, así como el de mayor avance legislativo en la materia. En el cantón de Zug, uno de los más pequeños de Suiza y ubicado a pocos kilómetros de Zúrich y Lucerna, se encuentra Crypto Valley, un espacio al estilo del conocido Silicon Valley californiano destinado a empresas emergentes y desarrolladoras que operan e innovan en el mundo de las tecnologías *blockchain* y la criptografía (Crypto Valley, 2021). Zug se promociona como un ecosistema líder en tecnologías *blockchain* y criptográficas del mundo. En 2016, esta ciudad comenzó a aceptar Bitcoin como medio de pago de algunos servicios públicos.

[7] Esta plataforma se presenta de la siguiente manera**:**

> Los responsables de la toma de decisiones en los negocios están buscando cada vez más implementar las tecnologías blockchain para mejorar la eficiencia, reducir los costos y disminuir los riesgos. Blockchain crea sinergias entre múltiples organizaciones autorizadas, lo que le permite crear modelos comerciales de mayor valor y completamente nuevos. La actividad de desarrollo en el *software* y la interfaz de IBM Blockchain Platform le proporciona la flexibilidad, velocidad y potencia necesaria para cumplir sus objetivos con blockchain (IBM, s/f)**.**

[8] Esta plataforma se presenta de la siguiente manera**:** "Cree cadenas de suministro más inteligentes y eficientes, reduzca el fraude, compruebe las transacciones con más rapidez y cree nuevos modelos de negocio vanguardistas con Azure Blockchain Service" (Microsoft Azure, s/f).

[9] Esta plataforma se presenta de la siguiente manera: "Amazon Managed Blockchain es un servicio completamente administrado que facilita la creación y administración de redes de blockchain escalables mediante el uso de los marcos de código abierto populares Hyperledger Fabric y Ethereum" (Amazon, s/f).

[10] Véase a Statista (2020).

Estados Unidos	No es una moneda de curso legal. Sin embargo, algunos minoristas las aceptan como pago.	Legales Su regulación depende de cada estado.	Las criptomonedas son consideradas valores. La regulación de cada estado difiere ampliamente en relación con los requisitos de la tributación de las ganancias de las inversiones en criptomonedas.
Australia	Legales Se le da el tratamiento de un bien.	Legales Deben registrarse ante Australian Transaction Reports and Analysis Centre (AUSTRAC)	Australia es considerado como uno de los países que cuenta con un clima bastante progresista con relación a las criptomonedas. Asimismo, también es considerado como un país que viene realizando importantes avances en relación con la tecnología *blockchain*.

Fuente: Elaboración propia

Es claro que el análisis de la regulación de las criptomonedas en diversos países (Derecho comparado) sería materia de un artículo independiente; sin embargo, la finalidad de este cuadro es dotar de un contexto general con relación a cómo avanza su regulación en algunos de los países más desarrollados, con el fin de establecer un parámetro comparativo con la situación de América Latina que a continuación pasamos a referir.

Nuestra región tiene dos países que han mostrado un rechazo y prohibición expresa a las criptomonedas y las transacciones realizadas con las mismas. Nos referimos a Bolivia, que ha prohibido explícitamente las criptomonedas y las transacciones[11], y Ecuador, que también ha emitido una prohibición de circulación de todas las criptomonedas, excepto el *token* SDE emitido por el gobierno.

Por el contrario, en México, Argentina, Brasil, Venezuela y Chile las criptomonedas no se encuentran prohibidas y son aceptadas como pago en algunos puntos de venta. Sin embargo, casi no existe regulación en relación con las transacciones efectuadas con estas y su tratamiento. Así, a pesar del veloz crecimiento del uso de las criptomonedas, su regulación se encuentra en un nivel bastante incipiente. Por ejemplo, varios de los países de la región, incluyendo el nuestro, carecen de referencias expresas al tratamiento fiscal de las criptomonedas, no pudiendo conocerse los costos fiscales en los que se podría incurrir. Ello, como no puede ser de otro modo, genera un ambiente de incertidumbre y resistencia a las inversiones a través de este activo. Precisamente es lo que ocurre en el Perú, ante la ausencia de normas expresas y de pronunciamientos oficiales de la Administración, prevalece un ambiente de incertidumbre y de falta de previsibilidad con relación a su tratamiento.

Ante ello, y considerando el crecimiento del mercado de los criptoactivos –en especial de las criptomonedas–, resulta de suma importancia que los países de América Latina adopten directrices que regulen y guíen su uso, con el fin de promover mayores inversiones y crecimiento en este mercado.

III. *BLOCKCHAIN*: ¿QUÉ ES? ¿CÓMO FUNCIONA?

La traducción literal del término *blockchain* es 'cadenas de bloques' y, si bien existe más de una forma compleja de definir esta tecnología, consideramos que la definición más adecuada es únicamente señalar que el *blockchain* es un libro de registro, así de simple.

En esta línea, consideramos que la definición otorgada por Marc Andreessen cumple con ser clara y precisa al señalar que

> una cadena de bloques es **esencialmente solo un registro, un libro mayor de acontecimientos digitales que está "distribuido" o es compartido entre muchas partes diferentes. Solo puede ser actualizado a partir del consenso de la mayoría de participantes del sistema y, una vez introducida, la información nunca puede ser borrada** […] (citado en Revista Gerencia, 2017) [el énfasis es nuestro].

En pocas palabras, la tecnología *blockchain* es una forma de contabilidad distribuida que, debido al uso de la criptografía, resulta altamente segura y funciona sobre la base de crear diferentes registros que estarán vinculados con todos los demás anteriores, formando en conjunto una cadena de bloques (Wright & De Filippi, 2015). Por tanto, señalamos que un *blockchain* es tan solo un tipo de *ledger*[12] distribuido que almacena su información en bloques de datos que se agrupan secuencialmente. Así, cada bloque está 'encadenado' al anterior y registrado de forma inmutable a través de una red *peer-to-peer* utilizando mecanismos de seguridad criptográficos, y mantiene su estado a

[11] Bolivia prohibió el uso de Bitcoin y otras criptomonedas a mediados de 2014.

[12] Cuya definición en español es 'libro mayor'.

través del consenso de todos los participantes, sin requerir la intervención de una autoridad central.

Así, *blockchain* permite registrar todo tipo de información que la red de participantes decida preservar. Esto se implementa mediante un *ledger* cuyo registro de información se hace por medio de 'bloques', los cuales contienen la información ordenada en forma cronológica y sin aceptar modificaciones. Solo se añade información, la cual se une acumulativamente al bloque anterior. Precisamente este *ledger* corresponde a la 'cadena de bloques': sucesivos, consensuados y seguros que la comunidad construye para mantener el registro histórico de transacciones. Una vez generado un bloque, este se replica en todos y cada uno de los servidores conectados a la red (Zetzsche *et al.*, 2018).

Ahora bien, antes de desarrollar de forma general algunos conceptos técnicos incluidos en el funcionamiento de la tecnología *blockchain* y cuya comprensión permitirán mayor familiaridad con la misma, es importante tener presente las tecnologías y protocolos en los cuales, entre otros, se sostiene: (i) es una red *peer-to-peer* o P2P, (ii) utiliza la Criptografía asimétrica; y (iii) es una Red distribuida.

En relación con el funcionamiento, una parte elemental del *blockchain* son los propios bloques, los cuales son esenciales en la construcción de la cadena y permiten su funcionamiento. Cada bloque, claro está, posee en su conformación una secuencia de datos. Específicamente, entre otros, cada bloque tiene en su conformación lo siguiente:

a) **Datos de las transacciones del bloque.**

b) **El *hash* anterior**: Puntualmente, debemos recordar que el término *hash* se utiliza para identificar una función criptográfica cuyo objetivo es codificar datos para formar una cadena de caracteres única, es decir, genera identificadores únicos e irrepetibles a partir de una información dada.

c) **El *hash* del bloque**

d) **El *timestamp*:** Traducido como 'sello de tiempo' representa un dato almacenado de modo único que tiene como propósito mostrar el momento exacto en el que el bloque fue 'minado'[13], validado por la red *blockchain* y almacenado.

e) **El *nonce***: Lo que quiere decir *number that can be only used once.* Como su nombre lo indica, es un número único que identifica a cada bloque.

Con fines ilustrativos se pude imaginar cada bloque de la siguiente manera:

Figura 1: Bloques del *blockchain*

Fuente: Elaboración propia

Gracias a la estructura explicada, cada bloque tiene un lugar específico e inamovible dentro de la cadena, pues cada uno contiene información del *hash* del bloque anterior. Así, cada bloque tiene una información segura con sello de fecha y hora, así como un número de identificación. La cadena completa se guarda en cada nodo[14] de la red que conforma el *blockchain*, por lo que se almacena una copia exacta de la cadena en todos los participantes de la red.

Finalmente, tal como lo hemos señalado, la tecnología *blockchain* se fundamenta en el consenso entre las partes sin que medie un tercero. Así, el consenso se trata una parte imprescindible entre los usuarios del *blockchain*. Este consenso se sustenta en un protocolo común que verifica y confirma las transacciones realizadas, y asegura la irreversibilidad de estas. La forma de materializarse es a través de un algoritmo, que en el caso del Bitcoin es el protocolo *proof of work* (PoW).

La tecnología *blockchain* tiene mayores detalles técnicos de funcionamiento, así como diversas variables, sin embargo, para los fines del presente artículo los anteriormente tratados resultan suficientes para acercarse a su funcionamiento.

[13] En el sistema de *blockchain*, los "mineros" tienen el rol de la creación de nuevos bloques y la verificación de los bloques añadidos a la cadena.

[14] Desde el punto de vista de la tecnología *blockchain*, los nodos se constituyen por todos aquellos ordenadores que están interconectados a la red ejecutando el *software* que se encarga de todo su funcionamiento. Estos nodos están interconectados entre sí a través de una red de pares conocida como red *peer-to-peer* (P2P).

Finalmente, en virtud de lo señalado, es claro que la tecnología *blockchain* representa un registro fiable y transparente al permitir que múltiples partes participen en la transacción y verifiquen los datos que se anotarán en cada registro, no existiendo la posibilidad de que alguna de las partes pueda cambiar posteriormente las entradas del registro. De acuerdo con ello, en resumen, sus principales características son las siguientes:

a) **Descentralización:** No existe una autoridad central que la mantenga o controle el registro. A través de la tecnología *blockchain*, se prescinde de los intermediarios y las autoridades centrales. Cada nodo de la cadena tiene la misma copia del registro y lo mantiene actualizado de acuerdo con las reglas del protocolo de consenso.

   Es decir, es toda la red la encargada de mantener el registro actualizado y no una sola persona o autoridad.

b) **Transparencia**: Al tratarse de una base de datos distribuida que se replica entre todos sus participantes, permite que cualquiera pueda ver y validar su contenido.

c) **Seguridad**: La incorporación de altos estándares de criptografía, junto con el hecho de replicarse entre todos los participantes sin permitir modificaciones a la información contenida, hacen de la tecnología *blockchain* una red que incorpora características altamente seguras. Por ello, se considera una tecnología prácticamente inviolable, pues, para cambiar la información que contiene, un ciberataque tendría que afectar simultáneamente a (casi) todas las copias del registro (Swan, 2015).

d) **Flexibilidad**: Es posible implementar la tecnología *blockchain* sobre la base de redes tanto públicas como privadas y adaptarla a cualquier tipo de proceso.

IV. PUNTOS DE CONTACTO ENTRE EL *BLOCKCHAIN* Y LA PROPIEDAD INTELECTUAL

Preliminarmente, debemos mencionar que actualmente existen numerosas invenciones relacionadas con la tecnología *blockchain*. Al respecto, adjuntamos un cuadro que contiene algunas patentes basadas en la referida tecnología (ver Tabla 2). Las empresas solicitantes están lideradas por IBM, Microsoft Technology Licensing e Intel Corporation. Sin embargo, el registro de patentes que contienen esta tecnología no es una muestra de la tecnología aplicada al Derecho; por ello, únicamente las mencionamos con fines ilustrativos.

Tabla 2: Patentes basadas en tecnología *blockchain*

Número de publicación	Título
CN106228344A	*A block chaining technique based on electronic government system construction method*
CN107566379	*A government affair information resource sharing system based on block chain*
WO2018020369	*Blockchain-implemented method and system*
US20150332283	*Healthcare transaction validation via blockchain proof-of-work, systems and methods*
CN107430755	*Cryptographic verification of provenance in a supply chain*
WO2017104899	*Blockchain-based certificate authentication system and authentication method using same*
WO2017213719	*Systems and methods for providing identity scores*

Fuente: Elaboración propia[15]

A partir de lo señalado en los párrafos anteriores, es claro que la tecnología *blockchain* resulta de utilidad en los sistemas basados en registros. En este sentido, la tecnología *blockchain* ofrece importantes condiciones para la gestión de registros y provee de funcionalidades a la interacción, lo que genera confianza, integridad y seguridad en los servicios. En virtud de lo expuesto, cualquier abogado de Propiedad Intelectual (en adelante, PI) llegará a la conclusión de que el *blockchain* es el medio perfecto para probar la existencia de los activos intangibles de forma fehaciente y clara, así como para protegerlos. Es por ello que ya existen numerosas empresas que vienen utilizando esta tecnología para asegurar derechos de PI. Ello se demuestra, por ejemplo, en las plataformas desarrolladas por Bernstein, Pons IP, Cysae y Cedro para acreditar la titularidad de documentos y asegurar la protección de secretos empresariales, certificar licencias de derechos de autor y, en general, la gestión de activos intangibles.

[15] Es posible acceder a la información en relación a las siguientes patentes realizando la búsqueda por número de publicación en el portal Espacenet Patent Search a través del siguiente enlace: https://worldwide.espacenet.com/?locale=en_EP.

Asimismo, a través de la tecnología *track & trace*, es posible combatir la falsificación marcaria. Por ejemplo, en el 2019, LVMH Moët Hennessy Louis Vuitton, más conocido como LVMH, en asociación con Microsoft y ConsenSys, anunció el lanzamiento de la plataforma AURA que constituye un sistema de rastreo y seguimiento de cada producto[16] y se espera que sea una herramienta para toda la industria de artículos de lujo. La referida plataforma está basada en Ethereum *blockchain* y utiliza Microsoft Azure. A través de AURA se vuelve factible que los consumidores accedan a todo el historial de los productos y, con ello, a la prueba de autenticidad de los mismos. Las marcas Louis Vuitton y Christian Dior ya están involucradas en la plataforma.

En esta línea, la característica de la trazabilidad que incorpora la tecnología *blockchain* se viene utilizando para seguir la evolución de productos comprendidos en una determinada cadena de suministro. Ello, tal como sucede en el caso de LVMH, resulta altamente interesante para industrias que dependen intensamente de los derechos de PI, como, por ejemplo, las industrias farmacéuticas. Así, la empresa farmacéutica Merck ha desarrollado un sistema que utiliza *blockchain* e inteligencia artificial (en adelante, IA). En términos sencillos, a través de la IA se identifican características únicas del producto (llamémoslas 'huella digital') y estas se vinculan a una firma digital. La firma digital se almacena de forma segura a través de la tecnología *blockchain* y ello permite una fácil detección de cualquier intento de modificar la firma digital, proporcionando un seguimiento integrado y seguro de la cadena de suministro completa.

Otro ejemplo que resulta interesante mencionar es lo implementado por la empresa Volvo. En el año 2019, Volvo Cars y Circulor, una compañía tecnológica dedicada a la investigación y el desarrollo de *blockchain*, anunciaron que se utilizará la tecnología *blockchain* para conseguir trazabilidad en la cadena de suministros en cuanto a la producción de las baterías utilizadas para el Volvo XC 40 Recharge P8, el primer vehículo completamente eléctrico de la compañía.

Ahora bien, en relación con la aplicación del *blockchain* en la PI fuera del ámbito privado, la principal novedad recae en el anuncio de la European Union Intellectual Property Office (en adelante, EUIPO) que desarrollará hasta el 2025[17] dos proyectos basados en la tecnología *blockchain*: IP Blockchain Register y el Blockathon.

En lo que respecta al IP Blockchain Register, la EUIPO busca (i) actualizar el *layout* de la base de datos TMview, y (ii) crear una red de *blockchain* que albergue todos los registros de marcas y diseños industriales (European Union Intellectual Property Office [EUIPO], 2020b). El objetivo es que para el año el 2025 se encuentren dentro de este registro la gran mayoría de las oficinas europeas y algunas oficinas internacionales de PI.

Si bien no se tiene mucha más información al respecto, consideramos que se trata de un proyecto positivo, en tanto dotaría de mayor eficiencia y transparencia a los registros de PI. Además, permitirá que en cualquier jurisdicción se cuente con datos verídicos, verificables, públicos e inmutables.

Con relación al segundo proyecto mencionado por la EUIPO, este tuvo origen en el Blockathon Forum celebrado en el año 2018, y consiste en la construcción de un sistema de autenticación descentralizado y escalable para combatir las falsificaciones, un sistema similar a la tecnología *track & trace* antes mencionada. Además, es importante mencionar que el Blockathon Forum fue promocionado como: "Anti-Counterfeiting Blockathon Forum, a network of people and organisations working together to shape and deliver the future anti-counterfeiting infrastructure" (EUIPO, 2018).

En virtud del panorama mencionado, se ha señalado acertadamente que

> el uso de la tecnología de la cadena de bloques para la gestión de los derechos de PI ofrece grandes posibilidades. La inscripción de los derechos de PI en un registro distribuido y no en una base de datos tradicional podría transformarlos en derechos de PI inteligentes (Clark, 2018, p. 32).

Sin embargo, esta misma organización señala que "para que se produzca el despegue de la tecnología de la cadena de bloques en la gestión de los derechos de PI sería necesario disponer de un conjunto de normas acordadas y que contaran con apoyo internacional" (Rose, 2020).

Teniendo en cuanta lo expuesto, es posible concluir que la tecnología *blockchain* proporciona he-

[16] Ken Timsit, Director general de ConsenSys Solutions, señaló: "AURA es innovadora para la industria del lujo. ConsenSys se enorgullece de contribuir y trabajar con LVMH en una iniciativa que servirá a toda la industria del lujo, protegiendo los intereses, la integridad y la privacidad de cada marca" (citado en Simms, 2019).

[17] Véase European Union Intellectual Property Office (2020a; 2020b).

rramientas propicias para la tutela de los derechos de PI, de hecho, es una de las ramas del Derecho que mayor provecho le puede sacar a su implementación. Puntualmente, los beneficios que traería el uso de la tecnología *blockchain* en la gestión de derechos de PI, pueden agruparse de la siguiente forma:

A. Adopción de los *smart contracts*

En términos sencillos, los *smart contracts* son acuerdos, escritos en código de programación, que ejecutan automáticamente funciones programadas cuando se cumplen ciertas condiciones preestablecidas. En otras palabras, cuando la condición A se cumple, genera que la acción B se realice (Revoredo, 2018). Asimismo, se debe precisar que el contenido de los *smart contracts* consiste en *scripts* (códigos informáticos) que son plasmados en lenguajes de programación y es posible que las condiciones se ejecuten automáticamente de acuerdo con lo programado, en la medida que el *smart contract* está almacenado en un *blockchain* (Sklaroff, 2017).

De este modo, es claro que su principal atractivo es que son ágiles y sencillos, pero debe de tenerse en cuenta que la información incorporada es inmutable y, en función a cómo sean programados en algunas circunstancias, no pueden ser revocados, por lo que es imprescindible conocer bien el contenido del código que ejecuta el contrato (Granieri, 2017).

En virtud de lo expuesto, es claro que los *smart contracts* serían de gran utilidad para hacer cumplir acuerdos en materia de PI. Se debe buscar que la información de PI esté contenida en un formato digital para que así se haga posible incorporarla a un *smart contract* y así las prestaciones pactadas que involucran el derecho de PI se cumplan automáticamente. Su utilidad podría aplicarse, por ejemplo, para el pago de regalías por la explotación de obras protegidas por derechos de autor o el uso de signos distintivos, ya que a través de un *smart contract* dicho pago podría ejecutarse de forma inmediata.

Se debe tener presente que, en los derechos de PI, al tratarse de derechos intangibles, muchas veces se torna difícil su vigilancia y a menudo los titulares de los mismos no reciben la remuneración correspondiente por su explotación. Gestionando estos derechos a través de la tecnología *blockchain* –por medio de los *smart contracts*–, se podrá garantizar que cada vez que se explote alguno, se transfiera automáticamente la cantidad correspondiente (pactada) a su titular. Así, al pactar en el contrato una retribución por cada reproducción de una obra musical o una regalía por cada producto vendido con la marca otorgada en licencia, se podría dar una transferencia de pagos en tiempo real al cual los derechos son explotados, lo cual, como no puede ser de otro modo, garantiza una gestión efectiva y equitativa a favor de los titulares de los derechos de PI.

B. Prueba de paternidad del derecho de autor

A través de la tecnología *blockchain* es posible llevar a cabo una gestión más eficiente de los derechos de autor, siendo esta fiable, transparente y automatizada. En la mayoría de legislaciones, por lo pronto en todos los países que han ratificado el Convenio de Berna, el derecho de autor es declarativo de derechos. Es decir, no será necesaria su inscripción para que el titular ostente derechos sobre su obra. Ello ocurre en el Perú, en donde se aplica el Decreto Legislativo 822, Ley sobre el Derecho de Autor, y la Decisión 351 de la Comunidad Andina, Régimen común sobre Derecho de Autor y Derechos Conexos. Sin embargo, muchas veces se opta por el registro en la medida que este otorga una fecha cierta. Precisamente, en un caso de infracción al derecho de paternidad (comúnmente conocido como plagio) corresponderá que el autor no solo pruebe su autoría, sino la fecha de la creación de la obra, es decir, su paternidad sobre la obra.

Al administrar una obra a través de la tecnología *blockchain*, el autor obtendrá al menos los siguientes beneficios que resultan sumamente relevantes para obtener una tutela efectiva de sus derechos: (i) tendrá una fecha cierta de la creación; y (ii) quedará acreditada su autoría. Se debe tener presente que el *timestamp,* así como la información de la transacción (en este caso la obra), entre otros, forman parte del bloque de una cadena *blockchain* y los mismos son inalterables.

C. Protección de secretos empresariales

Los secretos empresariales se consideran como uno de los activos intangibles con mayor valor que poseen las empresas.

Un secreto empresarial (también conocido como secreto industrial) es toda información o conocimiento reservado o confidencial (no divulgado) que posee valor comercial para una empresa (persona o institución). El valor comercial implica que dicha información pueda ser susceptible de uso y aprovechamiento, o para obtener ventaja competitiva, en el contexto de alguna actividad productiva, industrial o comercial (Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [Indecopi], 2020).

El secreto empresarial está considerado como un elemento de la PI; sin embargo, a diferencia de las patentes o marcas, no se trata de un derecho de exclusividad que deba ser concedido por alguna institución gubernamental para que tenga validez, sino más bien funciona como un 'monopolio de facto' que perdurará por el tiempo en que la información confidencial o el secreto se mantenga a salvo (Indecopi, 2020).

Gracias a la tecnología *blockchain*, las empresas pueden resguardar de una forma rápida, simple y confiable todos sus secretos empresariales. Se debe tener en cuenta que, gracias a las características de esta tecnología, una vez subido el secreto al sistema, este no podrá ser alterado ni eliminado y tendrá una fecha cierta. Ello, generará una evidencia probatoria incuestionable en relación con los siguientes factores: (i) el contenido de la información objeto de protección del secreto empresarial; y (ii) la fecha en la que se creó. De acuerdo a ello, en caso un tercero se apropiara de forma indebida del secreto empresarial de alguna compañía, la compañía afectada tendrá pruebas fehacientes para demostrar esta apropiación ilícita.

D. Trazabilidad para evitar la falsificación

Tal como han venido haciendo importantes compañías, a través de la tecnología *blockchain* es posible realizar un rastreo completo de los productos comercializados, este rastreo comprende desde el inicio de la producción hasta la comercialización final. Es decir, es posible contemplar una trazabilidad integral del proceso.

A partir de ello, al gestionar la trazabilidad de un producto a través de la tecnología *blockchain*, se permite identificar el 'ciclo de vida' de cada producto. Se debe tener presente que una de las funciones que aporta esta tecnología consiste en otorgar un identificador único que no puede ser alterado (el *hash*). En ese sentido, se podrá identificar individualmente cada producto. Además, al ingresar este producto a la cadena de bloques no es posible alterarlo ni reemplazarlo, es decir, se convierte en un activo inamovible e irrepetible.

De esta manera, aplicando la tecnología *blockchain*, los consumidores y los propios titulares de los productos podrán identificar y evitar las falsificaciones. Se debe tener presente que cada producto contendrá un identificador único (*hash*) que acreditará la originalidad del mismo.

V. CONCLUSIONES

En el Perú, no se ha establecido aún una política pública para la promoción y adopción de tecnologías *blockchain*. Esto implica la ausencia de reglas claras y controles básicos sobre la utilización de este tipo de instrumentos en actividades comerciales, así como la validez probatoria de los mismos. Esta falta de regulación genera incertidumbre y, con ello, ausencia de inversiones.

Si bien es cierto que es muy probable que esta tecnología aún no se adapte al sector público, ello no ocurre con relación al ámbito privado y la experiencia internacional así lo ha demostrado. Estamos frente a una tecnología que es utilizada cada vez más para regular relaciones entre privados y como medio de prueba para acreditar la existencia y el contenido de dichas relaciones. Por ello, antes de que esta tecnología saque mayor ventaja y se genere un vacío jurídico dentro del cual puede ser utilizada para actividades ilícitas, es necesario concebir un marco regulatorio apropiado.

Se debe tener presente que una de las principales ventajas de la tecnología *blockchain*, como lo hemos señalado, es proporcionar un sistema descentralizado, que no requerirá una autoridad central. En el ejemplo de las criptomonedas ello es muy claro, pues se trata de un sistema monetario sin un banco central. Sin embargo, esta tecnología se puede extender a muchísimos otros ámbitos, como, por ejemplo, una certificación de un documento sin notario, un registro fehaciente sin una autoridad registral, entre otros. La sola idea trae concepciones positivas, ya que eventualmente los sistemas de registros administrados por el Gobierno podrían ser manejados también por los privados. Sin embargo, es claro que la eventual adopción de esta tecnología también requiere un cambio social importante en el cual se asuma la responsabilidad de forma correcta.

Tal como lo señalamos al principio, no cabe duda que la eventual inclusión y regulación de la tecnología *blockchain* en nuestro ordenamiento jurídico traerá desafíos importantes y debemos de empezar a enfrentarlos con el fin de no desaprovechar las oportunidades que brinda su proceso evolutivo y poder anticiparlo adecuadamente.

REFERENCIAS

Amazon (s/f). Amazon Managed Blockchain. https://aws.amazon.com/es/managed-blockchain/

Blind signature. (12 de junio de 2017). En Wikipedia (wikipedia con cursiva). ttps://en.wikipedia.org/wiki/Blind_signature

Chaum, D. (1982). Blind Signatures for Untracealbe Payments. En D. Chaum, R.L. Rivest, & A.T. Sherman (eds.), *Advances in Cryptology* (pp. 199-203). Springer, Boston, MA.

Clark, B. (2018). La tecnología de la cadena de bloques y el Derecho de Propiedad Intelectual: ¿una pareja perfecta en el criptoespacio?. *OMPI Revista*, (1), 30-34.

Crypto Valley (2021). Crypto Valley. https://cryptovalley.swiss/

Endemann, B., Wladawsky-Berger, I., LaPointe, C., & Yen, H. (2020). *Blockchain: Technology Factsheet Series*. Harvard Kennedy School, Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/files/publication/Blockchain.pdf

European Union Intellectual Property Office [EUIPO] (2018). *Blockathon Forum 2018*. https://euipo.europa.eu/ohimportal/es/web/observatory/blockathon

(2020a). *Strategic Plan 2025.* https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/contentPdfs/about_euipo/strategic_plan/strategic-plan-2025_draft.pdf

(2020b, 28 de octubre). Interview to Miguel Ortega, Head of New Technologies at the EUIPO [video]. Youtube. https://www.youtube.com/watch?v=XqTbopE9SME

Granieri, M. (2017). Technological Contracts. En P. Montaneri (ed.), *Comparative Contract Law* (pp. 408-450). Elgar Publishing.

Herran Aguirre, A. F. (2019). El blockchain como tecnología de confianza. En J. Chipana Catalán (coord.), *Derecho y nuevas tecnologías: El impacto de una nueva era* (pp. 232-243). Editorial Jurídica THĒMIS.

Iansiti, M., & Lakhani, K. (2020). The truth about Blockchain. *Harvard Business Review*, (95), 118-127.

IBM (s/f). IMB Blockchain Platform. https://www.ibm.com/pe-es/blockchain/platform

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [Indecopi] (2020). *Guía práctica para la protección mediante secretos empresariales.* https://www.rutapi.pe/documents/6882212/6884127/7%29+Gu%C3%ADa+practica+para+la+protecci%C3%B3n+mediante+secretos+empresariales.pdf/e93097e4-7324-2ca0-d681-6a4410e077f8

Microsoft Azure (s/f). Cadena de Bloques. https://azure.microsoft.com/es-es/solutions/blockchain/

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf

Núñez Miller, J. (2017). Criptografía y consenso aplicado a la blockchain. En A. Preukschat (coord.), *Blockchain: Revolución Industrial de internet* (pp. 203-220). Gestión 2000.

Preukschat, A. (2017). *Blockchain: La revolución industrial de internet*. Gestión 2000.

Revista Gerencia (agosto 2017). Blockchain: La revolución tras Internet. *Revista Gerencia - Noticias, análisis e información*. http://www.emb.cl/gerencia/articulo.mvc?xid=4287&edi=182&xit=blockchain-la-revolucion-tras-internet

Revoredo, A. (8 de marzo de 2018). Blockchain y Smart Contracts ¿Hay futuro para los abogados? *Gestión.* https://gestion.pe/blog/cyberlaw/2018/03/blockchain-y-smart-contracts-hay-futuro-para-los-abogados.html

Rose A. (julio de 2020). *Las cadenas de bloques como transformadoras del registro de derechos de PI y fortalecedoras de la protección de derechos de PI no registrados.* OMPI Revista. https://www.wipo.int/wipo_magazine_digital/es/2020/article_0002.html

Simms, T. (16 de mayo de 2019). Louis Vuitton y Christian Dior revelan una plataforma blockchain para verificar los productos de lujo. *Cointelegraph.* https://es.cointelegraph.com/news/louis-vuitton-and-christian-dior-owner-unveils-blockchain-platform-to-verify-luxury-goods

Sklaroff, J. (2017). Smart Contracts and the cost of Inflexibility. *University of Pennsylvania Law Review*, *166,* 263-303.

Statista (junio de 2020). Investments plans for blockchain technology in organizations over the next 12 months worldwide as of 2020. https://www.statista.com/statistics/878612/worldwide-investment-plan-blockchain-technology/

Swan, M. (2015). *Blockchain: Blueprint for a New Economy.* O' Reilly.

Szabo, N. (1996). *Smart Contracts: Building for Digital Markets.* http://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf

Tian, C. (27 de julio de 2017). The Rate of Blockchain Patent Applications Has Nearly Doubled in 2017. *Coindesk.* https://www.coindesk.com/rate-blockchain-patent-applications-nearly-doubled-2017

Vigna, P., & Casey, M. (2016). *The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order.* St. Martin's Press.

Wright, A., & De Filippi, P. (2015). *Descrentralized blockchain technology and the rise of cryptographia.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664.

Zetzsche, D., Buckey, R., Douglas, A., & Föhr, L. (2018). The ICO Gold Rush: It's a Scam, It's bubble, it's super challenge for Regulators, *Harvard International Law Journal*, *60*(2), 267-315. https://dx.doi.org/10.2139/ssrn.3072298

10.18800/themis.202101.020

PLATAFORMAS DIGITALES Y RIESGOS DE CONGLOMERADO: DESAFÍOS PARA LAS AUTORIDADES DE COMPETENCIA EN IBEROAMÉRICA EN EL ANÁLISIS DE OPERACIONES DE CONCENTRACIÓN

DIGITAL PLATFORMS AND CONGLOMERATE RISKS: CHALLENGES FOR COMPETITION AUTHORITIES IN IBERO-AMERICA IN THE ANALYSIS OF CONCENTRATION OPERATIONS

Andrea Von Chrismar Medina*
Prieto Abogados

Benjamín Grebe Lira**
Prieto Abogados

This article explores the subject of merger operations, specifically, on digital platforms. Thus, it analyzes the possible risks of these and the challenges that antitrust agencies must face when analyzing them. In this way, the authors highlight various characteristics of this market such as its dynamism and unpredictability, which allows it to adapt to the increase in demand, and the important role of user data in merger operations.

To fulfill this objective, the article begins with a theoretical approach, providing definitions of key concepts for the understanding of merger operations on digital platforms. Nevertheless, it also offers a practical analysis, by exploring how these types of mergers have been taking place in reality, through recent cases of judgements relevance.

Keywords: Digital platforms; merger control; competition agencies; user data.

El presente artículo explora el tema de las operaciones de concentración, específicamente, en plataformas digitales. Así, analiza los posibles riesgos de estas y los retos que deben afrontar las agencias de competencia al analizarlas. De esta manera, los autores destacan variadas características de este mercado como su dinamismo e impredictibilidad –las cuales permiten que el mismo se adapte al aumento de demanda– y el importante papel de los datos de los usuarios en las concentraciones.

Para cumplir con su objetivo, el artículo empieza con un recorrido teórico mediante la definición de conceptos clave para el entendimiento de las operaciones de concentración en plataformas digitales. No obstante, también se hace un análisis práctico al exponer cómo se han venido dando este tipo de concentraciones en la realidad, a través de casos recientes de gran relevancia.

Palabras clave: Plataformas digitales; control de concentraciones; agencias de competencia; datos del usuario.

* Abogada. Magíster en Derecho de los Negocios por la Universidad Adolfo Ibáñez (Santiago de Chiles, Chile) y Master of Science in Regulation London School of Economics and Political Science, University of London (Londres, Reino Unido). Directora en Prieto Abogados (Santiago de Chile, Chile). Contacto: avonchrismar@prieto.cl

** Abogado. LL.M. en International Economic Law en Warwick University (Coventry, Reino Unido). Socio de Prieto Abogados (Santiago de Chile, Chile). Contacto: bgrebe@prieto.cl.

Nota del editor: El presente artículo fue recibido por el Consejo Ejecutivo de THEMIS-Revista de Derecho el 24 de enero de 2021, y fue aceptado por el mismo el 15 de abril de 2021.

I. INTRODUCCIÓN

El año 2004, el Tribunal de Defensa de la Libre Competencia de Chile (en adelante, TDLC) aprobó la fusión de dos de las principales compañías de telecomunicaciones y televisión pagada presentes en el país en ese entonces. Ello fue su primera resolución respecto a una operación de concentración. Con una visión que hoy en día parece obvia, pero que en esa época era algo más difícil de aventurar, el voto de mayoría del TDLC señaló que tenía el 'convencimiento' de que, en el mediano plazo, el "dinamismo tecnológico esperable de esta industria" podría "restringir o eliminar en el futuro las barreras a la entrada y hacer muy inestable las fronteras del mercado" (Resolución 01/2004, 2004, p. 45). Resulta interesante esta visión futurista pero tan clara acerca del aumento de la sustituibilidad en el tiempo y los cambios en la definición de los mercados (que demostró ser muy real), frente a todo lo que está ocurriendo hoy, casi veinte años después, con las nuevas plataformas digitales (y todas las que imaginamos y no imaginamos que vendrán) y el análisis que de ellas se hace bajo el prisma de la libre competencia.

Lo que comúnmente se denomina como plataforma digital engloba múltiples tipos de compañías tecnológicas, aplicaciones y sitios disponibles a través del acceso a datos de internet. Si bien un concepto delimitado o una categorización exhaustiva muy probablemente requeriría una actualización constante, atendiendo al rápido desarrollo de la tecnología y de los negocios digitales, es posible para cualquiera de nosotros identificar algunos tipos de plataformas con las que interactuamos a diario.

Algunas plataformas digitales operan como vitrina para la oferta de bienes y servicios (conocidas como Marketplace, Amazon y Mercado Libre); en otras, los usuarios pueden compartir contenido de texto y multimedia (por ejemplo, Twitter, Facebook, Instagram y Pinterest). También, existen aplicaciones de reproducción de contenido musical, multimedia en general o vía *streaming* (como es el caso de Netflix, Amazon Prime, DisneyPlus, Spotify y Youtube); aplicaciones de mensajería y redes con un número determinado de usuarios (como es el caso de Whatsapp, TikTok y Snapchat); aplicaciones de economía colaborativa, en los que los servicios con bienes intercambiados entre pares (como es el caso, por ejemplo, de tomar un viaje en automóvil por medio de Uber o de alojar en la casa de alguien por medio de Airbnb). Por otra parte, existen aplicaciones de reparto de comida y/o compras en tiendas y supermercados (UberEats, PedidosYa, Rappi, Grubhub, entre muchas otras) y aplicaciones con información acerca del estado del tráfico vehicular (Waze y Google Maps), entre muchas otras.

Con la llegada de la pandemia del COVID-19, los servicios y mercados digitales han acelerado la presencia y uso de estas plataformas en la vida cotidiana de las personas. En ese contexto, las distintas aplicaciones y sitios de internet que conocemos como plataformas digitales han pasado a tener un rol cada vez más relevante en la provisión de bienes y servicios. Todo ello explicado por la intensificación exponencial en su uso durante el último tiempo, asociado a las medidas de confinamiento adoptadas por las autoridades en gran parte del mundo.

Sin embargo, con anterioridad a la pandemia del COVID-19, las autoridades a cargo de velar por la protección y promoción de la libre competencia en diversas jurisdicciones a nivel global han analizado distintas operaciones de concentración (fusiones, adquisiciones y *joint ventures* permanentes) en las que alguna de las partes, o todas ellas, operan por medio de plataformas digitales o empresas incipientes de tecnología (conocidas estas últimas como *startups* tecnológicos).

En términos generales, durante el análisis de los eventuales efectos en la competencia de un mercado que puede tener una operación de concentración, es posible distinguir efectos adversos para la competencia de –al menos– tres tipos: (i) efectos unilaterales, cuando la entidad resultante de la operación de concentración puede ejercer poder de mercado en forma unilateral, ya sea sobre los clientes o consumidores o para excluir competidores; (ii) efectos coordinados, cuando la operación facilita o puede hacer más efectivo el comportamiento coordinado de la entidad resultante de la operación con sus competidores (Fiscalía Nacional Económica [FNE], 2012); y (iii) efectos de conglomerado, cuando la operación, que involucra a entidades que operan en distintos mercados, puede facilitar a la entidad resultante de ella la capacidad de restringir el acceso al mercado de los competidores por medio de la vinculación de compras o empaquetamiento en productos o servicios complementarios (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2017).

El análisis de estos tipos de efectos unilaterales, coordinados y de conglomerado también es realizado por las autoridades de competencia respecto de aquellas operaciones de concentración en las que participa alguna plataforma tecnológica o *startup*.

Debido a determinadas características presentes en algunos mercados digitales, como es su dina-

mismo, las externalidades de red o el hecho de tratarse en algunos casos de mercados de dos lados (es decir, que intermedia a dos grupos de usuarios distintos; por ejemplo, en el caso de los Marketplace, que conecta vendedores y compradores), el análisis de estas –desde el punto de vista de la libre competencia– puede representar desafíos para las autoridades expertas en la materia.

El presente artículo desarrolla, en primer lugar, una revisión de la literatura reciente sobre los desafíos que enfrentan las autoridades de competencia al analizar mercados en los que operan las plataformas digitales, especialmente, respecto del planteamiento y desarrollo de argumentos referidos a los riesgos de conglomerado en el análisis de competencia de operaciones de concentración entre plataformas. En segundo lugar, por medio de la síntesis de seis casos seleccionados referidos a plataformas digitales, se analiza de qué manera cuatro distintas autoridades de competencia a nivel iberoamericano (específicamente en Chile, México, Brasil y España) han abordado los desafíos de incerteza y los riesgos de conglomerado asociado al uso de datos en sus decisiones más recientes. Finalmente, en tercer lugar, se presentan las conclusiones.

II. ANÁLISIS DE COMPETENCIA EN OPERACIONES DE CONCENTRACIÓN QUE INVOLUCRAN PLATAFORMAS DIGITALES

En general, las plataformas digitales representan un desafío desde el punto de vista del análisis de competencia. Todo esto es producto de los efectos de red, la importancia de los datos de los usuarios, los riesgos de conglomerado derivados de los datos, los altos componentes de innovación y dinamismos de los mercados digitales, que se traduce en muchas ocasiones en una falta de certeza y asimetrías de información en desmedro de las agencias de competencia a cargo de su análisis y fiscalización; la probabilidad de operaciones que busquen solo anticiparse y evitar la competencia; y las eventuales conductas de empaquetamiento. A continuación, se desarrolla cada uno de estos desafíos.

A. Efectos de red

El uso de las plataformas puede generar efectos de red, es decir, que el uso de la plataforma por parte de un número determinado de usuarios influye –de manera positiva o negativa– en la utilidad que tenga la plataforma para un determinado usuario (Arroyo Barrigüete, 2007). Esto puede llevar a que los potenciales entrantes o competidores no logren disciplinar la conducta de una firma relevante en el mercado.

Un ejemplo claro del efecto de red que se genera en las plataformas digitales es el atractivo mayor que presenta, por ejemplo, una red social, en la medida que tenga más usuarios. En esos casos, estaremos frente a una externalidad de red positiva, porque el uso de la plataforma aumentará en la medida que crezca el uso de los otros usuarios.

En efecto, es común realizar la distinción entre efectos de red directos e indirectos en las plataformas digitales. Los efectos directos de red consisten en aquellos dados por un valor del producto o servicio de cara al consumidor o usuario en la medida que aumente el número de usuarios de la plataforma, como por ejemplo ocurre con las aplicaciones de tráfico vehicular. Por su parte, los efectos indirectos de red son aquellos referidos al valor del producto o servicio derivado del aumento en el número de productos o servicios complementarios que ofrezca la plataforma, lo que a su vez incide en el número de usuarios de la plataforma. Estos últimos, son los efectos de red que se analizan, por regla general, como riesgos de conglomerado en el análisis de operaciones de concentración en mercados digitales referidos a los incentivos de una firma digital para entrar a nuevos mercados (Bourreau & de Streel, 2019).

B. Datos de usuarios

Otro desafío que enfrentan las autoridades de competencia es lograr realizar un análisis de los efectos de red ya señalados teniendo en consideración la relevancia de los datos de los usuarios de las distintas plataformas digitales como activo valioso con una mirada prospectiva, sobre todo tratándose de mercados altamente dinámicos como es el caso de las plataformas digitales.

Diversas agencias de competencia y académicos han argumentado que la acumulación de datos de usuarios de una plataforma digital en un determinado actor puede ser una circunstancia que podría alterar los niveles de competencia del mercado.

Así, se ha observado una creciente preocupación respecto de las ventajas competitivas que puede otorgar el *big data* a las empresas tecnológicas, dotándolos de poder de mercado (Nayak, 2019). En estos casos, las autoridades de competencia deben evaluar las implicancias competitivas de los datos, si es que logran identificar que un determinado actor cuenta con alguna ventaja. Un ejemplo de esas ventajas sería una base de datos de usuarios que sea difícil o costosa de replicar, o que se requiera mucho tiempo para ello por parte de un competidor o entrante al mercado (McSweeny & O'Dea, 2018).

Si bien en ciertos casos una categoría particular de datos puede representar un mercado relevante en sí mismo (Caso *Dun & Bradstreet Corp.*, 2010), los riesgos identificados con mayor frecuencia por las autoridades de competencia al analizar estos mercados han sido los riesgos respecto de apalancamiento del poder de mercado. Este riesgo se materializa cuando una plataforma es capaz de trasladar el poder de mercado que tiene en una actividad en la cual ya cuenta con datos, hacia otra actividad o mercado producto de su entrada a través de la operación de concentración que se somete al análisis de la agencia de competencia.

En este sentido, se ha observado que una plataforma digital con poder de mercado puede generar una mayor preocupación desde el punto de vista de, por un lado, la protección de datos personales de los usuarios y de su privacidad; y, por otro, la protección de la competencia en el mercado, producto de los riesgos de conglomerado. Esto surge, precisamente, porque las ventajas o efectos de red antes señalados también pueden hacerse extensivas al acceso de datos que las plataformas tienen con relación a los usuarios y sus preferencias de consumo, de manera desagregada y prácticamente en tiempo real, generando incentivos para que la plataforma se incorpore a nuevos mercados.

Conforme a lo anterior, las plataformas digitales acceden a una gran cantidad de datos sobre el mercado y sus usuarios, los que alimentan diversos algoritmos que mejoran constantemente la eficiencia de la plataforma. Estos datos no están disponibles para los competidores de esa plataforma ni para las autoridades que regulan esa actividad (Petropoulos, 2017).

Si bien en algunas jurisdicciones la protección de los derechos de los consumidores, los datos personales y la competencia están radicadas en una misma agencia o institución[1], lo cierto es que, desde el punto de vista de la libre competencia, lo relevante para el análisis será determinar si el acceso a los datos puede o no implicar una ventaja competitiva para la plataforma en un determinado mercado. Al respecto, algunos autores han señalado que las plataformas incumbentes en un determinado mercado tienen una ventaja competitiva por el acceso a los datos de los usuarios, lo que sería muy difícil de igualar por parte de una plataforma rival, aun cuando pueda esta última tener un producto o servicio de mejores características (De Elejalde, 2020).

El análisis por parte de autoridades de competencia acerca de la intersección entre aspectos referidos a los datos de los usuarios de las plataformas y los efectos en la competencia derivados de operaciones de concentración en mercados digitales no es algo nuevo. En efecto, se ha planteado al respecto, por ejemplo, que una estrategia de apalancamiento de poder de mercado por medio de la integración vertical de plataformas en distintos mercados o actividades podría generar efectos excluyentes en el largo plazo.

Así, este tipo de estrategias serían problemáticas, desde el punto de vista de la competencia, al aumentar el poder de mercado producto de operaciones de concentración con firmas altamente innovadoras, cuando estas no tienen otro objetivo que el uso de datos de usuarios de gran escala como ventaja competitiva de conglomerado respecto de los competidores actuales o potenciales (Chirita, 2019a).

Esto ha sido reconocido por la doctrina como un dilema regulatorio que enfrentan, principalmente, las autoridades con competencia en materias de política de protección del consumidor y antimonopolios (Botta & Wiedemann, 2019). Ello se debe, principalmente, a que las legislaciones de protección del consumidor, por lo general, establecen reglas más limitadas y sanciones que, en términos de desincentivo de las conductas infractoras, serían menos efectivas que las aplicables en materia de antimonopolios.

Así, de acuerdo a Botta y Wiedemann (2019), si bien las agencias con competencia en ambas áreas tendrían incentivos para adoptar el camino fácil de aplicar la protección de los consumidores en ciertos casos para evitar procesos complejos de análisis de definiciones de mercado relevante y poder de mercado, este no sería el camino más efectivo. Esto porque, a juicio de estos autores, la legislación en materia de competencia debiese ser más atractiva de implementar, en la medida que ella contemple sanciones más severas y la posibilidad de adoptar compromisos de conducta, otorgando flexibilidad y dinamismo (Botta & Wiedemann, 2019).

Este planteamiento cobra relevancia tratándose de plataformas y datos de usuarios, ya que esos compromisos por parte de las empresas y/o de las entidades resultantes de las fusiones u operaciones de concentración podrían ser revisados si las condiciones del mercado cambian, lo que es alta-

[1] Como es el caso, por ejemplo, de la Comisión Europea, la Autorità Garante della Concorrenza e del Mercato en Italia, entre otras.

mente probable tratándose de mercados dinámicos como los digitales. Además, los autores indican que las medidas en materia de competencia son más propensas a fomentar la competencia en los mercados digitales, ya que imponer condiciones más duras a las plataformas dominantes podría favorecer la entrada de nuevos actores al mercado (Botta & Wiedemann, 2019).

C. Riesgos de conglomerado

En línea con lo anterior, se ha planteado que los riesgos de conglomerado en el análisis de fusiones y concentraciones se acentuarían tratándose de operaciones en las que participa alguna plataforma digital.

Así, algunos autores sugieren que las teorías de daño que las autoridades de competencia planteen en sus análisis, deben adaptarse a los incentivos de las firmas en la economía digital. En particular, esto implicaría extender las teorías de empaquetamiento, flexibilizar los requisitos de la doctrina de las facilidades esenciales para el caso del acceso a datos y tomar directamente en cuenta los efectos de una operación de concentración en la innovación (Bourreau & de Streel, 2019).

Inclusive, otra parte de la doctrina ha sido más severa aún respecto de cómo debiesen las autoridades de competencia enfrentar este tipo de riesgos al momento de analizar operaciones de concentración que involucren plataformas digitales. Así, se ha postulado que el análisis de operaciones de concentración en mercados digitales debe considerar las implicancias económicas de la privacidad, de modo que ninguna operación debiese ser aprobada de manera incondicional si esta involucra el uso de datos de una cantidad relevante de usuarios (Chirita, 2019b).

En este sentido, desde hace algunos años se ha observado un aumento en la preocupación referida a los datos y la presunta concentración del acceso a los mismos en manos de menos empresas. Esto ha generado solicitudes a las autoridades, por parte de la opinión pública, de una regulación al respecto, y una mayor supervisión por parte de la legislación y autoridades antimonopolios (Körber, 2016).

Asimismo, otra preocupación desde el punto de vista regulatorio surge de las bases de datos de usuarios que están en manos de las plataformas digitales de economía colaborativa más relevantes (como por ejemplo, Uber y Airbnb), quienes –a su vez– compiten en cierta medida con los actores 'tradicionales' de esas industrias, pudiendo en esos casos la tecnología resultar disruptiva para muchas de esas empresas (Petropoulos, 2017).

Otras publicaciones más recientes postulan que los ecosistemas digitales se generan por los datos que recolectan, como un subproducto del *engagement* de los usuarios con sus plataformas gracias a la tasa y diversificación de los gigantes tecnológicos (como Amazon, Google, Netflix y Facebook, que incluyen transacciones y compras), y no solo por las externalidades y efectos de red o las economías de escala y ámbito (Petit & Teece, 2020, pp. 7-8).

Conforme a las posturas descritas, en todo caso, los datos representarían tanto una oportunidad de negocios como incerteza en el desarrollo de los mismos. Lo anterior, se debería a la indefinición acerca de las razones por las cuales algunos ecosistemas digitales superan sin mayor dificultad la falta de certeza respecto de la producción conjunta y los problemas de activos de conocimiento, mientras que otras no lo logran.

D. Innovación y dinamismo del mercado e incertidumbre para las autoridades de competencia

La indefinición acerca de lo que hace que una plataforma enfrente, con o sin dificultades, el dinamismo propio del mercado digital y/o se adapte por medio de la innovación genera –evidentemente– un problema de incertidumbre e información imperfecta para las autoridades a cargo de la aplicación de las legislaciones antimonopolio.

Este problema se vería exacerbado cuando se trata de plataformas digitales. Así, autores como Petit y Teece (2020, p. 10) plantean que es imposible determinar, durante el análisis que realiza la autoridad de competencia, la diferencia entre una práctica observada y alguna circunstancia alternativa que no existe actualmente y que pudiese observarse a futuro, dada la naturaleza dinámica de la industria digital. Esto lleva a las autoridades de competencia a alcanzar conclusiones en ocasiones erróneas (Petit & Teece, 2020, p. 10).

Al respecto, los mismos autores han planteado que una solución para este problema, desde el punto de vista de la legislación en materia de competencia, sería que se complementen las herramientas que tienen disponibles las autoridades con lo que denominan como "capacidades dinámicas" para el enfoque del análisis que realicen tanto economistas como abogados, llamando a una suerte de renacimiento en materia antimonopolio (Petit & Teece, 2020, p. 12).

Este planteamiento de Petit y Teece, aunque suene disruptivo, es posible de evidenciar en los análisis que ya han venido realizando diversas autoridades

en materia de competencia. En efecto, el dinamismo característico de los mercados digitales ha llevado a que algunas agencias reconozcan teorías de daños o riesgos derivados de fusiones y operaciones de concentración referidas a conglomerados distintos a aquellos identificados por las autoridades de competencia de acuerdo a la literatura económica clásica (OCDE, 2020b, p. 27).

Tratándose de análisis de competencia en casos de operaciones de concentración entre plataformas, es posible identificar la organización de productos o servicios de cara al usuario, organizados como parte de un ecosistema digital. La existencia de estos ecosistemas digitales generaría sinergias para los consumidores o usuarios, en el sentido de poder acceder a un solo ecosistema o plataforma que vincule diferentes productos y mercados, por ejemplo, bajo una marca y condiciones de privacidad.

Si bien lo anterior resultaría muy atractivo de cara al usuario, desde el punto de vista de la libre competencia, la integración de varias actividades en una misma plataforma podría ser problemático. Esto atendiendo a que la proliferación de estos ecosistemas digitales que vinculen distintos mercados puede, a la vez, generar barreras a la entrada de otros actores cuando un actor con poder de mercado busque adquirir otras empresas o plataformas. Esto, además, aumentaría los riesgos de coordinación derivados del aumento del contacto multimercado entre las distintas empresas tecnológicas (OCDE, 2020b, p. 28).

E. *Killer acquisitions*

Otra preocupación que es posible identificar en el análisis de las operaciones de concentración en mercados digitales es el eventual efecto de cierre en el mercado de la empresa adquirida, aun cuando la plataforma que la adquiere tenga una participación relevante en un mercado distinto. Esto porque la operación puede responder, más bien, a una estrategia de la plataforma ya presente en el mercado para evitar la competencia, eliminando a un competidor incipiente, en las denominadas *killer acquisitions* (OCDE, 2020b, p. 28).

De acuerdo a Cunningham, Ederer y Ma (2021), las plataformas incumbentes podrían tener incentivos para adquirir empresas incipientes o nuevas solo con el objeto de descontinuar los proyectos innovadores de esas empresas y así adelantarse –y evitar– a la competencia futura.

Al respecto, la Organización para la Cooperación y el Desarrollo Económicos (en adelante, OCDE) ha señalado recientemente que las autoridades de competencia han tenido un rol más bien tímido respecto de este tipo de riesgos para la competencia al analizar adquisiciones de empresas nuevas o incipientes, siendo necesario un enfoque más vigoroso (2020c).

Sin embargo, en este análisis es importante distinguir –y he ahí un dilema para la autoridad reguladora o de libre competencia– si la supuesta *killer acquisition* es realmente una operación de esa naturaleza o, más bien, es parte de un proceso legítimo de consolidación del mercado como resultado de la sobrevivencia de aquellos actores más eficientes por sobre otros que no lo son, o que no tienen capital o escala para lanzar un producto innovador.

Por otra parte, esta preocupación también surge cuando, de concretarse una adquisición de otra plataforma en otra actividad o mercado, se permite a la plataforma adquirente o resultante de la operación incurrir en una conducta de exclusión paralelamente en múltiples mercados digitales. Esto podría darse, de acuerdo a la OCDE, por ejemplo, por medio de la aplicación generalizada, de la plataforma, de cláusulas de precios de reventa o de nación más favorecida en todos los mercados en los que esté presente (2020b, p. 28).

F. Conductas de empaquetamiento

Por otra parte, otros riesgos de conglomerado que preocupan a las autoridades de competencia pueden surgir en operaciones de concentración de plataformas digitales cuando estas aplican una política de empaquetamiento de las políticas de privacidad o términos del consentimiento para el uso de datos con los que deben estar de acuerdo los usuarios. Esto se daría, por ejemplo, si una plataforma con una posición dominante obtiene el consentimiento para la recolección de datos de los usuarios en varias circunstancias. Así, si luego esa misma plataforma decide entrar a un nuevo mercado, en el cual existe un traslape de los usuarios respecto de los cuales cuenta con datos, podría usar ese consentimiento –ya existente– para recolectar datos de los usuarios en ambos mercados (OCDE, 2020b, p. 27).

En este sentido, y en la línea de lo planteado por Petit y Teece (2020), el empaquetamiento de políticas de privacidad sugiere que el enfoque dinámico de riesgos de conglomerado puede ajustarse a las características y comportamientos particulares en, al menos, algunos de los mercados de plataformas digitales, manteniéndose el desafío para las autoridades de competencia de desarrollar capacidades dinámicas para el análisis en los demás casos.

Conforme a lo anterior, se observa que –aun cuando el desarrollo de los mercados digitales es más bien reciente y esencialmente dinámico– existe cierto consenso, a nivel académico, de organismos internacionales como la OCDE y de autoridades de libre competencia, respecto de la existencia de los importantes desafíos en materia de fusiones y operaciones de concentración en mercados digitales, y en particular de plataformas, conforme a los desafíos ya descritos.

Sin descartar que esto responda a un fenómeno de isomorfismo normativo (producto de la pertenencia de distintas economías a la OCDE y a la reputación técnica de su Comité de Competencia) o mimético (producto de la imitación de criterios y recomendaciones dados por la OCDE por parte de las agencias de competencia, aun cuando estas pertenezcan a economías que no son partes de la organización), lo cierto es que los riesgos de conglomerado ya descritos han sido ampliamente identificados y analizados tratándose de operaciones de concentración en mercados digitales. Esto ha generado, durante los últimos años, el consecuente desarrollo de casuística por parte de las distintas agencias competentes en la materia.

En ese contexto, es posible observar que el análisis realizado por diversas agencias de competencia a nivel iberoamericano, con relación a operaciones de concentración referidas a plataformas digitales que han sido sometidas a su conocimiento, ha sido consistente con las distintas preocupaciones para la competencia vinculadas a los riesgos de conglomerado, indicados por la amplia literatura revisada como cruciales respecto del análisis de competencia referido a plataformas digitales.

III. CASOS

Los casos referidos en este artículo son los siguientes: (i) operación de concentración entre Walmart y Cornershop en Chile y en México; (ii) operación de concentración entre Uber y Cornershop en Chile y México; (iii) operación de concentración entre Naspers y Delivery Hero en España; y (iv) operación de concentración entre Just Eat y La Nevera Roja en España.

A. Caso Walmart /Cornershop

1. Chile

La operación sometida al análisis de la Fiscalía Nacional Económica (en adelante, FNE), consistió en la adquisición por parte de Walmart Chile, dedicada al negocio de supermercados, del negocio de servicios de compra y entrega a domicilio de productos consumibles *on demand* de Cornershop en Chile. Esta operación, finalmente, no se concretó, a pesar de contar con la aprobación de la autoridad.

En su informe, la FNE destacó el dinamismo del mercado de las plataformas *online* que permiten las compras de supermercados, considerando importantes cambios registrados entre 2017 y 2018, como el aumento considerable del tamaño del mercado, el ingreso de tres nuevos actores y las variaciones significativas en las participaciones de mercado de los distintos actores (Informe de aprobación, Rol FNE F161-2018, 2019, p. 5).

Con relación al mercado relevante, la autoridad distinguió el mercado *online* de las compras presenciales en supermercados (*brick and mortar*). Aquello principalmente porque los primeros serían utilizados solo por un número limitado y diferente de consumidores, junto con no encontrarse disponibles en todo el territorio nacional. En consecuencia, ambos segmentos en los que participaban las partes de la operación atenderían a públicos objetivos distintos.

Resulta interesante que la FNE reconoce en su informe que un análisis de riesgos a partir de la estructura actual de mercado no reflejaría adecuadamente las condiciones futuras de competencia entre las plataformas al tratarse de un mercado, esencialmente, dinámico. Conforme a lo anterior, el análisis asume expresamente un grado relevante de incertidumbre sobre la posición en el mercado en el futuro de los distintos actores (Informe de aprobación, Rol FNE F161-2018, 2019, p. 16). Luego, la FNE incluye una especie de *'disclaimer'*, por medio del cual indica que su análisis obedece a las condiciones actuales de un mercado con especial dinamismo, cuya evolución en el tiempo no es previsible para la autoridad (Informe de aprobación, Rol FNE F161-2018, 2019, pp. 20-21).

Con relación al uso de datos, la FNE descartó que Walmart pudiese obtener una ventaja competitiva relevante al acceder a datos sobre el comportamiento y patrones de consumo de los clientes de los supermercados competidores en un contexto de comercio digital en el cual no es desafiado.

Según la FNE, lo anterior es producto de que, si bien los datos recolectados por la plataforma de Cornershop constituían una herramienta valiosa para Walmart, a su juicio no sería relevante como riesgo. Walmart solo tendría acceso a información referida a un número acotado de clientes, considerando que la penetración del *e-commerce* en ese segmento era menor al 1%, por lo que no se generaría una asimetría competitiva significativa en favor del supermercado (Informe de aprobación, Rol FNE F161-2018, 2019).

Además, la FNE consideró en su análisis los riesgos referidos al acceso de datos recopilados por Cornershop por parte de Walmart, descartando que el riesgo fuese de tal magnitud que no pudiese ser respondido por los competidores existentes en el segmento de supermercados.

Conforme a lo anterior, el análisis desarrollado por la autoridad en este caso incluyó nuevamente una mirada dinámica del mercado, reconociendo la incertidumbre inherente a los mercados digitales, pero realizando una proyección acerca de cómo podrían responder los distintos actores.

2. México

La Comisión Federal de Competencia Económica (en adelante, Cofece) resolvió rechazar la operación de concentración por medio de la cual Walmart Holdings pretendía adquirir Cornershop MX (Resolución Expediente CNT-161-2018, 2019).

Walmart Holdings, filial de Walmart Inc., operaba al momento de la notificación de la operación en el mercado mexicano por medio de sociedades subsidiarias dedicadas a operar tiendas de autoservicio, farmacias y tiendas en línea, y a la comercialización de bienes por cuenta propia o de terceros a través de supermercados, almacenes y tiendas en línea. Por su parte, Cornershop MX pertenecía a Cornershop LLC, y prestaba servicios logísticos de exhibición, compra y entrega inmediata a usuarios finales de productos al por menor ofrecidos por tiendas de autoservicio y otros comercios a través de páginas de internet y de aplicaciones para dispositivos móviles.

La Cofece observó que las actividades desarrolladas por las partes de la operación objeto de su análisis estaban relacionadas en la cadena de valor del servicio logístico de compra y entrega inmediata de productos ofrecidos por comercios a través de páginas de internet y la plataforma de Cornershop MX. Así, identificó que Walmart Holdings y Cornershop MX participaban en distintos eslabones de la cadena de compra y entrega inmediata de productos ofrecidos por comercios a través de internet, por lo que la operación tendría efectos verticales (Resolución Expediente CNT-161-2018, 2019).

Al respecto, y atendiendo a que Cornershop MX operaba en un mercado de dos lados[2], la Cofece consideró que el análisis del mercado relevante debía considerar el análisis de sustitución en ambos lados de la demanda. Así, explicó que la plataforma debía mantener la demanda de los dos grupos de consumidores para poder existir, ya que el beneficio que un lado de los consumidores obtiene de la plataforma depende de la existencia de demanda del otro lado de clientes, y viceversa (Comisión Federal de Competencia Económica [Cofece], 2019).

El planteamiento de la Cofece, en este sentido, guarda relación con los efectos de red indirectos que se observan en las plataformas, las que serán viables en la medida que cuenten con una base sustentable de usuarios y de comercios que fortalezcan los efectos de red.

Esos efectos se ven disminuidos si es que las plataformas establecidas cuentan con contratos de exclusividad. En efecto, la Cofece señaló al respecto que en la medida que la exclusividad limite el número de socios comerciales a los que la nueva plataforma puede acceder, será menos competitiva en términos de variedad de productos ofrecidos en comparación con sus competidores, junto con ponerlas en desventaja en términos de precios (Resolución Expediente CNT-161-2018, 2019, p. 52).

Luego, dicha entidad procedió a analizar la competencia que enfrentaba Cornershop MX en distintas ciudades mexicanas, concluyendo que en varias de ellas no enfrenta competencia, a la vez que Walmart Holdings era la tienda de autoservicio mejor posicionada dentro de las plataformas en esas ciudades (Resolución Expediente CNT-161-2018, 2019). Conforme a lo anterior, la autoridad mexicana consideró la importante participación de mercado de Walmart Holdings, tanto en el mercado de las tiendas físicas como en el mercado digital en ciertas localidades, como indicativo de que esta podría desplazar a los competidores de Cornershop MX. Para ello, solo se requeriría que Walmart negara la oferta de sus productos a través de esas plataformas, o lo hiciera bajo condiciones distintas y desfavorables.

Además, la Cofece estimó que Walmart podría desplazar a sus competidores a través del uso indebido de la información detallada de los usuarios que utilizaban la plataforma de Cornershop MX. En la misma línea, estimó que Cornershop también tendría incentivos para establecer ventajas exclusivas en favor de Walmart o incluso, podría impedir el

[2] Esto quiere decir que tiene como clientes, por un lado, a los consumidores finales usuarios de la plataforma y, por otro lado, a los comercios que al estar en la plataforma pueden llegar al consumidor final sin necesidad de involucrarse en la recolección y envío de los productos.

acceso a la plataforma a los competidores de este. Finalmente, resolvió rechazar la operación, atendiendo que las condiciones propuestas por las partes no corregían los riesgos detectados y porque la empresa resultante de la operación podría tener la capacidad de establecer barreras a la entrada, impedir a terceros el acceso al mercado o desplazar a sus competidores en el mercado de las plataformas y de las tiendas de autoservicio (Cofece, 2019, p. 5).

La Cofece, al analizar el riesgo del uso de la información para fines anticompetitivos, consideró que la información que recababa la plataforma de Cornershop MX era estratégica. Esto contrasta con lo resuelto por la autoridad chilena respecto de la misma operación en Chile. En efecto, la Cofece consideró que la información a la que accedería Walmart por medio de Cornershop MX le permitiría conocer el patrón de consumo de clientes específicos en áreas específicas, lo que constituía, a su juicio, una ventaja competitiva y un riesgo de conglomerado.

Si bien las partes de la operación propusieron a la autoridad mexicana abstenerse de utilizar los datos referidos a información proporcionada por los comercios, así como la recopilada o desarrollada por la plataforma de Cornershop MX, la Cofece estimó que el compromiso era ineficaz para mitigar el riesgo de que Walmart desplazara indebidamente a otras tiendas de autoservicio a través del uso de dicha información (Resolución Expediente CNT-161-2018, 2019, pp. 85-86).

Conforme a lo anterior, el planteamiento de la Cofece en esta decisión estuvo fundado en el riesgo de cierre de mercado, ante la eventualidad de implementar Walmart una estrategia para evitar la competencia.

B. Caso Uber/Cornershop

1. Chile

La operación notificada a la FNE consistía en la adquisición por parte de Uber, empresa constituida en Estados Unidos dedicada al desarrollo de plataformas digitales a nivel mundial, de derechos que le permitirían influir decisivamente en la administración de Cornershop. Esta última, participaba en el comercio electrónico mediante plataformas digitales que intermedian la compra en línea y despacho a domicilio de productos de supermercados y otros comercios.

En Chile, y al momento de la notificación, Uber ofrecía servicios de intermediación para el transporte de pasajeros en automóviles por medio de la plataforma Uber, y de compra y entrega a domicilio de comida preparada por restaurantes y otros comercios por medio de la plataforma Uber Eats. Por su parte, Cornershop operaba a través de su plataforma del mismo nombre que provee servicios de compra en línea y entrega de bienes, principalmente de supermercados u otros comercios.

El análisis de la FNE señala que, durante la etapa final de la investigación, la pandemia de del COVID-19 constituyó una instancia para la recopilación de información valiosa y adicional acerca del efecto de dicha contingencia en el mercado de las plataformas de intermediación (Resolución de aprobación, Rol FNE F217-2019, 2020, p. 4).

En efecto, la autoridad de competencia evidenció que, desde la perspectiva de la demanda, se aceleraron cambios relevantes en el mercado producto de la pandemia, aumentando la demanda para los servicios de reparto de pedidos de supermercados. Ante esto, la estructura de la oferta habría sufrido modificaciones, apresurándose o anticipándose, por ejemplo, el desarrollo o despliegue de planes de expansión en el segmento de ventas en línea por parte de los competidores tanto de Uber como de Cornershop (Resolución de aprobación, Rol FNE F217-2019, 2020, p. 4).

La FNE, en este sentido consideró la pandemia del COVID-19 como un experimento natural, que corroboró que la expansión de los rivales de las partes de la operación eran proyectos predecibles que ante la contingencia sanitaria se aceleraron. Sin perjuicio de ello, la autoridad chilena aclaró en su decisión que la pandemia del COVID-19 no alteró ni determinó los resultados de la investigación, sino que solo vino a reforzar algunas de las estimaciones y conclusiones de la misma, especialmente el dinamismo de los mercados digitales (Resolución de aprobación, Rol FNE F217-2019, 2020). Así, la FNE terminó por aprobar la operación entre Uber y Cornershop, después de haber extendido su tramitación tras estimar que la operación podía reducir sustancialmente la competencia, por lo que ameritaba un estudio en profundidad de esta (Resolución de aprobación, Rol FNE F217-2019, 2020, p. 1).

A mayor abundamiento, en su informe, la FNE analizó diversos riesgos, entre ellos los de conglomerado por empaquetamiento de servicios de mercados relacionados. Para ello, la FNE realizó una encuesta a los usuarios, contenida en el Anexo del Informe (Informe de aprobación, Rol FNE F217-2019, 2020, Anexo). Los resultados mostraron que las estrategias de utilización de la posición de Cornershop para debilitar la competencia en

los mercados donde participa Uber y de utilización de la posición de Uber para debilitar la competencia en el segmento de supermercados, resultarían costosas para la entidad fusionada (Resolución de aprobación, Rol FNE F217-2019, 2020, p. 8).

Esto, porque la encuesta realizada por la autoridad chilena demostró, por un lado, que los consumidores finales de Cornershop no tendrían a la fecha del estudio una alta valoración de programas de fidelización que incorporen beneficios en los otros segmentos, por lo que las plataformas digitales de restaurantes tendrían posibilidades competitivas equivalentes (Resolución de aprobación, Rol FNE F217-2019, 2020, p. 8). Por otro lado, concluyó que una estrategia de empaquetamiento suficiente como para limitar las posibilidades de expansión de los competidores de Cornershop era poco plausible, dada la baja valoración de los consumidores finales de Cornershop por beneficios en otros mercados de plataformas de intermediación, según los resultados de la encuesta (Resolución de aprobación, Rol FNE F217-2019, 2020, p. 8).

Además, la investigación de la FNE habría demostrado que los competidores en el segmento de supermercados contaban con herramientas competitivas para reaccionar frente a estrategias de esta naturaleza por parte de la entidad resultante de la operación, lo que –en todo caso– además se habría acelerado ante la crisis sanitaria causada por la pandemia del COVID-19 (Resolución de aprobación, Rol FNE F217-2019, 2020, pp. 8-9).

Finalmente, y con relación a los riesgos de exclusión derivada de la concentración de datos e información de usuarios, la FNE evaluó si dicha información podría aportar una ventaja competitiva relevante a la entidad fusionada que le confiriera poder de mercado. Al respecto, la autoridad de competencia señaló que, si bien la información y datos de los consumidores finales representaba un elemento de utilidad para competir en este mercado, no constituirían el principal insumo para operar, sino únicamente un elemento de mejora funcional de los servicios ofrecidos (Resolución de aprobación, Rol FNE F217-2019, 2020, p. 9).

Finalmente, y con relación a un posible riesgo explicativo derivado de la disminución de la protección de los datos personales de los consumidores, la FNE examinó la capacidad de la entidad fusionada para condicionar una mayor cantidad de servicios a la aceptación de una política de privacidad común. Una estrategia de este tipo, a juicio de la FNE, se traduciría en una disminución de la calidad de los servicios ofrecidos a los consumidores finales. Al respecto, la autoridad chilena concluyó que la operación no significaría un cambio relevante para afectar las políticas de privacidad de los consumidores finales. Agregando luego que estos eventuales riesgos explotativos emanarían, más bien, de una condición propia de los mercados de plataformas, sin que resultara atribuible como efecto propio de la operación analizada (Resolución de aprobación, Rol FNE F217-2019, 2020, pp. 9-10).

Conforme a lo anterior, el análisis desarrollado por la autoridad en este caso incluyó una mirada dinámica del mercado, aprovechando incluso el experimento natural del impacto de la crisis sanitaria y las medidas de confinamiento en el aumento de la demanda por intermediación de compras.

Además, la FNE incluyó en su análisis consideraciones referidas a los datos como ventaja competitiva y a las posibles implicancias de determinadas políticas de privacidad, en línea con lo planteado por gran parte de la doctrina. Con todo, la FNE aprobó la operación sin medidas ni condiciones respecto del uso de datos, aun cuando ambas plataformas combinaban una cantidad relevante de usuarios. Lo anterior, en consideración al tamaño y capacidad de respuesta de los otros actores del segmento de supermercados, adoptando así la FNE una decisión en línea con lo planteado por la OCDE, pero con un criterio más laxo que el planteado por algunos autores, como Chirita (2019a; 2019b).

2. México

La Cofece conoció recientemente de la operación consistente en la compra de la plataforma Cornershop por parte de la plataforma Uber, la cual fue autorizada por la autoridad mexicana en diciembre de 2020.

Esta decisión fue resuelta, una vez que la competencia por parte de Cofece para realizar el análisis de dicha operación fuera establecida por el Primer Tribunal colegiado en Materia Administrativa especializado en Competencia Económica, Radiodifusión y Telecomunicaciones, tras haberse atribuido el Instituto Federal de Telecomunicaciones esa competencia a finales de 2019, una vez que las partes habían notificado la operación a la Cofece.

En particular, la Cofece exploró los potenciales riesgos de conglomerado, donde Uber pudiese trasladar los efectos de red hacia el negocio de *groceries* (comestibles) o viceversa, concluyendo que existían otros agentes que ejercen presión competitiva en ese negocio, además de competidores potenciales que podrían dar una oferta en dicho servicio en un tiempo relativamente corto (Cofece, 2021).

Este caso resulta interesante, en parte, porque el análisis de competencia fue realizado por la autoridad de competencia mexicana durante la crisis sanitaria generada por la pandemia del COVID-19, al igual que en el Caso Uber/Cornershop en Chile. Las circunstancias de la pandemia generaron cambios relevantes en el sector del comercio electrónico en general en México. En efecto, la Cofece estableció dentro de los antecedentes que tuvo a la vista para aprobar la operación, la información recopilada por la Asociación Mexicana de Venta Online, en sus reportes de impacto del COVID-19 en la venta *online*. Estos reportes muestran un crecimiento de un 152% de las visitas a las plataformas de entrega de comida en México entre los meses de febrero y octubre del 2020, contrastando con la disminución de las visitas a plataformas de pagos de servicios *online* y movilidad (Asociación Mexicana de Venta Online, 2020, p. 34).

De este modo, el análisis desarrollado por la autoridad mexicana en este caso incluyó una mirada dinámica del mercado, considerando datos acerca del uso de las plataformas generados con posterioridad a la notificación, es decir, sobre la base de circunstancias observadas en el transcurso de la investigación. Lo anterior podría considerarse, en concepto de Petit y Teece (2020), como el ejercicio de capacidades dinámicas para el enfoque del análisis de los mercados digitales, en línea con lo recomendado por organismos internacionales como la OCDE.

C. Caso Naspers/Delivery Hero en Brasil

El Consejo Administrativo de Defensa Económica (en adelante, CADE) del Ministerio de Justicia y Seguridad Pública de Brasil resolvió aprobar sin condiciones la operación mediante la cual Naspers Limited (en adelante, NL) adquirió participación en Delivery Hero (en adelante, DH) (Parecer 5/2018/CGAA1/SGA1/SG, 2018).

A la fecha del análisis desarrollado por el CADE, NL era una empresa sudafricana que, en sus operaciones en Brasil, invertía en empresas que operaban en los segmentos de publicidad, pagos, comercio y pedidos de comida hechos *online*, operando en el segmento de pedidos de alimentos en línea por medio de plataformas iFood y Spoonrocket. Por su parte, DH era un actor global en el segmento de pedidos y entregas de comida *online* y operaba en Brasil por medio de las plataformas OrdersJá y Subdelivery.

El CADE analizó el traslape horizontal entre NL y DH en el segmento de los pedidos de comida en línea, y resolvió aprobar la operación; aquello, considerando que la posición relevante de iFood en el mercado existía con anterioridad a la operación, sin que esta cambiara sustancialmente producto de la misma. Además, la autoridad brasilera de competencia señaló que la operación tenía lugar en un mercado con fuertes oportunidades de expansión, con la entrada de actores relevantes a nivel internacional en los últimos años (como Uber Eats), y respecto del cual se esperaba a futuro una intensificación en la rivalidad competitiva (Parecer 5/2018/CGAA1/SGA1/SG, 2018). En este sentido, el análisis del CADE muestra que la autoridad veía como alta la probabilidad de entrada de nuevos actores con potencial disruptivo, lo que llevó a concluir que la operación no dañaba el entorno competitivo.

Asimismo, resulta interesante observar que la decisión del CADE incluye una advertencia. Señala que iFood ya había adquirido diez empresas en Brasil, entre *startups* y empresas de grupos internacionales, estrategia que, ante el riesgo de representar una barrera a la entrada de nuevos agentes, debía ser monitoreada de cerca por la autoridad de competencia en casos futuros (Parecer 5/2018/CGAA1/SGA1/SG, 2018). Además, la decisión del CADE indicó que la existencia de contratos de exclusividad entre iFood y grandes cadenas de restaurantes, con alta visibilidad y mayor capacidad de atraer a los consumidores, también podrían representar eventuales barreras a la entrada de nuevos actores, haciendo menos atractivas a las plataformas rivales de cara a los clientes finales.

Considerando todo esto, la decisión de la autoridad brasilera aprueba sin condiciones la operación y al mismo tiempo advierte a NL el monitoreo que tendrá en eventuales futuras adquisiciones por parte suya, considerando la posición dominante que detenta iFood en el mercado de las plataformas, a manera de desincentivar una posible estrategia de *killer acquisitions*.

D. Caso Just Eat/La Nevera Roja en España

La Dirección de Competencia de la Comisión Nacional de los Mercados y la Competencia (en adelante, CNMC) de España resolvió aprobar la operación de concentración por medio de la cual Just Eat Holding Limited (en adelante, JE) adquirió el 100% del capital social de la compañía Digital Services LII (Gp), S.A.R.L., que indirectamente disponía del 100% del capital social del Grupo Yamm Comida a Domicilio, S.L., que operaba bajo el nombre La Nevera Roja (en adelante, LNR) (Resolución del Expediente C/0730/16, 2016).

Al momento del análisis de la operación por parte de la CNMC, JE pertenecía a un grupo empresarial

británico que operaba en el sector de la gestión de pedidos de comida a domicilio por internet, actuando como intermediario entre consumidores finales y restaurantes, a través de su plataforma *online*. Por su parte, LNR era una sociedad española que también actuaba como intermediario entre consumidores y restaurantes, por medio de su plataforma *online*.

La CNMC consideró que el modelo de negocios que desarrollan estas plataformas *online* depende de dos demandas interdependientes, dando lugar a un contexto de los denominados mercados de dos caras o *two-sided markets*.

Conforme a ello, la autoridad española en su análisis distingue dos mercados: por un lado, el mercado de plataformas *online* de gestión de pedidos de comida a domicilio, en el que actuarían como demandantes los restaurantes; y, por otro lado, el mercado de los servicios de comida a domicilio, en el que actúan como demandantes los clientes finales.

Finalmente, la CNMC resolvió aprobar la operación, con compromisos por parte de JE, todos ellos, respecto del mercado de los servicios en el cual los restaurantes representan la demanda (Resolución del Expediente C/0730/16, 2016). En este sentido, si bien la operación fue aprobada con medidas o compromisos, ninguno de ellos guardó relación con el uso de los datos de los clientes finales a los que tenían acceso ambas plataformas.

En efecto, los compromisos adoptados guardaron relación, más bien, con mitigar los riesgos identificados respecto de la demanda de los restaurantes y que pudiesen actuar como cerrojo respecto de otras plataformas (riesgos de abusos excluyentes por medio de la implementación de exclusividades).

Los compromisos quedaron establecidos en los siguientes términos: (i) JE se comprometería a no mantener o establecer ningún tipo de exigencia de exclusividad formal o *de facto*, total o parcial, en la relación contractual que mantuviese con los restaurantes afiliados (actuales o futuros) a sus plataformas en España; (ii) JE se comprometería a no vincular, ni directa ni indirectamente, el nivel de las comisiones acordadas con los restaurantes (actuales o futuros) con ninguna relación de exclusividad con las plataformas de JE en España; y (iii) JE se comprometería a no implementar ninguna medida, formal o *de facto*, que pudiera penalizar a un restaurante afiliado (actual o futuro) con motivo de su afiliación a una plataforma de un tercero (Resolución del Expediente C/0730/16, 2016).

IV. CONCLUSIONES

Las autoridades de competencia enfrentan diversos desafíos al momento de aprobar, con o sin medidas, o prohibir, operaciones de concentración que involucren plataformas digitales.

El análisis de los efectos de red que generan las plataformas y los ecosistemas digitales va de la mano, además, con el problema de la incertidumbre e información imperfecta. En efecto, los mercados digitales muestran comúnmente significativas economías de escala, con altos costos fijos y bajos o nulos costos variables (OCDE, 2020a, p. 17). Esto los dota de gran dinamismo e impredictibilidad, lo que exige a las autoridades antimonopolios contar con una mirada prospectiva en su análisis de competencia de estos mercados.

El dinamismo propio de las plataformas digitales, así como las interrogantes que se generan respecto del uso de datos y su evolución, han sido reconocidos por algunas autoridades de competencia, quienes –en determinados casos– han debido enfrentar experimentos naturales de *shock* exógeno en los mercados de plataformas de intermediación. Sin ir muy lejos, la pandemia del COVID-19 sin duda ha sido, al menos para el caso de la operación de concentración entre Uber y Cornershop analizada por las autoridades de competencia en Chile y México, un antecedente que vino a corroborar el dinamismo del mercado y las capacidades de los rivales de adaptarse a aumentos de demanda por los servicios.

También, las autoridades de competencia han tenido la oportunidad de desarrollar capacidades dinámicas en sus análisis de operaciones de concentración de plataformas. En este sentido, destaca el análisis del CADE en el caso de Naspers y Delivery Hero, en el cual la autoridad brasilera mostró una preocupación por intervenir sin afectar negativamente la innovación, considerando las perspectivas de crecimiento del mercado y la presencia de actores internacionales, lo que dificultaría –a juicio de esa autoridad– decir que una plataforma cuenta con un poder de mercado estable (Parecer 5/2018/CGAA1/SGA1/SG, 2018).

Asimismo, la creciente relevancia de las plataformas ha venido aparejada de una mayor preocupación respecto de los datos de los clientes y usuarios de las plataformas. Si bien esto puede ser relevante desde el punto de vista de los derechos de los consumidores y de la protección de la privacidad, los casos comentados han señalado que, para efectos del análisis de libre competencia de una operación de concentración, los datos de usuarios son relevantes, en la medida que puedan ser con-

siderados como un activo valioso, que otorgue una ventaja difícil de replicar en el tiempo o a un costo determinado.

Los riesgos de conglomerado en el análisis de competencia de operaciones de concentración entre plataformas han sido planteados en los casos analizados. La mayoría de las decisiones incluyeron argumentos bajo la lógica de que una plataforma digital con poder de mercado podría tener incentivos para utilizar los datos de los usuarios para luego incorporarse a nuevos mercados. De este modo, aun cuando con matices, se observa que en determinados casos recientes de análisis de operaciones de concentración en mercados digitales, las autoridades de competencia a nivel iberoamericano objeto de estudio en este artículo han abordado los desafíos de incertidumbre y de riesgos de conglomerado asociados al uso de datos de los usuarios en sus decisiones.

Con todo, es necesario recordar que las reglas que promueven y defienden la libre competencia no prohíben ni sancionan el poder de mercado en sí. Por ende, tampoco está prohibido el poder sobre datos de usuarios que un determinado actor del mercado pudiese tener, ya que para la procedencia de sanciones se requiere de una conducta abusiva de ese poder de mercado (ya sea explotativa o exclusoria). En este sentido, aun cuando los casos de operaciones de concentración que involucran plataformas digitales son cada vez más frecuentes, todavía existen muchas incógnitas acerca de la relevancia de los datos en los mercados digitales, por lo que se requiere mayor investigación a este respecto (Körber, 2016).

En este sentido, la recomendación formulada por la OCDE en esta materia está orientada a las autoridades de competencia, quienes deberán ser capaces de aplicar análisis basados en efectos, junto con la necesidad de evitar la adopción de acciones que puedan crear desincentivos a la innovación (OCDE, 2020a, p. 59). Asimismo, la organización ha hecho un llamado a las agencias de competencia para que estas adopten un rol más vigoroso en el análisis de las adquisiciones de empresas nuevas o incipientes, levantando el riesgo de un posible *under-enforcement* en esta materia (OCDE, 2020a)

Conforme a lo anterior, el análisis de riesgos para la competencia derivados de operaciones de concentración que involucran plataformas digitales representa un desafío tanto para aquellas agencias que ya vienen conociendo de casos referidos a mercados digitales, como para aquellas que deberán conocer de estos a futuro sin contar con experiencia previa, como consecuencia, por ejemplo, de la entrada en vigencia de nuevos sistemas de control de operaciones de concentración[3].

En consecuencia, un mayor conocimiento e investigación en estas materias, sin duda, sería un aporte para las autoridades de competencia y reguladores a nivel iberoamericano. Esto lograría reducir el riesgo de intervenciones apresuradas o decisiones adoptadas con escaso entendimiento de los mercados digitales, las que en ocasiones pueden generar más daño que aquel que pretendían evitar.

REFERENCIAS

Arroyo Barrigüete, J. L. (2007). *Externalidades de Red en la Economía Digital Introducción a la modelización de mercados de redes mediante la teoría de sistemas dinámicos.* Marcial Pons Ediciones Jurídicas y Sociales S.A.

Asociación Mexicana de Venta Online (2020). *Reporte 5.0 Impacto Covid-19 en Venta Online México*. https://www.amvo.org.mx/estudios/reporte-5-0-impacto-covid-19-en-venta-online-mexico/

Botta, M., & Wiedemann, K. (2019). The Interaction of EU Competition, Consumer, and Data Protection Law in the Digital Economy: The Regulatory Dilemma in the Facebook Odyssey. *The Antitrust Bulletin, 64*(3), 428-446. https://dx.doi.org/10.2139/ssrn.3462983

Bourreau, M., & de Streel, A. (2019). *Digital Conglomerates and EU Competition Policy*. Centre on Regulation in Europe. http://www.crid.be/pdf/public/8377.pdf

Chirita, A. (2019a). *Abusive Global Platform Dominance or Competition on the Merits?* (Durham Law School Research Paper 2019). https://ssrn.com/abstract=3540987

(2019b). Data-Driven Mergers Under EU Competition Law. En J. Linarelli & O. Akseli (eds.), *The Future of Commercial Law: Ways Forward for Harmonisation* (pp. 147-183). Hart Publishing.

Comisión Federal de Competencia Económica [Cofece] (2019). *Sobre el análisis de concentraciones con modelos de negocios innovadores: Operación no autorizada Walmart-Cornershop.*

[3] Como en el caso de Perú, a partir de la publicación, con fecha 7 de enero de 2021, de la Ley 31112 que establece el Régimen del control Previo de Operaciones de Concentración Empresarial.

Análisis de casos. https://www.cofece.mx/wp-content/uploads/2019/08/AnCAs-CornerShop-12agsoto2019.pdf

(2021). *Concentración Uber-Cornershop*. Análisis de caso. https://www.cofece.mx/wp-content/uploads/2021/02/art-Uber-cornershop-03febrero2021.pdf

Cunningham, C., Ederer, F., & Ma, S. (2021). Killer Acquisitions. *Journal of Political Economy, 129*(3), 649-702. https://doi.org/10.1086/712506

De Elejalde, R. (2020). Plataformas digitales: nuevos desafíos para políticas de defensa de la libre competencia. *Observatorio Económico FENUAH,* (148), 4-5. https://doi.org/10.11565/oe.vi148.377

Fiscalía Nacional Económica [FNE] (2012). *Guía para el Análisis de Operaciones de Concentración.* https://www.fne.gob.cl/wp-content/uploads/2012/10/Guia-Fusiones.pdf

Körber, T. (2016). Is Knowledge (Market) Power? - On the Relationship Between Data Protection, 'Data Power' and Competition Law. *NZKart,* 303-334.

McSweeny, T., & O'Dea, B. (2018). Data, Innovation, and Potential Competition in Digital Markets - Looking Beyond Short-Term Price Effects in Merger Analysis. *CPI Antitrust Chronicle February 2018*, 1-7.

Nayak, N. (2019). *Barrier to Entry and Disruptive Innovation Potential in Big Data Markets: A Literature Review.* https://ssrn.com/abstract=3388218

Organización para la Cooperación y el Desarrollo Económicos [OCDE] (2017). *Foro Latinoamericano y del Caribe de Competencia. Sesión II: Control de fusiones en América Latina y el Caribe - Evolución y tendencias recientes.* https://one.oecd.org/document/DAF/COMP/LACF(2017)2/es/pdf

(2020a). *Abuse of Dominance in Digital Markets.* https://www.oecd.org/daf/competition/abuse-of-dominance-in-digital-markets-2020.pdf

(2020b). *Roundtable on Conglomerate Effects of Mergers - Background Note by the Secretariat.* https://one.oecd.org/document/DAF/COMP(2020)2/en/pdf

(2020c). *Start-ups, Killer Acquisitions and Merger Control - Background Note by the Secretariat.* https://one.oecd.org/document/DAF/COMP(2020)5/en/pdf

Petit, N., & Teece, D. (diciembre de 2020). *Taking Ecosystems Competition Seriously in the Digital Economy*. Trabajo presentado en Hearing on Competition Economics of Digital Ecosystems de la Organización para la Cooperación y el Desarrollo Económicos, Lausana, Suiza.

Petropoulos, G. (2017). An economic review of the collaborative economy. *Bruegel Policy Contribution Issue*, (5), 1-17.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Comisión Federal de Competencia Económica [Cofece], 27 de mayo de 2019, Pleno Resolución Expediente CNT-161-2018 (Méx.).

Comisión Nacional de los Mercados y la Competencia [CNMC], 31 de marzo de 2016, Resolución del Expediente C/0730/16 (Just Eat/La Nevera Roja) (Esp.).

Consejo Administrativo de Defensa Económica [CADE], 8 de marzo de 2018, Parecer 5/2018/CGAA1/SGA1/SG, Processo 08700.007262/2017-76 (Naspers/Delivery Hero) (Bras.).

Dun & Bradstreet Corp., F.T.C. 091 0081, Docket No. 9342 (2010) (EE.UU.).

Fiscalía Nacional Económica [FNE], 11 de enero de 2019, Informe de aprobación, Rol de causa: FNE F161-2018 (Chile).

Fiscalía Nacional Económica [FNE], 29 de mayo de 2020, Anexo del Informe de aprobación, Rol de causa: FNE F217-2019 (Chile).

Fiscalía Nacional Económica [FNE], 29 de mayo de 2020, Informe de aprobación, Rol de causa: FNE F217-2019 (Chile).

Fiscalía Nacional Económica [FNE], 29 de mayo de 2020, Resolución de aprobación, Rol de causa: FNE F217-2019 (Chile).

Tribunal de Defensa de la Libre Competencia, 25 de octubre de 2004, "Consulta sobre fusión de Metropolis Intercom S.A. y VTR S.A.", Resolución 1/2004 (Chile).

10.18800/themis.202101.021

SMART CONTRACTS COMO SOLUCIÓN EFICIENTE A LOS NUEVOS PROBLEMAS DEL CONSUMIDOR EN EL *E-COMMERCE*

SMART CONTRACTS AS AN EFFICIENT SOLUTION TO THE CONSUMER'S DISTRUST OF E-COMMERCE

Isabella Monsante Moy*
Pontificia Universidad Católica del Perú

Ariana Novoa Suárez**
Exmiembro del Consejo Directivo de THĒMIS
Pontificia Universidad Católica del Perú

Alejandra Quintanilla Gutiérrez***
Exmiembro del Consejo Ejecutivo de THĒMIS-Revista de Derecho
Miranda & Amado

The exponential growth of e-commerce in Peru has generated new problems in the effectiveness of consumer rights and the consequent consumer distrust in e-commerce transactions. Government authorities have repeatedly mentioned that a solution to these problems would be the regulation of electronic consumer's relationships established at national level. This solution goes on the same page with the tendency of the European Union to regulate digital markets. However, is the legislative initiative an ideal solution to solve the new problems generated by e-commerce?

In this article, the authors find that regulation of e-commerce would not completely solve the new problems generated by it. They evidence the necessity of utilizing market solutions based on new technological mechanisms such as smart contracts. These tools, together with the incentive of the authorities that protect consumers' rights, will be able to efficiently solve the new problems that are generated in this new decade.

Keywords: Consumers; e-commerce; smart contracts; regulatory impact analysis; international cooperation

El crecimiento exponencial del e-commerce *en el Perú ha generado nuevos problemas en el cumplimiento de los derechos de los consumidores y la consecuente desconfianza del consumidor en las transacciones de comercio electrónico. Diversas autoridades han propuesto como solución que se regulen las transacciones de* e-commerce *realizadas en el ámbito nacional, en línea con la tendencia de la Unión Europea a regular los mercados digitales. Sin embargo, ¿es la iniciativa legisladora una solución idónea para resolver los nuevos problemas generados por el* e-commerce*?*

En el presente artículo, las autoras analizan cómo una ley de e-commerce *no resolvería por completo los nuevos problemas generados por este y plantean la necesidad de contar con soluciones desde el mercado, elaboradas a partir de nuevos mecanismos tecnológicos como los* smart contracts*. Estas herramientas, junto con el incentivo de las autoridades que protegen derechos de los consumidores, podrán resolver de forma eficiente los nuevos problemas que se generan en esta nueva década.*

Palabras clave: Consumidores; e-commerce*;* smart contracts*; análisis de impacto regulatorio; cooperación internacional*

* Estudiante de Derecho en la Pontificia Universidad Católica del Perú (PUCP) (Lima, Perú). Asistente de Docencia en la Facultad de Derecho de la PUCP. Practicante pre-profesional en Cuatrecasas (Lima, Perú). Contacto: isabella.monsante@pucp.edu.pe

** Estudiante de Derecho en la Pontificia Universidad Católica del Perú (PUCP) (Lima, Perú). Exmiembro del Consejo Directivo de THĒMIS. Asistente del curso de Contratos en la Facultad de Derecho y del curso de Derecho en Estudios Generales Letras de la PUCP. Practicante pre-profesional en Bullard, Falla, Ezcurra+ (Lima, Perú). Contacto: anovoa@bullardabogados.pe

*** Abogada. Ex asistente legal corporativa en la Comisión de Defensa de la Libre Competencia del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Lima, Perú). Asociada del área corporativa de Miranda & Amado (Lima, Perú). Contacto: alejandra.sqg@gmail.com

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 11 de enero de 2021, y aceptado por el mismo el 17 de abril de 2021.

"*Whereas in the 20th century capitalism was organised around large, industrial companies, much of the contemporary economy is organised around software-driven platforms*"

Mark Fenwick & Erik Vermulen

I. INTRODUCCIÓN

En la última década, el comercio electrónico (en inglés, *e-commerce*) ha cobrado gran importancia a nivel global y, por supuesto, el Perú no ha sido ajeno a este fenómeno.

En el año 2009, el Perú representaba solo el 1.27% del valor del comercio electrónico en Latinoamérica. Sin embargo, diez años después, nuestro país se ha posicionado en el sexto lugar en ventas *online* en la región con un 5% de valorización en este sector. Así, aunque el *e-commerce* en el Perú sigue siendo un mercado relativamente pequeño, ha crecido de forma continua y consistente a través de los años (Cámara Peruana de Comercio Electrónico [Capece], 2019, p. 4).

Además, en el 2020, como consecuencia de la pandemia del COVID-19 y las medidas estatales de inmovilización ciudadana, se ha incrementado exponencialmente en toda la región el número de compradores *online*. Así, el Perú pasó de 6 millones en 2019 a 11.8 millones en el 2020 (Radio Programas del Perú [RPP], 2021a). Más aún, el Perú ha sido el país de Latinoamérica con mayor crecimiento en el sector de *e-commerce* (Montes, 2021).

No obstante, el cambio de una relación de consumo presencial a una relación de consumo electrónica ha generado nuevos retos que la normativa actual se encuentra limitada para solucionar. Como establece el jurista León Hilario, en los escenarios de *e-commerce*, "se prefieren […] la autorregulación y el trato directo en lugar de los mecanismos pasados de moda del Código Civil" (2019, p. 60).

En ese sentido, cualquier regulación que no resuelva los nuevos problemas generados por el *e-commerce* pierde vigencia, "si no es que ha quedado derogada en los hechos, en observancia del principio de efectividad de las normas" (León Hilario, 2019, p. 60).

Por ejemplo, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (en adelante, Indecopi) ha informado que, al cierre de agosto del 2020, se han generado un total de 60 000 quejas y reportes en relaciones de consumo electrónicas (Bravo Tejeda, 2020b). Entre los reclamos más comunes se encuentra que el proveedor no entregó el producto, no se les reembolsó el dinero pagado, la cancelación o anulación del pedido sin previo aviso, entre otros (Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [Indecopi], 2020).

Asimismo, se generaron problemas que escapaban del ámbito de aplicación del Código de Protección y Defensa del Consumidor vigente, debido a que algunos proveedores establecen como ley y jurisdicción aplicable la de su domicilio legal o la que les sea más favorable. En el año 2015, el *e-commerce* transfronterizo representaba solo el 14% de las compras *online*; en cambio, en el 2019 aumentó a un 25% (Capece, 2019, p. 5). Cabe resaltar que las páginas web de comercio electrónico transfronterizo tienen en sus términos y condiciones, leyes y jurisdicción aplicables que excluyen a la normativa aplicable al país del consumidor.

Estos nuevos problemas generan mayor desconfianza en el mercado del *e-commerce*. Los consumidores no tienen la posibilidad de ir a un establecimiento y poder reclamar por el incumplimiento (tardío, defectuoso, parcial) porque no saben cómo localizar a su proveedor y, si es que ubican la sede social, los costos de tutela son tan elevados que desincentivan su uso.

Por ello, se debe buscar resolver estos nuevos problemas desde un enfoque que garantice los derechos de los consumidores e incentive el desarrollo de la economía a través del *e-commerce*. Dicha búsqueda llevará al uso de herramientas tecnológicas para efectivizar el cumplimiento de los derechos.

Las tecnologías basadas en el *blockchain*, como los *smart contracts*, fomentan la protección al consumidor en diversos aspectos. Al mismo tiempo, se configuran como una potencial solución a la falta de confianza en el mercado del *e-commerce*.

En ese sentido, la primera parte de este trabajo se concentra en definir qué se entiende por *e-commerce*, el alcance de este mercado en nuestro país y los principales problemas que se generan en estas relaciones de consumo.

En la segunda parte se dedicará a realizar un breve análisis del impacto regulatorio de la creación de una ley de *e-commerce* con el propósito de determinar si se cumplen con los objetivos de mitigar los riesgos generados por las transacciones electrónicas y establecer si existe una alternativa más idónea para la solución de problemas.

En la tercera parte, se hará un especial énfasis en los beneficios que los *smart contracts* traen para los actores involucrados (consumidores y empre-

sas) mediante la revisión de diversos casos de aplicación de estos mecanismos en relaciones de consumo electrónicas. Asimismo, se realizará una comparación de cómo el sector aerocomercial utilizó los *smart contracts* para la autotutela de los derechos de los consumidores frente a la tardía solución que planteó la autoridad gubernamental al mismo sector económico en la Resolución 2107-2020/SPC-INDECOPI (2020) de la Sala Especializada en Protección al Consumidor del Tribunal del Indecopi (en adelante, la Sala).

En la cuarta parte, se plantearán recomendaciones del empleo de tecnologías para el sector privado a la luz de las recomendaciones de diversos organismos internacionales como la Organización para la Cooperación y Desarrollo Económicos (en adelante, OCDE) y la Unión Europea, así como estudios internacionales de economía conductual. Estas recomendaciones tienen por objetivo aumentar la confianza de los consumidores garantizando sus derechos por su condición de tales.

II. *E-COMMERCE* EN EL PERÚ

A. Definición de *e-commerce*

El *e-commerce* no es una figura nueva en el país ni mucho menos en el continente. Al contrario, se ha venido desarrollando desde hace más de una década. En este lapso, diversas entidades se han pronunciado al respecto de la misma y han tratado de analizar las similitudes y diferencias de una relación de consumo presencial y una de *e-commerce*.

En esta línea, la Organización Mundial del Comercio indica lo siguiente:

> El comercio electrónico es **la compra o venta de bienes o servicios realizada a través de redes informáticas por métodos específicamente diseñados para recibir o colocar pedidos**. Aun cuando los pedidos de bienes o servicios se reciben o colocan electrónicamente, no es necesario que el pago y la entrega o prestación final de los bienes o servicios se realicen en línea (2013, p. 2) [el énfasis es nuestro].

Según el Indecopi, el comercio electrónico es "**aquel conjunto de actividades económicas lucrativas que se realizan a través de redes informáticas por métodos específicamente diseñados para la oferta y recepción de pedidos de bienes o servicios**" (Resolución Final 1632-2015/CC2, 2015, párr. 18) [el énfasis es nuestro].

Así, el *e-commerce* no solamente implica las ventas que el empresario y el usuario realizan a través de internet, sino que "**engloba todas las fases del negocio empresarial, siempre que estas se realicen a través de la red"** (Millé, 1998, citado en Resolución Final 1632-2015/CC2, 2015, párr. 18) [el énfasis es nuestro].

A partir de ello, podemos entender al *e-commerce* como "la virtualización de las transacciones comerciales" y, en cierto sentido, como consecuencia de un mayor acceso a las nuevas tecnologías por parte de la población (Aldana, 2018, p. 16). Así, se han generado nuevas formas de contratación en las cuales, mediante un solo clic, se puede entablar una relación de consumo[1].

B. Desarrollo del *e-commerce* a nivel nacional

El desarrollo del *e-commerce* en nuestro país antes del 2020 había sido continuado y consistente. Sin embargo, la pandemia del COVID-19 se ha configurado como un hito que marcará el inicio de una nueva era en la cual este tipo de transacciones formarán parte del día a día de los peruanos.

Prueba de ello son las estadísticas establecidas por la Cámara de Comercio de Lima, la cual indicó que, haciendo una comparación entre las transacciones de *e-commerce* realizadas en el mes de junio del 2019 y el mes de junio de 2020, este último habría crecido en 225% frente al mismo mes del año pasado (RPP, 2020).

De acuerdo con los estudios de la Cámara Peruana de Comercio Electrónico (en adelante, Capece), el *e-commerce* creció un 50% durante el 2020, registrando ganancias de US$ 6 000 millones.

Además, el presidente de la Capece, Helmut Cáceda, señaló que en 2020 se ha acelerado el comercio electrónico de cinco años en solo seis meses. De esta manera, a diferencia de otros sectores económicos, el *e-commerce* se ha visto fuertemente impulsado como consecuencia de la pandemia del COVID-19.

[1] Cabe señalar que este trabajo se concentra en la economía del *e-commerce* entre proveedor y consumidor, donde existe, en efecto, una relación de consumo. En esa línea, destacamos que las economías colaborativas, no forman parte de este trabajo. En nuestro país, la Resolución 0084-2020/SDC del Indecopi marcó un precedente importante en esta materia, sosteniendo que, en las economías colaborativas, no existe relación de consumo entre la plataforma de 'contacto' y el cliente. Así, en esta decisión, se sostiene que Uber no mantiene una relación de consumo entre el cliente que solicita un taxi y esta plataforma, ya que ella solo sirve como intermediación entre el proveedor (el taxista) y el cliente (el pasajero) (Resolución 0084-2020/SDC, 2020). En efecto, plataformas como Uber, Airbnb o Rappi, ahorran costos de transacción a las empresas y clientes, y permiten tener un mayor flujo de la economía en determinados sectores (en los ejemplos: servicios de taxi, hospedaje y gastronomía).

Antes del coronavirus, solo 65 800 comercios (1.5%) vendían a través del canal digital, pero esta cifra se cuadruplicó ante las medidas de cuarentena e inmovilización. Así, el número de compradores *online* en el Perú pasó de seis millones en 2019 a 11.8 millones en el 2020 (RPP, 2021a).

Respecto al método de pago, en el 2020, el 35% de las compras fueron realizadas con tarjetas, cuando antes estos solo representaban el 12.5%.

Sin perjuicio de lo mencionado, así como ha aumentado el número de compras por internet también lo ha hecho la cantidad de reclamos por parte de los consumidores.

C. Problemas del *e-commerce* en el Perú

1. Problemas respecto de la prestación en la relación de consumo

Ante el aumento exponencial de compras por internet como resultado de la pandemia, también se han incrementado el número de reclamos por parte de los consumidores. Según el Centro Especial de Monitoreo del Indecopi (CEMI), durante 2020 se registraron, aproximadamente, 56 829 reportes y consultas de consumidores asociadas a incidencias en comercio electrónico. Dentro de las conductas más reportadas se encuentra la no entrega del (56.26%), el no reembolso de dinero (14.65%), los pedidos incompletos (6.55%) y la cancelación de pedido por falta de *stock* (5.23%), entre otros.

Además, cabe resaltar que hubo 38 144 reclamos concluidos ante el Servicio de Atención al Ciudadano (SAC) del Indecopi, nivel que fue mayor en 5.0 veces más que lo reportado en el año 2018 y 3.4 veces más que lo reportado en el año 2019 (Indecopi, 2021).

Con respecto a la no entrega del producto, en julio de 2020, la Secretaría Técnica de la Comisión de Protección al Consumidor 3 del Indecopi estableció una medida cautelar contra trece empresas de comercio electrónico. Así, ante el número excesivo de reclamos respecto al incumplimiento en la entrega de productos adquiridos de forma *online*, Indecopi estableció que estas empresas tenían un plazo de diez días para que realicen las prestaciones prometidas o devuelvan el dinero a los consumidores afectados. Además, la Secretaría Técnica inició procedimientos administrativos sancionadores contra cada una de estas empresas por la presunta infracción al deber de idoneidad (El Comercio, 2020).

Con respecto a la anulación de pedidos, en 2015, Indecopi emitió la Resolución 3816-2015/SPC respecto al caso de un usuario que adquirió tres colchones a S/ 1.00, a través de la tienda *online* de Ripley. Sin embargo, Ripley anula la compra, pues el colchón realmente tenía un precio de S/ 1500.00 y, como consecuencia de un error del sistema, aparecía a solo S/ 1.00 en el catálogo virtual. La Sala Especializada en Protección al Consumidor señaló que,

> cuando el denunciante pone en conocimiento del proveedor su aceptación a la oferta y el proveedor emite las órdenes de compras, entonces el proveedor se encuentra en la obligación

CEMI: *Ranking* de las conductas reportadas, marzo-diciembre 2020

Nº	Conducta reportada	Total	%
1	No entrega de producto o pedido	31 973	56.26
2	No reembolso de dinero	8 323	14.65
3	Pedido incompleto	3 725	6.55
4	Cancelación de pedido por falta de stock	2 973	5.23
5	Falla de producto	2 008	3.53
6	Por procesar*	1 064	1.87
7	Plataforma virtual no procesa compra	1 018	1.79
8	Cobros indebidos	954	1.68
9	No acceso a cambio de producto	870	1.53
10	Otra competencia	767	1.35
11	Publicidad engañosa	690	1.21
12	No atención de canales de comunicación	661	1.16
13	No entrega de LDR o inoperativo	402	0.71
14	No desafiliación o cancelación de suscripción	313	0.55
15	Atención no idónea del personal	304	0.53
16	Otros	784	1.38
	Total	**56 829**	**100**

* Falta procesar la conducta reportada.

Fuente: Centro especial de Monitoreo
Elaboración: Gerencia de Estudios Económicos del Indecopi (en Indecopi, 2021, p. 6)

> de reconocer la oferta publicitada, pues de lo contrario estarían defraudando las expectativas del consumidor (Indecopi, 2018, p. 36).

Asimismo, en 2016, Indecopi analizó el caso de un consumidor que compra un set de muebles a través de la plataforma *e-commerce* de Linio. Pero, la empresa cancela la compra sin ninguna explicación al usuario. Ante esto, en la Resolución 1971-2016/CC2, Indecopi señaló que Linio debió cumplir con las prestaciones contratadas en el plazo y modos previstos, pues no puede cancelar una compra de manera unilateral (2016).

2. Problemas respecto de la ley y jurisdicción aplicables a las relaciones de consumo

Debemos diferenciar entre el comercio electrónico doméstico y el *e-commerce* transfronterizo o *cross-border*. Mientras que el primero hace referencia a páginas web con dominio del mismo país en el que se encuentra el consumidor; el segundo se refiere a las páginas web de comercio electrónico que tienen en sus términos y condiciones leyes y jurisdicción aplicables que excluyen a la normativa aplicable al país del consumidor.

Así, en el caso de los consumidores peruanos que contraten a través de la página web de Alibaba.com[2], deben tener en cuenta la cláusula de resolución de controversias de los términos y condiciones establece lo siguiente:

> El presente acuerdo se regirá por las leyes de la República Popular China ("RPC") si usted contrata con Hangzhou Alibaba Advertising Co., LTD, según lo dispuesto en el párrafo 2.1; y las partes en el presente acuerdo se someten a la jurisdicción exclusiva del Tribunal Básico de Yuhang, Hangzhou, RPC. Si su acuerdo es con Alibaba.com Hong Kong Limited o Alibaba.com Singapore E-commerce Privated Limited, el presente acuerdo se regirá por las leyes de la Región administrativa especial de Hong Kong ("Hong Kong") independientemente de su conflicto con las disposiciones legales; y las partes del presente acuerdo se someten a la jurisdicción exclusiva de los Tribunales de Hong Kong, salvo que la normativa aplicable establezca lo contrario. Si su acuerdo es con Aliexpress Russia Holding Pte LTD., el presente acuerdo se regirá por las leyes de la federación rusa ("rusia"), exceptuando sus normas sobre conflicto de leyes, y las partes del presente acuerdo se someten a la jurisdicción exclusiva de los tribunales de rusia, salvo que la normativa aplicable establezca lo contrario (2019, párr. 8.7) [minúsculas agregadas].

En el caso de los consumidores peruanos que contraten a través de la página web de Amazon[3], deben tener en cuenta la cláusula de resolución de controversias de los términos y condiciones establece lo siguiente:

> Ley Aplicable: Al usar cualquier Servicio de Amazon, usted acepta que las Leyes Federales de Arbitraje y las leyes del estado de Washington, independientemente de los principios de conflicto de leyes, regirán estas Condiciones de uso y cualquier disputa de cualquier clase que pudiera derivar entre usted y Amazon.
>
> Disputas: Cualquier disputa o reclamo relacionado, en cualquier sentido, con el uso de cualquier Servicio de Amazon, o con cualquier producto o servicio vendido o distribuido por Amazon o a través de Amazon.com se resolverá mediante arbitraje vinculante, en lugar de un juzgado, salvo que presente los reclamos ante un tribunal de demandas de menor cuantía si tales reclamos califican para ello. Las Leyes Federales de Arbitraje se aplicarán a este acuerdo (2021, párrs. 27 & 25).

Esta situación es especialmente preocupante, porque, aunque en el año 2015 el *e-commerce* transfronterizo representaba solo el 14% de las compras *online*, en el año 2019 aumentó a un 25% (Capece, 2019). Entonces, a mayor aumento del *cross border e-commerce*, aumenta el número de consumidores peruanos que se quedan desprotegidos por la tutela del tradicional Código de Protección y Defensa del Consumidor.

Esta desprotección se genera porque los términos y condiciones de las páginas web que cada vez más usan los peruanos para realizar sus transacciones *e-commerce* excluyen directamente la aplicación de cualquier tutela generada por autoridades gubernamentales del país de origen de consumidor.

D. La desconfianza del consumidor frente al *e-commerce*

Existen diversos factores que influyen en la confianza con el consumidor, de los cuales, los tres principales son los siguientes: (i) factor cultural;

[2] Para mayor información, véase el Acuerdo de Suscripción Gratuita de Alibaba.com (https://rule.alibaba.com/rule/detail/4293.htm).

[3] Para mayor información, véanse las Condiciones de Uso de Amazon (https://www.amazon.com/-/es/gp/help/customer/display.html?nodeId=GLSBYFE9MGKKQXXM).

(ii) factor generacional; y, (iii) factor de la confianza en sentido estricto. Los primeros dos de ellos son factores más estáticos y, por ende, más complejos de mitigar; sin embargo, el factor de la confianza basada en la inseguridad del consumidor en las transacciones electrónicas, es decir, el factor de la confianza en sentido estricto, puede mitigarse mediante mecanismos *ex ante* o *ex post*. De hecho, será para este último factor para el cual se propondrán soluciones desde la tecnología.

Respecto al factor cultural, la cultura nacional influye directamente en la confianza del individuo (Hallikainen & Laukkanen, 2018). Ello se debe a que una misma cultura suele compartir creencias que condicionan a sus integrantes a desarrollarse y responder a ciertas circunstancias de manera similar. De este modo, factores de la teoría de Hofstede como son el individualismo, la distancia del poder, masculinidad, el colectivismo o la orientación a largo plazo, son factores que, a su vez, influyen en la confianza de los individuos en la sociedad (Hallikainen & Laukkanen, 2018).

Por otro lado, el factor generacional es un factor importante en la desconfianza frente al *e-commerce*. Es innegable que existe una progresión hacia la apertura frente a la tecnología según la generación a la que uno pertenece. Así, a la generación 'X' le parecerá menos familiar usar una plataforma o un aparato electrónico que a una persona perteneciente a la generación 'Y' o más conocida como *millennials*. Las personas pertenecientes a la generación 'X', incorporan a la tecnología en casi todos los aspectos de su vida con completa normalidad (Calvo-Porral & Pesqueira-Sanchez, 2019).

Finalmente, el factor de la confianza en sentido estricto, el más dinámico, crea un cierto recelo de parte del consumidor peruano, debido al incumplimiento generalizado de las prestaciones en estas relaciones de consumo (cumplimiento parcial, tardío o defectuoso). Lo que acaba generando inseguridad en el consumidor en sus transacciones electrónicas.

Si bien en el Perú han incrementado de manera significativa las compras por internet estos últimos años, debido a los problemas mencionados en la sección anterior, nuestro país presenta el mayor índice de desconfianza a comparación de México, Colombia, Brasil, Chile y Argentina (Capece, 2019).

La desconfianza es una de las barreras que perjudica la relación entre consumidor y proveedor. En definitiva, la falta de confianza del consumidor frente al *e-commerce* no solo limita a este a medios presenciales de consumo, sino que también, en el mundo contemporáneo en el que muchos negocios operan de manera electrónica, significa un freno en la economía muy importante. En esa línea, si se quiere incrementar el consumo, y el tráfico de bienes y servicios, resulta imprescindible mitigar la desconfianza del consumidor electrónico. La interrogante que nos planteamos a lo largo de este trabajo es el mecanismo de regulación más eficiente para garantizar esta confianza: la regulación estatal o la autorregulación.

E. Propuesta de ley de *e-commerce* en el Perú

Ante los problemas presentados, en octubre de 2020, la presidenta del Consejo Directivo del Indecopi comunicó ante diversos medios que se encontraba preparando una propuesta normativa para regular las transacciones por *e-commerce* y fortalecer la protección de los consumidores.

De acuerdo a las autoridades gubernamentales, la propuesta normativa surge como consecuencia de reconocer que la contratación a través de páginas web o redes sociales no le permite al consumidor tener un contacto directo con la prestación o servicio que adquiere, por lo que existe una sujeción del consumidor a la información que le otorgue el proveedor, lo que genera una mayor asimetría informativa.

Frente a esta iniciativa, la Asociación de Emprendedores Digitales (en adelante, ASEDI) indicó estar a favor de "impulsar medidas que promuevan la confianza y bienestar de los consumidores" (Gestión, 2020). Sin embargo, ASEDI mostró reservas a algunas de las ideas planteadas por el Indecopi. Por ejemplo, ante la propuesta de que los consumidores tengan la posibilidad de arrepentirse de la compra realizada, ASEDI indico lo siguiente: "Consideramos que es válido este derecho del consumidor, pero debería regularse por el mercado como sucede en cualquier parte del mundo" (Gestión, 2020).

En abril de 2021, el Indecopi publicó el documento de trabajo titulado Propuestas para la protección del consumidor en el comercio electrónico y la seguridad de productos, como primera iniciativa oficial de regulación del comercio electrónico en el Perú.

Dicho esto, no hay duda de que ante el crecimiento del *e-commerce* se hacen necesarias nuevas formas de fomentar la confianza en los consumidores garantizando sus derechos e incentivando el consumo electrónico. La pregunta sería: ¿la ley de *e-commerce* resolverá los nuevos problemas presentados al consumidor electrónico peruano?

III. ANÁLISIS DEL IMPACTO REGULATORIO DE UNA NORMA DE PROTECCIÓN AL CONSUMIDOR ELECTRÓNICO

Cuando un ordenamiento jurídico detecta un problema que afecta a un sector específico de ciudadanos, debe reunir y analizar evidencia para dar soporte a las futuras políticas públicas generadas en dicho contexto. En ese proceso, llamado análisis de impacto regulatorio (en adelante, AIR), se verifica la existencia del problema, sus posibles causas, evaluar si la acción del ordenamiento jurídico es necesaria, así como analizar las ventajas y desventajas de posibles soluciones (Quintana Sánchez, 2011, p. 16).

Dicho análisis permite determinar los objetivos regulatorios buscados e identificar todas las alternativas que son capaces de alcanzarlos, las cuales deben evaluarse, utilizando el mismo método, para informar a los tomadores de decisiones sobre la efectividad y eficiencia de las diferentes opciones normativas (o no) y permitir que se elija la opción más efectiva y eficiente, con el menor costo posible y los menores efectos negativos indeseados (Organización para la Cooperación y el Desarrollo Económicos [OCDE], 2008).

Esto se lleva a cabo como un esfuerzo del Estado por reducir los costos impuestos a las empresas privadas a través de las obligaciones exigidas por un marco legal:

> [el AIR] nace como una muestra tangible del compromiso de los gobiernos de aliviar a la iniciativa privada de cargas legales ante la percepción generalizada de que la industria se encontraba sobre regulada (Quintana Sánchez, 2011, p. 16).

Sin embargo, la finalidad del AIR no es constituirse como un mecanismo de simplificación administrativa, sino más bien funcionar como herramienta clave para mejorar la calidad de las normas legales y en particular de la regulación. Su finalidad destacada es dar un enfoque más racional para la elaboración de normas legales, a través de una metodología que se ha venido estandarizando y aplicando en distintas realidades y países (Quintana Sánchez, 2011, p. 19).

Esta metodología incluye varias etapas de análisis recomendadas, las mismas que se explican a continuación.

A. El problema

Como se detalló en los numerales precedentes, el aumento del *e-commerce* como forma de captar consumidores y realizar diversas transacciones utilizando herramientas digitales, ha generado nuevas situaciones de conflicto que la normativa peruana vigente sobre protección al consumidor no ha llegado a resolver del todo.

La autoridad gubernamental encargada del cumplimiento de la normativa de protección al consumidor, Indecopi, ha manifestado una posición de preocupación ante el incremento de controversias en las transacciones *e-commerce* y ha propuesto como solución la creación de una 'Ley de *e-commerce*'.

Las interrogantes que nos dejan son, principalmente: (i) si Indecopi ha realizado un análisis de impacto regulatorio para poder verificar alguna alternativa a la creación de regulación que permita alcanzar los mismos objetivos, y (ii) si es que la creación de la norma solucionará los problemas respecto de las prestaciones en las relaciones de consumo y respecto de la ley y jurisdicción aplicables a las mismas.

En ese sentido, a partir de la descripción de los principales problemas que ha generado el *e-commerce* (apartado II.B), se delimitará los objetivos que debe cumplir cualquier regulación propuesta, y finalmente, se analizará si existen alternativa(s) más efectiva(s) y eficiente(s) a la regulación.

B. Objetivos que debería cumplir la normativa sobre *e-commerce*

A fin de decidir el contenido de una iniciativa normativa, se requiere definir qué aspectos del problema se van a solucionar con la intervención regulatoria, en tanto que "pueden existir otros aspectos del mismo problema que pueden solucionarse sin necesidad de más intervención" (Quintana Sánchez, 2011, p. 17).

Según el problema identificado, los objetivos pueden ser de varios niveles, desde generales hasta muy particulares para ir dando solución al problema por partes. En ese sentido, la intervención pública en el comercio electrónico debe tener como principales objetivos: (i) mecanismos que efectivicen el cumplimiento de las prestaciones en integridad e identidad, así como una adecuada y célere tutela de los consumidores; y (ii) posibilidad de resolver conflictos derivados del *e-commerce* transfronterizo sobre la ley y jurisdicción aplicables a dichas relaciones jurídicas.

C. ¿Cuáles son las diversas opciones para conseguir los objetivos planteados?

La tercera etapa del AIR "consiste en escoger entre las distintas alternativas que se tienen para

dar solución al problema, es decir, identificar las opciones regulatorias (o no) que existen y permitirían alcanzar el o los objetivos trazados" (Quintana Sánchez, 2011, p. 17).

La autoridad gubernamental plantea como solución regulatoria la creación de una ley para el *e-commerce*, pero existen alternativas a la regulación que podrían solucionar los problemas planteados. Las que analizaremos en el presente artículo excluyen la creación de normativa y pretenden utilizar a los agentes del mercado o la cooperación internacional para tutelar los derechos de los consumidores: (i) la cooperación internacional para resolver conflictos que implican empresas transnacionales; y (ii) los *smart contracts* como mecanismos automáticos de solución de problemas de los consumidores.

1. Propuesta de regulación: creación de ley de *e-commerce*

Esta no es la primera vez que en nuestro país se habla de un proyecto de ley *e-commerce*. En el año 2000 surgió el Proyecto de Promoción del Comercio Electrónico, el cual pretendía ser "una ley marco con la finalidad de otorgar seguridad jurídica a todas las transacciones vía internet desde la perspectiva de una ley uniforme propuesta por la CNUDMI (Comisión de las Naciones Unidas para el Derecho del Mercado Internacional)" (Postigo & Dupuy, 2000, p. 324).

Dicho proyecto siguió la tendencia de mediados de los años noventa e inicios de los 2000, en donde varios países implementaron legislación interna para regular las transacciones electrónicas, servicios electrónicos y *e-commerce*.

Por ejemplo, en el año 2002, España promulgó la Ley de Servicios de la Sociedad de la Información y Comercio Electrónica, mediante la cual se establecen nuevos derechos para los consumidores, como el derecho a recibir un presupuesto previo a la transacción electrónica. No obstante, aparte de regular los derechos de los consumidores, también contiene regulación sobre datos personales, publicidad no autorizada e información indispensable para los términos y condiciones.

En ese sentido, el fin de la legislación española es, principalmente, condensar en una sola regulación los riesgos que pueden tener los consumidores en la potencial y propia relación de consumo.

Con respecto a Latinoamérica, Ecuador sigue la tendencia española con la Ley 2002-67, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, la cual regula los mensajes de datos, la firma electrónica, la contratación electrónica y telemática, la prestación de servicios electrónicos y los derechos de los usuarios de las mismas.

Nuevamente, el fin de la emisión de la norma es, principalmente, condensar la regulación que concierne a una relación jurídica electrónica, especialmente las de consumo.

Ahora bien, de acuerdo con lo establecido por la presidenta del Consejo Directivo de Indecopi, la regulación sobre *e-commerce* no tendrá como finalidad condensar regulación sobre contratación electrónica, sino que pretenderá una mayor eficiencia en los derechos de los consumidores e incluir derechos como el arrepentimiento de la contratación.

En la propuesta publicada en abril del presente año, se proponen diversas figuras como, por ejemplo, el derecho de arrepentimiento. Al respecto, se señala que se plantea establecer la facultad del consumidor de dejar sin efecto, unilateralmente y sin necesidad de justificación, la compra o contratación de un producto o servicio en un plazo máximo de quince días.

Respecto al cumplimiento de los objetivos, consideramos que una regulación sobre *e-commerce* en nuestro país tiene dos principales limitaciones.

En primer lugar, si es que la regulación sanciona el incumplimiento de las prestaciones, o el establecimiento de cláusulas abusivas electrónicas, la tutela de los derechos de los consumidores demoraría un promedio de tres años. Toda tutela por parte de la autoridad gubernamental tendría que seguir con el procedimiento administrativo que no brinda efectividad en el cumplimiento de los derechos de los consumidores.

En segundo lugar, una regulación cuyo ámbito de aplicación son las transacciones de *e-commerce* realizadas en territorio peruano, no tendrían la posibilidad de resolver conflictos derivados del *e-commerce* transfronterizo, cuyas páginas web tienden a excluir la legislación del país de origen del consumidor.

En conclusión, una ley de *e-commerce* seguiría conservando el mismo problema en el retraso de la tutela en los derechos de los consumidores, en la medida que los conflictos que se generen seguirán siendo resueltos por el mismo procedimiento actual y por el Indecopi. Asimismo, la ley no podría tutelar los derechos de los consumidores que renuncian a la ley y jurisdicción nacional, cláusula que se establece cada vez con mayor frecuencia en el *e-commerce* transfronterizo.

2. Primera alternativa a la regulación: cooperación internacional para resolver los problemas del *e-commerce*

En efecto, el mundo web no conoce de fronteras y, en muchos casos, las plataformas electrónicas traspasan las barreras nacionales. El mayor poder de negociación que tienen estas empresas transnacionales frente al consumidor o al órgano regulador de un país latinoamericano en particular, facilita la creación de cláusulas dentro de los contratos con el consumidor que pueden dejar fácilmente sin uso cualquier tutela desde el derecho peruano.

Colocando un ejemplo, Amazon o Airbnb tienen un mercado asegurado de consumidores (demanda inelástica) en Latinoamérica, que estarían dispuestos a aceptar los términos y condiciones que los obligan a resolver sus controversias bajo normativa de Estados Unidos, escenario que se vuelve excesivamente oneroso para el consumidor y, como consecuencia, ve desprotegidos sus derechos.

Dicho escenario ha generado, entonces, que diversos órganos gubernamentales que protegen los derechos de los consumidores en diversos países de Latinoamérica se unan frente a los reclamos de consumo hacia las empresas transnacionales. De esta forma, cada país incrementa su poder de negociación frente a la trasnacional.

De este modo, al ser un bloque regional de países, estos adquieren mayor poder de negociación con las empresas de *e-commerce* llegando a un mutuo acuerdo que garantice los derechos de los consumidores de dichas plataformas a nivel regional. Siguiendo nuestro ejemplo, Amazon tendrá un incentivo mayor de atender las cuestiones de los países en conjunto, puesto que querrá conservar su presencia en el mercado latinoamericano en su conjunto.

Como ejemplo tangible, se tiene el caso de Airbnb y la Unión Europea que, mediante la Airbnb Enforcement Action se lograron establecer una serie de acuerdos que protegían de mejor manera al consumidor: entre otros, (i) la obligación de proveer el precio al cliente; y (ii) la eliminación de la cláusula que prohibía la facultad del consumidor de demandar al anfitrión en caso de daño personal u otros daños no contemplados (European Commission, 2019).

Sin perjuicio de lo mencionado, creemos que la cooperación internacional, por sí sola, resulta insuficiente para generar una tutela de los derechos de los consumidores, ya que ello depende de un incumplimiento sistemático que llame la atención de las autoridades gubernamentales, así como de la voluntad de los demás países a fin de dirigirse a las empresas transnacionales, lo que involucra elementos políticos subjetivos.

Del mismo modo, atendiendo a la realidad Latinoamericana inmersa en corrupción, se debe encontrar una solución que no dependa de las autoridades gubernamentales, sino que se garanticen estos derechos de manera casi automática y que, sobre todo, el territorio no sea un impedimento para el cumplimiento de cualquier derecho de los consumidores.

3. Segunda alternativa a la regulación: uso de *smart contracts* como tutela a los consumidores

A fin de establecer si mecanismos como los *smarts contracts* cumplen con los objetivos de efectivizar el cumplimiento de las prestaciones en integridad e identidad, así como una adecuada tutela de los consumidores; y la posibilidad de resolver conflictos derivados *e-commerce* transfronterizo, es necesario analizar en qué consisten estas herramientas y porqué generan una tutela automática.

IV. *SMART CONTRACTS* Y SU INCENTIVO POR EL ESTADO COMO MEJOR ALTERNATIVA A LOS PROBLEMAS DEL *E-COMMERCE*

Desde nuestra perspectiva, las nuevas tecnologías basadas en el *blockchain*, como los *smart contracts*, pueden fomentar la protección al consumidor en diversos aspectos de manera eficiente. Asimismo, se configuran como una potencial solución a la falta de confianza en el mercado y de conflictos derivados del *e-commerce* transfronterizo.

A. Conceptos básicos

1. *Blockchain*

El *blockchain*, también conocido como cadena de bloques, es una tecnología de registro distribuido o, por sus siglas en inglés, DLT (*distributed ledger technology*) la cual permite que múltiples agentes realicen transacciones sin la necesidad de ningún intermediario.

Debido a que la tecnología de registro distribuido o DLT es un *software* que organiza una base de datos a través de mantener múltiples copias idénticas de un registro digital de manera distribuida, verificada y actualizada, un *blockchain* sería un tipo de tecnología que implica un registro distribuido de datos en bloques, los cuales se encuentran encadenados cronológicamente a través de un cifrado *hash*, el cual es confirmado mediante el

consenso de los participantes de la red 'mineros' (Smart Contracts Alliance, 2018).

2. *Smart contracts*

Los *smart contracts* pueden ser definidos, sin perjuicio de las discusiones doctrinarias respecto a su naturaleza, como un protocolo computarizado que ejecuta los términos de un contrato previamente establecidos en un código, el cual se ejecuta sin la necesidad de un intermediario ante la ocurrencia de una condición establecida (De Caria, 2019).

La característica principal de esta herramienta es la autoejecución, pues utilizan tecnología *blockchain* para establecer un *enforcement* digital, a fin de verificar la ejecución del contrato (Allam, 2018).

En el contexto del *blockchain*, los *smart contracts* se encuentran encriptados dentro de la cadena de registro distribuido, de donde obtienen un código único (Christidis & Devetsikiotis, 2016). Se inicia la etapa de ejecución cuando se 'añade' la transacción al *smart contract*, como un envase único cuyo contenido es la operación económica.

Desde ese momento, la transacción se ejecuta de manera independiente y automática, tal y como se ha descrito, en cada nodo de la red, respetando los términos establecidos en la transacción.

B. *Smart contracts* como solución al problema de la confianza

Como señalan el Dr. Cristian Thorun, fundador y director ejecutivo de ConPolicy (Institute for Consumer Policy de Berlín, Alemania) y la Dra. Jana Diels, miembro de la misma institución, la tecnología *blockchain* puede fortalecer la protección al consumidor en relación a la seguridad, autenticidad y calidad de los productos (2020). En ese sentido, una persona con residencia en Perú podría realizar la compra de un producto extranjero sin temor a ser estafado, pues tendría acceso permanente al registro de la cadena de suministro.

Por las características del *blockchain*, el consumidor sería capaz de rastrear su producto de forma detallada con mayor precisión y seguridad que los actuales servicios que pueden ofrecerse. Esto posee especial relevancia, pues, como hemos visto, la normativa del Código de Protección y Defensa del Consumidor solo posee como ámbito de aplicación y tutela a las páginas web con dominio peruano.

Más aún, utilizando el *blockchain* pueden verificarse los orígenes del producto adquirido y el consumidor puede adquirir mayor información sobre la cadena de producción detrás del mismo. Por ejemplo, Faizod ha incrustado en sus textiles un chip con tecnología Radio Frequency Identification (en adelante, RFID) –chips de identificación por radiofrecuencia– que almacena los distintos pasos del proceso de producción y logística con soporte de un *blockchain*. De esta forma, los consumidores simplemente pueden escanear este chip para conocer el origen de la tela, el impacto ambiental de la producción, entre otros (Thorun & Diels, 2020).

Aunque, en apariencia, la idea de colocar chips en la ropa pueda sonar extremadamente lejana, grandes marcas internacionales como Zara han incursionado en estas iniciativas con resultados exitosos. Desde 2014, Inditex, la matriz de Zara, ha implementado este tipo de chips con tecnología RFID en sus prendas para controlar el *stock* de sus tiendas. Como indicó entonces la empresa:

> [e]ste innovador sistema tecnológico permite la identificación única de cada prenda a través de ondas de radiofrecuencia que se graba en un chip dentro de la alarma, lo que proporciona una mayor agilidad en la distribución y una mayor precisión en la gestión de las prendas en las tiendas (Rodríguez, 2020).

Además, ahora, Inditex utiliza esta herramienta para tener "una red comercial integrada, a nivel físico y online" (Rodríguez, 2020).

Este tipo de herramienta también ha tenido bastante acogida con marcas de lujo como Ferragamo (El Comercio, 2016) y Moncler (Valdés, 2016), las cuales han implementado los chips con tecnología RFID en sus productos para evitar las falsificaciones. Así, los clientes pueden identificar la autenticidad de sus compras escaneando estos chips con sus celulares.

Por otro lado, nuevas tecnologías con base en el *blockchain* también permiten una mejor fiscalización de la calidad del producto. Por ejemplo, en el sector farmacéutico existen ciertos medicamentos, como las vacunas, que deben ser transportados bajo ciertos estándares específicos, como la temperatura o nivel de humedad. Ante esto, el servicio postal nacional de Suiza y la empresa Modum, con el apoyo de la empresa multinacional SAP (Systems, Applications, and Products in Data Processing), diseñaron cajas de contención que pueden mantener la temperatura requerida para transportar diversas clases de medicinas (Rohr, 2019).

Para poder monitorear las condiciones del producto utilizan sensores Internet of Things (IoT) y almacenan la información en el *blockchain* Ethereum. De esta forma, pueden asegurarse de que la

temperatura sea la adecuada en todo el lapso del transporte. Más aún, la data almacenada puede ser analizada por un *smart contract* que exige para la ejecución de la transacción el cumplimiento de diversos estándares de calidad. Así, el *smart contract* solo ejecuta el pago y emite el comprobante si el transporte del medicamento ha sido idóneo (Rohr, 2019).

Entonces, podemos apreciar que esta clase de nuevas tecnologías no solo benefician ampliamente a los consumidores, quienes pueden acceder de forma sencilla a mayor información sobre sus productos; sino que las empresas proveedoras pueden aprovechar estas herramientas según sus necesidades específicas para maximizar sus ganancias y generar confianza en el mercado. En esta línea, compartimos lo expuesto por Thorun y Diels (2020) cuando mencionan que, al hacer posibles los *smart contracts*, la tecnología *blockchain* tiene el potencial de llevar la aplicación de los derechos individuales de los consumidores al siguiente nivel. Es decir, puede facilitar enormemente que los consumidores hagan valer por sí mismos sus derechos.

Ahora, revisaremos el caso de Fizzy, aplicativo desarrollado por la empresa de seguros AXA que permitía a sus clientes acceder a la devolución automática de su pasaje ante incumplimientos de las aerolíneas en el itinerario de los vuelos. Después de explicar las grandes ventajas que implicaba este servicio y reflexionar en torno a las razones por las cuales fue sacado del mercado, analizaremos la Resolución 2107-2020/SPC-INDECOPI. En específico, nos centraremos en distinguir cómo mediante el uso de *smart contracts* se podría haber tutelado de forma más eficiente los derechos de los, aproximadamente, más de 39 000 consumidores afectados, así como los posibles beneficios que podría representar para las empresas involucradas adoptar este tipo de tecnologías.

C. Comparación de soluciones desde la norma y desde los *smart contracts* en el sector aerocomercial

1. Caso Fizzy

En 2017, la multinacional de seguros AXA lanzó el aplicativo Fizzy con el objetivo de ofrecer a sus clientes la posibilidad de obtener la devolución de su dinero ante el retraso de sus vuelos de forma sencilla y automática. De esta forma, el cliente podía ingresar a la plataforma web de Fizzy la información de su vuelo y comprar algunas de las opciones de cobertura disponibles (el pago se podía realizar mediante una transacción de tarjeta de crédito) (Hill, 2019).

Luego del pago, el seguro era creado y registrado en el *blockchain* Ethereum con apoyo de un *smart contract*. El *smart contract* era capaz de obtener la información sobre el estado del vuelo mediante el acceso a datos de base públicos vía un oráculo. Así, si es que el vuelo se retrasaba por más de dos horas o era cancelado, automáticamente y sin necesidad de iniciar ningún tedioso procedimiento de reclamo, se reembolsaba a la cuenta bancaria del cliente el total del pasaje adquirido (Hill, 2019).

Los beneficios que ofrecía Fizzy son claros tanto para los consumidores como para las empresas. Por un lado, los usuarios de esta plataforma tenían asegurada la devolución de su dinero en un plazo máximo de siete días, sin necesidad de iniciar ningún procedimiento de reclamo. Por otro lado, las aerolíneas se ahorraban el tener que corroborar de forma interna la posible afectación de los cientos clientes que se produce cuando hay un vuelo retrasado.

A pesar de que solo en su primer año en el mercado Fizzy vendió, aproximadamente, 11 000 *smart contracts* y se posicionó como uno de los principales usuarios de la *blockchain Ethereum* (Hoffmann, 2020); en 2019, fue cerrado por AXA debido a que la plataforma no alcanzó los objetivos financieros planteados y, según la empresa, no era rentable. ¿Qué sucedió? De acuerdo al Dr. Hoffman, director de Swiss FinTech Innovation Lab y profesor de la Universidad de Zurich, al no asociarse a empresas del sector como agencias de viaje, aeropuertos o aplicaciones de viaje, AXA no consiguió ampliar sus canales de venta y público objetivo (2020).

Asimismo, un *marketing* insuficiente pudo haber contribuido a que Fizzy no alcanzara mayor popularidad. Se debe recordar que Fizzy ha sido uno de los primeros seguros basados en el *blockchain* que se han ofrecido en el mercado a nivel mundial. Así, los potenciales consumidores no eran conscientes de las ventajas de este novedoso tipo de productos (Hoffmann, 2020).

Por otro lado, en opinión de Hoffman, la estructura de pago no era la más óptima posible, ya que el depósito de reembolso podía demorar hasta un plazo de siete días en realizarse, lo cual es relativamente lento para un *smart contract* (2020). Sin perjuicio de lo mencionado, cabe resaltar que la plataforma de Fizzy funcionó de forma exitosa por dos años y logró atender a miles de clientes. Así, AXA ha declarado que seguirá incursionando en esta clase de innovaciones tecnológicas y que ha ganado experiencia valiosa en la construcción, financiamiento y desenvolvimiento de *smart contracts* por la red de Ethereum (Hill, 2019).

2. Caso Indecopi

En noviembre de 2020, la Sala confirmó la responsabilidad administrativa de las aerolíneas Latam Airlines Perú S.A. (en adelante, Latam Perú) y Latam Airlines Group S.A. Sucursal Perú (en adelante, Latam) por la demora, reprogramación y cancelación de 276 vuelos, nacionales e internacionales, durante 2017. También, se debe resaltar que, según cálculos de la Comisión de Protección al Consumidor de Lima Norte, el número de pasajeros afectados habría sido de 2568 en el caso de Latam y 36 798 en el caso de Latam Perú (Indecopi, 2020b).

De esta forma, ambas empresas atentaron contra el deber de idoneidad del servicio recogido en el artículo 19 del Código de Protección y Defensa del Consumidor. Así, aunque tanto Latam Perú como Latam aludían a que estos incumplimientos en el itinerario de los vuelos se debían a casos de fuerza mayor, no pudieron acreditarlo.

Asimismo, la Sala confirmó como medida correctiva la devolución del costo del pasaje a todos los consumidores que no hayan gozado de la prestación del servicio. Es decir, los usuarios que adquirieron un boleto, registraron su embarque y no viajaron debido al incumplimiento de Latam o Latam Perú, según corresponda. Además, el pago por parte de las aerolíneas debe realizarse sin requerimiento previo de los clientes. Ahora, cabe resaltar que, anteriormente, ambas empresas habían declarado en su apelación lo siguiente:

> la medida correctiva ordenada no cumplía con la finalidad de revertir los efectos de la conducta infractora, en la medida que al haberse cancelado y/o retrasado los vuelos, no mantenían registro de algún listado de pasajeros para realizar el cruce de información, dado que los pasajeros fueron reubicados en los vuelos de protección, no existiendo a la fecha un registro de aquellos pasajeros que realizaron el check-in y luego decidieron no viajar; sin perjuicio de lo señalado, en caso existieran consumidores afectados, podían solicitar directamente a través de su página web la devolución íntegra del valor del boleto aéreo adquirido (Resolución 2107-2020/SPC, 2020, párr. 9. vi).

Al respecto, la Sala indicó que ambas empresas se encuentran obligadas a tener el registro de pasajeros por cada vuelo, "e incluso si los pasajeros fueron ubicados en vuelos ajenos a su empresa, podía gestionar tales pruebas con las compañías aéreas correspondientes" (Resolución 2107-2020/SPC, 2020, párr. 125). En esta línea, la Sala señaló que las administradas poseen treinta días hábiles desde la notificación de la resolución para cumplir la medida correctiva (o sea, hasta el 11 de enero de 2021). También, la Sala ordenó que deberán acreditar ante la Comisión el cumplimiento de la medida en el lapso de cinco días hábiles después del vencimiento del plazo para realizar la devolución del pasaje a los afectados (Resolución 2107-2020/SPC, 2020).

Ahora bien, ¿cómo los *smart contracts* y la tecnología *blockchain* podrían haber tutelado de manera más eficiente los derechos de los consumidores en el presente caso? Basándonos de la experiencia de Fizzy, los usuarios que hubieran adquirido esta clase de seguros podrían haber recibido la devolución de su pasaje de forma automática en un máximo siete días y sin necesidad de iniciar ningún tipo de reclamo ante las aerolíneas.

Cabe resaltar que el incumplimiento de los itinerarios por parte de Latam y Latam Perú ocurrió entre febrero y agosto de 2017. Más de tres años después, recién se ha emitido una resolución que obliga a las empresas a realizar la reposición correspondiente.

Además, se debe tener en consideración que desde que empezó la pandemia en Perú hasta marzo de este año, Indecopi ha registrado 422 sanciones contra diversas empresas del transporte aéreo de pasajeros. Entre las conductas más reportadas ante Indecopi se encuentran la falta de reembolso del dinero, la falta de atención de reclamos o solicitudes, los cobros indebidos, y la falta de atención en los canales de comunicación de la empresa (RPP, 2021b).

La implementación de *smart contracts* para la devolución del dinero traería amplios beneficios para todos los actores involucrados. Por el lado de las empresas, las aerolíneas se podrían ahorrar todo el proceso logístico que implica el tener que atender las quejas de miles de usuarios a nivel nacional. De esta forma, evitan potenciales conflictos y ofrecen una herramienta tecnológica que otorga confianza a sus clientes. Por el lado de los consumidores, estos ven tutelados de una forma más eficiente sus derechos.

D. Incentivos para la aplicación de nuevas tecnologías como refuerzo de los derechos de los consumidores

Como hemos podido apreciar a lo largo del presente trabajo, el uso de herramientas como *smart contracts* y *blockchain* permiten tutelar de forma más eficiente los derechos de los consumidores. Asimismo, al aplicar la tecnología *blockchain* para tutelar a los consumidores, estos incrementarán su confianza frente a la empresa lo cual genera mayores ventas e ingresos para estas. En ese sentido, las demás empresas también tendrán un incentivo de

aplicar la misma tecnología en aras de incrementar sus ventas y, al mismo tiempo, tutelar de manera más eficiente los derechos de los consumidores.

Ahora bien, ¿cuál es el rol que debe tener el Estado ante estas herramientas? Desde nuestra perspectiva, es esencial que los organismos gubernamentales generen incentivos para la promoción del uso de nuevas tecnologías por parte de las empresas. De este modo, además de tener incentivos internos de parte del propio mercado para incrementar la confianza de los consumidores, es necesario que el Estado brinde beneficios de distinta índole –por ejemplo, tributarios– a las empresas que adopten estas tecnologías.

En efecto, en un reciente estudio del Parlamento Europeo se ha recomendado implementar la inteligencia artificial para garantizar los derechos de los consumidores de manera automática sin tener que emitir un reclamo que, como bien se sabe, puede demorar hasta meses sin obtener respuesta (Schulte-Nölke *et al.*, 2020). Entonces, se puede deducir que la Unión Europea promueve, como políticas para los Estados, que se emplee la tecnología para asegurar los derechos de los consumidores y, de esa forma, se promueva, de manera eficiente, ese nicho de la economía.

V. PERSPECTIVA INTERNACIONAL SOBRE LA APLICACIÓN DE HERRAMIENTAS *BLOCKCHAIN* PARA LA SOLUCIÓN DE PROBLEMAS DE LOS CONSUMIDORES

En los últimos años, se han pronunciado distintos organismos internacionales para emitir ciertos parámetros de políticas a emplear para el *e-commerce* en aras de garantizar los derechos de los consumidores.

En ese sentido, hemos recogido las principales recomendaciones de la Organización para la Cooperación y el Desarrollo Económicos, como referente latinoamericano por su informe orientado a América Latina, y de la Unión Europea, como referente europeo que tiene como principales objetivos orientar a los países a otorgar al consumidor una mayor protección dentro del *e-commerce* de tal manera que se promueva, de una manera eficiente, este sector de la economía. Del mismo modo, se expondrá como ejemplo legislación comparada e iniciativas del sector privado de países latinoamericanos y de Europa en torno al *e-commerce*.

A. Organización para la Cooperación y el Desarrollo Económicos

Por un lado, la Organización para la Cooperación y el Desarrollo Económicos publicó un informe en el cual trazó políticas para Latinoamérica y el Caribe titulado Políticas de banda ancha para América Latina y el Caribe: Un manual para la economía digital (2016).

En primer lugar, se plantean los tres objetivos principales que buscan mejorar la relación entre el operador y el usuario en el *e-commerce*: (i) una mayor información sobre los servicios ofrecidos; (ii) una mayor observación en el manejo de quejas en la etapa de ejecución de los contratos; y (iii) facilitar el cambio o terminación del contrato (OCDE & Banco Interamericano de Desarrollo [BID], 2016).

Asimismo, plantea tres objetivos clave para el *e-commerce* en esta región: la creación de un marco para las transacciones, reducción de barreras de acceso a este tipo de economía y promover la adopción de *e-commerce* en los países. En esa línea, este informe identifica que, para crear una regulación eficiente con relación al consumidor electrónico, se debe tomar como base la información obtenida directamente de las quejas de los consumidores, para identificar áreas problemáticas específicas (OCDE & BID, 2016).

También, recomiendan que, para que exista transparencia entre los consumidores y la plataforma de *e-commerce*, es necesario trabajar de la mano con una base de datos común nacional para recopilar información y trabajar en conjunto en medidas regionales efectivas sobre la base de principios comunes (OCDE & BID, 2016). Por lo que un manejo a través de la tecnología como se plantea en este trabajo, facilitaría la adopción de esta política.

En segundo lugar, se pretende asegurar el entendimiento de los consumidores de los términos y condiciones, recibos de pago, y otros aspectos contractuales. En esta línea, otra de las prioridades debe ser el manejo de quejas de los consumidores, ya que una vasta cantidad de quejas que llegan a la entidad gubernamental correspondiente no es buen indicio (OCDE & BID, 2016).

Un tangible desarrollo desde el sector privado en conjunto del sector público de incentivos para la protección al consumidor en Latinoamérica es la creación de cámaras de comercio electrónico. En estas cámaras se discuten políticas a adoptar por las empresas afiliadas, así como decisiones en conjunto. De hecho, Perú cuenta con la Cámara Peruana de Comercio Electrónico (Capece). No obstante, vale la pena exponer las situaciones de otros países que pueden servir de guía a la Capece para ayudar a implementar políticas internas como los *smart contracts*. En Argentina se tiene la Cámara Argentina de Comercio Electrónico (CACE) cuyo objetivo

es capacitar y desarrollar el comercio electrónico vía la asesoría jurídica y corporativa, contribuciones a las legislaciones, etc. (OCDE & BID, 2016).

Igualmente, en Brasil se creó, en el 2010, la Cámara Brasilera de Comercio Electrónico conformada por consumidores, compañías, autoridades gubernamentales y académicos. Asimismo, Colombia y Uruguay, al igual que estos países, crearon, respectivamente, la Cámara Colombiana de Comercio Electrónico y la Cámara de la Economía Digital de Uruguay que desempeñan actividades similares a las anteriores (OCDE & BID, 2016).

Por su parte, México creó, en el 2014, la Asociación de Ventas Online de México, cuyo objetivo principal es promover las ventas en línea generando confianza entre el consumidor y los negocios trabajando de lado con entidades bancarias y talleres de capacitación para las empresas (OCDE & BID, 2016).

Luego de haber presentado las recomendaciones para la adopción de políticas de la OCDE para América Latina y El Caribe, y de haber presentado mecanismos de cooperación entre empresas del sector privado como son las cámaras de comercio electrónico, vale la pena exponer los lineamientos y recomendaciones de la Unión Europea.

B. Unión Europea

El Parlamento Europeo, en mayo del 2020, emitió un estudio titulado Legal Framework for E-Commerce in the Internal Market con ánimos de, más tarde ese mismo año, emitir dos propuestas legislativas (*Acts*) oficiales que regulen la materia y que, por supuesto, se expondrán en este trabajo.

En esa línea, el mismo Parlamento Europeo recomienda implementar la inteligencia artificial para garantizar los derechos de los consumidores de manera automática sin tener que emitir un reclamo que, como bien se sabe, puede demorar hasta meses sin obtener respuesta (Schulte-Nölke *et al.*, 2020). En ese sentido, colocan como ejemplo la devolución automática del dinero por un boleto con la cancelación o demora del vuelo o tren (Schulte-Nölke *et al.*, 2020). Como hemos visto, esto se puede lograr a partir de *smart contracts*.

De esto se puede apreciar que la Unión Europea promueve, como política para los Estados, que se emplee la tecnología para asegurar los derechos de los consumidores y, de esa forma promover, de manera eficiente, ese nicho de la economía. En efecto, la Unión Europea creó una comisión, cuyo periodo de duración es desde el 2020 hasta el 2024, para crear y ejecutar la *Digital Services Act* y *Digital Markets Act*, cuyos proyectos a ser aprobados ya fueron publicados en diciembre del 2020. Estas propuestas de ley, además de regular ciertos ámbitos del *e-commerce*, pretenden, sobre todo, incentivar el uso de la tecnología en el ámbito social y económico.

La *Digital Markets Act*, tiene un ámbito de aplicación para plataformas de economía colaborativa, por lo que resulta de especial interés exponerla para así poder recopilar lineamientos útiles. Claro está que la regulación adoptada busca, mediante la protección del consumidor, un crecimiento económico que beneficie también a las empresas operadoras en el comercio electrónico; de hecho, la adopción de esta *Act* por parte de los Estados europeos estima que la economía virtual crezca en un aproximado de 6%. No obstante, consideramos que la legislación por sí misma no puede hacer crecer exponencialmente una economía, puesto que, como hemos visto, no garantiza de manera efectiva los derechos de los consumidores por lo que disminuye la confianza de este frente al *e-commerce*. Así, la legislación (si hubiere) tendría que ir orientada a incentivar alternativas tecnológicas propias del mercado, como hemos propuesto, como garantía de los derechos del consumidor.

En ese sentido, la propuesta adoptada por la *Digital Markets Act* pretende tener un constante y distribuido monitoreo de la ejecución de la misma. Ello se pretende lograr mediante la fiscalización de los algoritmos y bases de datos de las empresas. Cobra especial importancia la creación de la categoría *gatekeeper* que hace referencia a las empresas de *e-commerce* que tienen una importante presencia en el mercado y cuyas acciones puedan influir significativamente en el mismo (*Digital Markets Act*, 2020). Un ejemplo de *gatekeeper* en Perú sería Saga Falabella o SODIMAC, tiendas también de *e-commerce* que cuentan con un elevado número de consumidores diarios.

Ahora bien, la Comisión Europea establece un marco legal para propiciar el diálogo entre los *gatekeepers* y la propia comisión a miras de evaluar las conductas a implementar (*Digital Markets Act*, 2020). No obstante, queda claro que esta norma tendría un conflicto directo en nuestro ordenamiento, debido a que las conductas son sancionadas *ex post* y las empresas no deben solicitar permisos de actuación. Es por ello que, en nuestro ordenamiento, resulta más eficiente contar con mecanismos tecnológicos *ex ante*, propiciados por el mismo mercado. De este modo, se puede asegurar la garantía a los derechos de los consumidores. Por supuesto, ello se daría en el marco de un constante diálogo con entidades estatales –por ejemplo, como se mencionó, mediante las cámaras de

comercio– a fin de que el Estado brinde ciertos incentivos a las empresas para la adopción de estas tecnologías además de los propias del mercado.

En adición, otro dato importante que contempla esta *Act* es el trabajo junto a los *trusted flaggers* que son individuos u organizaciones expertas en la detección de contenido de índole ilegal que pueda estar contenida en alguna de las plataformas de *e-commerce*. Ello, pues, no resulta muy ajeno a la realidad del mercado peruano, por lo que las empresas afiliadas a la Capece cuentan con un servicio de verificación de un tercero sobre la seguridad de la empresa electrónica.

Así, la implementación de los *trusted flaggers* para un monitoreo a las plataformas de comercio electrónico de las empresas afiliadas, es un buen incentivo para que el consumidor incremente su confianza frente al comercio electrónico. Sin embargo, es importante reconocer que el mismo mercado debe hace más visibles estas políticas tecnológicas, que buscan garantizar la seguridad, a los mismos usuarios.

Por último, la Comisión Europea insiste en usar servicios de identificación mediante tecnología que permite la verificación de la identidad del usuario, precisamente para incentivar la confianza en el consumidor en las transacciones electrónicas. En efecto, es frecuente que el consumidor electrónico no quiera emplear su tarjeta de crédito para realizar compras electrónicas por temor a una clonación de tarjetas y que ellas puedan ser usadas para realizar compras desde otras plataformas *e-commerce* (Schulte-Nölke *et al.*, 2020). En ese sentido, los *smart contracts* se adecúan a este problema mediante su tecnología de seguridad de *blockchain*.

C. Recomendaciones desde lo planteado por los organismos internacionales y estudios de economía conductual

1. Desde los organismos internacionales

Después de haber expuesto algunas recomendaciones de organismos internacionales, así como ejemplos de políticas de otros países, vale la pena hacer una recomendación general propia para la adopción de acciones a la luz de lo expuesto anteriormente.

En primer lugar, resulta fundamental recalcar que los organismos internacionales y organizaciones regionales resaltan el uso de la tecnología para garantizar los derechos del consumidor.

Por otro lado, se deben adoptar políticas en base a la experiencia nacional. Por ello, se debe hacer una recopilación y revisión de las quejas emitidas por los consumidores, para lo cual puede trabajarse de la mano de entidades como el Indecopi. Precisamente, para lograr un mejor manejo de la administración de estas quejas para luego crear mejores políticas, resultaría sumamente beneficioso que se incentive la incorporación de la mayor cantidad de empresas a la actual Cámara de Comercio Electrónico (Capece). Asimismo, sería beneficioso que se cuente con reuniones periódicas previamente establecidas con autoridades del Indecopi, miembros de la Asociación Peruana de Consumidores y Usuarios (ASPEC), y personal técnico especializado en materia legal y tecnológica, de tal manera que se logre incentivar el intercambio de información, ideas, sugerencias y quejas para fomentar un acuerdo entre diversos actores en el comercio electrónico para la creación de mejores políticas internas del mercado con el uso de tecnologías.

Por otra parte, de forma similar a lo que la Unión Europea pretende lograr con los *trusted flaggers*, resultaría pertinente que la Capece trabaje de la mano de empresas certificadas en identificar malas prácticas de comercio electrónico, las cuales, mediante algoritmos e inteligencia artificial, pueden lograr controlar mejor que se cumpla con la normativa ya establecida de protección al consumidor en general. De este modo, el consumidor tendrá la garantía de que las empresas pertenecientes a la Capece cuentan con un monitoreo autorregulado autónomo que vigila las buenas prácticas de las empresas de comercio electrónico mediante el monitoreo de algoritmos para identificar de manera más eficiente cualquier irregularidad, además cualquier otra con la cual estas ya cuenten (certificación por un tercero).

Por último, la tecnología del *blockchain* y *smart contracts* ayuda a evitar la suplantación de identidad de una persona respecto a su tarjeta de crédito o débito. Está claro que las empresas de comercio electrónico deberán trabajar en conjunto con los bancos para lograr estos mecanismos de manera efectiva.

2. Recomendaciones desde los estudios de la economía conductual para el sector privado

Por su parte, resulta imperante, también, establecer recomendaciones al sector privado desde los estudios de la economía conductual. Estas recomendaciones apuntan a generar y fortalecer la confianza del consumidor para incrementar el crecimiento de la economía del comercio electrónico.

Antes que nada, es importante alinear las soluciones desde esta perspectiva con los factores de capacidad, integridad y benevolencia desarrollados

previamente. En esa línea, es importante reconocer los frenos que se le imponen al consumidor para comprar en internet. Los profesores Agag y El-Masry identifican tres de estos frenos: (i) la experiencia misma del consumidor y su inclinación a confiar; (ii) la reputación de la tienda; y (iii) la facilidad de uso percibida y la calidad de la página web (2016).

Del mismo modo, varios estudios traen a colación que los consumidores desconfían de las páginas de *e-commerce* por tener términos y condiciones demasiado extensos o, incluso, difíciles de acceder en las páginas web. Ante ello, es indispensable que los proveedores brinden una página web de fácil uso, así como también unos términos y condiciones de fácil acceso y amigables, como, por ejemplo, dividiéndolos en secciones.

Por otro lado, como afirma Aldana Ramos, "el consumidor que no confía en el sistema sencillamente preferirá el tradicional método de adquisición de bienes: el presencial, donde puede interactuar de manera directa con el producto [...]'' (2018, p. 17). Entonces, sugerimos que el proveedor coloque mayor detalle del producto, tanto gráfico –distintas fotos del producto– como escrito –por ejemplo, medidas–. En esa misma línea, resulta sumamente importante que productos que ya no se hallan en *stock* desaparezcan de la página a la que tiene acceso el consumidor, puesto que sucede muchas veces que el cliente se dirige a pagar y el producto resulta estar agotado. Ello, precisamente desincentiva al consumidor *online* de ir de compras *online*, ya que podría considerar que, simplemente, está perdiendo el tiempo.

Por último, Lee y Turban (2001) mantienen que dos hallazgos importantes para fortalecer la confianza del consumidor en el *e-commerce* son la seguridad a la hora de realizar transacciones y que la tienda cuente con una certificación de un tercero. En ese sentido, resulta fundamental utilizar inteligencia artificial para desarrollar algoritmos que permitan darle seguridad al consumidor a la hora de realizar sus transacciones. Por ello, sugerimos que la certificación de confianza *online* que ofrece de manera opcional la Capece sea obligatoria. Ello, no solo le brindará una seguridad superficial al consumidor para realizar una transacción, sino que esta certificación debe ir de la mano con una vigencia que traiga consigo una evaluación de los algoritmos y prácticas de la tienda que garanticen los derechos de protección al consumidor *online*.

Ante ello, sugerimos que el mismo mercado tome en cuenta estas recomendaciones para implementarlas en sus plataformas en conjunto con la adopción de la tecnología de *smart contracts* para mitigar el problema de la desconfianza del consumidor y, así, incrementar el consumo electrónico viéndose las mismas empresas directamente beneficiadas.

VI. VALORIZACIÓN Y COMPARACIÓN DE LAS ALTERNATIVAS FRENTE A LA REGULACIÓN DE UNA LEY DE *E-COMMERCE*

En el presente artículo se han explorado, principalmente, dos alternativas a la regulación de una ley de *e-commerce* en el Perú que podrían solucionar los problemas planteados. Al valorar y comparar la conveniencia de las distintas opciones identificadas previamente, podemos notar que la opción más conveniente es que los propios privados, como deudores de la relación de consumo referente a la entrega de la prestación, generen mecanismos de autoejecución de tutela para generar confianza en los consumidores, independientemente del territorio de estos y donde se realiza la entrega.

De acuerdo con Quintana Sánchez, es necesario:

> estimar los costos que implicaría adoptar cada una de dichas opciones y, estimar también los beneficios esperados con la intervención reguladora (es decir los beneficios de dar solución al problema inicialmente identificado). a fin de comparar luego los costos de las distintas opciones y, de ser el caso, tales costos con los beneficios que se espera obtener (2011, p. 18).

En esa línea, este trabajo apuesta por una regulación misma del mercado, a través de los *smart contracts* para brindar tutela al consumidor. Esto se debe a que consideramos que los *smart contracts* son mecanismos automáticos que garantizan los derechos de los consumidores, mientras que, de tratarse de una ley, no se garantiza una tutela inmediata de los derechos, sino más bien, una sanción que busque reparar la afectación a los derechos del consumidor. De hecho, como ya se abordó, esto puede tardar varios años. Por otro lado, un mecanismo de tutela como los *smart contracts* garantiza la protección al consumidor en transacciones internacionales y no limita su protección al ámbito peruano.

Con respecto a los costos de gobierno que incurriría una ley de *e-commerce*, el Estado, en reiteradas oportunidades, ha indicado que no busca comprometer los fondos del tesoro público y solo se trataría de una redistribución interna del presupuesto anual asignado al Indecopi. Sin embargo, consideramos que lo mencionado no sería coherente en los hechos, ya que, para temas de *e-commerce*, se tendría que invertir en una fiscalización ya no presencial (como la que siempre se ha rea-

lizado); sino una electrónica. Al ser una actividad nueva, es lógico asumir los altos costos de logística, seguridad e implementación que implicaría.

Asimismo, como hemos visto, la tutela de la ley de *e-commerce* a los consumidores se verá restringida a las transacciones celebradas en el ámbito nacional. Entonces, en el caso que un consumidor peruano realice una transacción en una página web que excluya la ley y jurisdicción nacional, la ley de *e-commerce* quedaría en desuso. Esto es especialmente preocupante si se tiene en cuenta que el *e-commerce* transfronterizo ha venido creciendo de forma sostenida en los últimos años y como se ha expuesto, algunas páginas utilizadas por peruanos, como Amazon, ya excluyen la ley peruana.

Por otro lado, al respecto del mecanismo de cooperación internacional, este es usado actualmente por el Indecopi para tratar de tutelar a los consumidores del *e-commerce* transfronterizo. Como hemos mencionado, esta medida genera incertidumbre porque no es coactiva y depende de las mismas relaciones políticas entre los países. Al no haber una tutela específica y coactiva, los consumidores se encuentran en una situación de incertidumbre.

Por todo lo anterior, creemos que el uso de los *smart contracts* por las empresas resulta más eficiente que proteger los derechos mediante una norma específica. Ello, además, tiene como consecuencia directa e inmediata, aumentar la confianza del consumidor frente al *e-commerce* y potenciar ese sector de la economía.

No obstante, es necesario que el Estado genere incentivos para las empresas –como, por ejemplo, incentivos tributarios– además, por supuesto, de los que el mismo mercado brinda, entre otros, la confianza. Queda claro que el empleo de estas tecnologías no solo resulta beneficioso para las empresas y el consumidor, sino que también para el mismo Estado al ahorrarse costos administrativos y legislativos bastante altos.

VII. CONCLUSIONES

A raíz de la pandemia, el mercado del *e-commerce* ha aumentado de forma exponencial en menos de un año, desbordando las expectativas de todos los actores involucrados. Ante esto, consideramos que el freno principal que impide el crecimiento de este sector es la desconfianza por parte del consumidor, la cual es provocada, principalmente, por dos situaciones: (i) problemas respecto a la prestación en sí misma, y (ii) problemas respecto a ley y jurisdicción aplicable a la relación de consumo.

A fin de poder resolver dichos retos, es necesario contar una herramienta que cumpla con efectivizar el cumplimiento de las prestaciones en integridad e identidad, así como una adecuada tutela de los consumidores, y que resuelva conflictos derivados del *e-commerce* transfronterizo con la misma eficacia que resuelve los conflictos del e-*commerce* doméstico. Este objetivo no se va a lograr con la aplicación de una norma que regule el comercio electrónico, en la medida que un gran número de compañías incluyen en sus términos y condiciones la renuncia de los consumidores a la ley de su territorio.

Las alternativas propuestas a la regulación para la solución de los nuevos problemas a los consumidores fueron el uso de la cooperación internacional y mecanismos como *smart contracts*. De dichas herramientas, solo la última pudo generar una automática tutela de los derechos de los consumidores, así como resolver con la misma eficacia los conflictos del *e-commerce* doméstico como el transnacional. Las otras alternativas no logran una tutela efectiva de los derechos de los consumidores independientemente de la ley o jurisdicción aplicable.

En ese sentido, dado que los *smart contracts* son mecanismos autoejecutables que se activan automáticamente una vez que se cumplen los parámetros predeterminados en el mundo real, tienen el potencial de mejorar la seguridad y la calidad del producto, así como proteger a los consumidores contra los productos falsificados. Especialmente, como hemos visto, en el sector aerocomercial, el uso de *smart contracts* para la devolución automática del dinero mediante aplicativos como Fizzy tiene el potencial de revolucionar el mercado de una forma sin precedente.

Esto cobra especial importancia en nuestro contexto actual. Como hemos revisado en el presente trabajo, la propuesta del Indecopi de abril del presente año ha recomendado el establecimiento del derecho de arrepentimiento en un plazo de quince días sin necesidad de justificación. Si esto se llega a concretar, lo más probable es que haya un aumento de devoluciones y las empresas tendrán que buscar un mecanismo eficiente para cumplir esta obligación con los consumidores.

Estamos en una época en donde la tecnología *blockchain* tiene el potencial de llevar la aplicación de los derechos individuales al siguiente nivel, generando una tutela que sí es efectiva para los consumidores, independientemente de si estamos ante una transacción de *e-commerce* doméstica o transfronteriza. En la misma línea, los organismos internacionales plantean el uso de soluciones no

solo desde la regulación, sino que también y, sobre todo, desde el empleo de tecnologías para garantizar los derechos de los consumidores.

Así, la Unión Europea ha instado al empleo de tecnologías para garantizar los derechos del consumidor colocando como un ejemplo tangible la devolución instantánea de los boletos de tren cuando ha habido una reprogramación del viaje. Ello, por supuesto, es perfectamente posible por medio de los *smart contracts*, ya que permitiría que se le pueda devolver al cliente el dinero de manera instantánea a su cuenta de banco (si ha utilizado una para la compra del pasaje) sin tener que recurrir a los mecanismos de reclamo de la empresa o, en última instancia, a los mecanismos de reclamo estatales.

REFERENCIAS

Agag, G. M., & El-Masry, A. (2016). Why Do Consumers Trust Online Travel Websites? Drivers and Outcomes of Consumer Trust toward Online Travel Websites. *Journal of Travel Research, 56*(3), 347-369.

Aldana Ramos, E. G. (2018). Uno, dos, tres… ¡catorce! O sesenta y seis Confianza y noción de consumidor final: un caso de comercio electrónico en protección al consumidor. *Derecho & Sociedad*, (50), 13-25.

Alibaba.com (9 de octubre de 2019). Acuerdo de suscripción gratuita. https://rule.alibaba.com/rule/detail/4293.htm

Allam, Z. (2018). On smart contracts and organisational performance: A review of smart contracts through the blockchain technology. *Review of Economic and Business Studies*, *11*(2), 137-156.

Amazon (3 de mayo 2021). Condiciones de uso. https://www.amazon.com/-/es/gp/help/customer/display.html?nodeId=GLSBYFE9MGKKQXXM

Bravo Tejeda, F. (2020a, 23 de agosto). Comercio electrónico Perú: La guía más completa del mercado. *Ecommerce News*. https://www.ecommercenews.pe/ecommerce-insights/2020/crecimiento-del-comercio-electronico-en-peru.html#:~:text=Seg%C3%BAn%20la%20CAPECE%20a%20inicios,entre%20un%2070%20a%2090%25

(2020b, 1 de octubre). Indecopi: Aumenta a 60 mil los reclamos relacionado con comercio electrónico desde la emergencia sanitaria. *Ecommerce News*. https://www.ecommercenews.pe/comercio-electronico/2020/indecopi-reclamos-ecommerce.html.

Cámara Peruana de Comercio Electrónico [Capece] (2019). *Reporte Oficial de la Industria Ecommerce en Perú. Crecimiento de Perú y Latinoamérica 2009-2019*. https://www.inteligenciaparanegocios.com/wp-content/uploads/2020/02/Reporte-Oficial-de-la-Industria-Ecommerce-en-Peru.pdf

Calvo-Porral, C., & Pesqueira-Sanchez, R. (2019). Generational differences in technology behaviour: comparing millennials and Generation X. *Kybernetes*. *49*(11), 2755-2772. https://doi.org/10.1108/K-09-2019-0598

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE Access, 4*, 2292-2303. doi: 10.1109/ACCESS.2016.2566339

De Caria, R. (2020). Definitions of Smart Contracts. En L. DiMatteo, M. Cannarsa & C. Poncibò (eds.), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (pp. 19-36). Cambridge University Press. doi:10.1017/9781108592239

El Comercio (12 de marzo de 2016). Ferragamo pone microchips en zapatos para combatir la piratería. https://elcomercio.pe/economia/mundo/ferragamo-pone-microchips-zapatos-combatir-pirateria-393582-noticia/?ref=ecr

(20 de julio de 2020). Indecopi da plazo de 10 días a 13 empresas para entregar productos vendidos por Internet. El Comercio. https://elcomercio.pe/economia/peru/compras-por-internet-indecopi-da-plazo-de-10-dias-a-13-empresas-para-entregar-productos-vendidos-por-internet-saga-falabella-sodimac-promart-oeschle-ripley-comercio-electronico-nndc-noticia/

European Commission (2015). Chapter III: Guidelines on Impact Assessment. En *Better Regulation Guidelines* (Working Document, pp. 14-30). https://ec.europa.eu/info/sites/default/files/better-regulation-guidelines.pdf

(2019). *Airbnb Enforcement Action Factsheet*. https://ec.europa.eu/info/sites/default/files/live_work_travel_in_the_eu/consumers/documents/airbnb_factsheet.pdf

Gestión (31 de octubre de 2020). Emprendedores esperan que regulación del Indecopi sobre eCommerce impulse ventas. Gestión. https://

gestion.pe/economia/asedi-espera-que-propuesta-del-indecopi-sobre-ecommerce-impulse-confianza-en-consumidores-nndc-noticia/?ref=gesr

Hallikanein, H., & Laukkanen, T. (2018). National culture and consumer trust in e-commerce. *International Journal of Information Management*, *38*(1), 97-106. https://doi.org/10.1016/J.IJINFOMGT.2017.07.002

Hill, E. (10 de noviembre de 2019). AXA drops Ethereum-based flight insurance platform. *Coin Rivet*. https://coinrivet.com/axa-drops-ethereum-based-flight-insurance-platform/

Hoffmann, C. H. (2020) A double design-science perspective of entrepreneurship – the example of smart contracts in the insurance market. *Journal of Work-Applied Management, 13*(1). https://doi.org/10.1108/JWAM-08-2020-0037

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [Indecopi] (2018). *Agenda Digital*. https://www.indecopi.gob.pe/documents/1902049/3742118/Agenda+digital+16.05.2018.pdf/4f28e644-deed-b4d9-b4b4-e4eeb6ff09f0

(2020a, 29 de mayo). El Indecopi recibió 1027 reclamos y reportes relacionados al comercio electrónico, a nivel nacional [nota de prensa]. https://repositorio.indecopi.gob.pe/bitstream/handle/11724/7466/NP%20200529%20Indecopi%20Fiscalizaci%C3%B3n%20del%20comercio%20electr%C3%B3nico.pdf?sequence=1&isAllowed=y

(2020b, 12 de noviembre). El Indecopi halla responsabilidad y ordena a las aerolíneas Latam y Latam Perú devolver el valor de pasajes a consumidores de 276 vuelos demorados, cancelados o reprogramados en el 2017 [nota de prensa]. https://repositorio.indecopi.gob.pe/handle/11724/7892

(2021). *Propuestas para la protección del consumidor en el comercio electrónico y la seguridad de productos* (Documento de Trabajo institucional del Indecopi). https://cdn.www.gob.pe/uploads/document/file/1776699/Documento%20de%20Trabajo%20-%20Comercio%20electronico%20%20version%20final%5BF%5D.pdf.pdf

Montes, S. (29 de marzo 2021). El comercio electrónico en la región creció 66% en 2020 y llegó a US$66.765 millones. *La República*. https://www.larepublica.co/globoeconomia/el-e-commerce-en-latinoamerica-aumento-66-durante-2020-y-llego-a-us66765-millones-3145702

Lee, M., & Turban, E. (2001). A trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce*, *6*(1), 75-91. https://doi.org/10.1080/10864415.2001.11044227

León Hilario, L. (2019). *Derecho privado. Parte general. Negocios, actos y hechos jurídicos*. Fondo Editorial de la Pontificia Universidad Católica del Perú.

Organización Mundial del Comercio [OMC] (2013). *El Comercio Electrónico en los países en desarrollo. Oportunidades y retos para las pequeñas y medianas empresas.* https://www.wto.org/spanish/res_s/booksp_s/ecom_brochure_s.pdf

Organización para la Cooperación y el Desarrollo Económicos [OCDE]. (2008). *Introductory Handbook for Undertaking Regulatory Impact Analysis (RIA)*. https://www.oecd.org/gov/regulatory-policy/44789472.pdf

Organización para la Cooperación y el Desarrollo Económicos [OCDE] & Banco Interamericano de Desarrollo [BID] (2016). *Políticas de banda ancha para América Latina y el Caribe: Un manual para la economía digital*. OECD Publishing. http://dx.doi.org/10.1787/9789264259027-es

Postigo, R., & Dupuy, J. (2000). Acerca del comercio electrónico, reforma del Código Civil y Código de comercio. Entrevista a Jorge Muñiz Ziches. *Ius et Veritas*, *10*(20), 324-327.

Presidencia del Consejo de Ministros (2017). *Manual para la aplicación del análisis de calidad regulatoria*. https://sgp.pcm.gob.pe/wp-content/uploads/2017/08/Manual-Analisis-de-Calidad-Regulatoria.pdf

Quintana Sánchez, E. (2011). Análisis de Impacto Regulatorio en la Regulación Peruana de Servicios Públicos. *Derecho y Sociedad*, (36), 15-29.

Radio Programas del Perú [RPP] (2020, 20 de octubre). Comercio electrónico: ¿Cómo reclamar si tuve problemas con mis compras por internet? https://rpp.pe/economia/economia/compras-online-como-reclamar-si-mi-pedido-no-llego-compras-por-internet-cyber-wow-e-commerce-coronavirus-en-peru-indecopi-noticia-1278323?ref=rpp

(2021a, 8 de marzo). Comercio electrónico alcanzó los US$ 6,000 millones en el 2020.

https://rpp.pe/economia/economia/comercio-electronico-alcanzo-los-us-6000-millones-en-el-2020-compras-online-coronavirus-en-peru-noticia-1324840?ref=rpp

(2021b, 2 de abril). Indecopi: Estas son las más de 700 empresas de transporte aéreo y terrestre sancionadas en 2020. https://rpp.pe/economia/economia/indecopi-estas-fueron-las-empresas-de-transporte-aereo-e-interprovincial-mas-multadas-en-el-2020-aerolineas-noticia-1329214?ref=rpp

Rodríguez, O. (4 de julio 2020). RFID: la tecnología que permite a Zara saber dónde está cada una de sus prendas. *El Independiente*. https://www.elindependiente.com/economia/2020/07/04/rfid-la-tecnologia-que-permite-a-zara-saber-donde-esta-cada-una-de-sus-prendas/

Rohr, J. (1 de mayo 2019). SAP Helps Swiss Post and Modum Build Blockchain Solution for Temperature-Controlled Logistics. *SAP*. https://news.sap.com/2019/03/swiss-post-modum-blockchain-solution-temperature-logistics/

Schulte-Nölke, H., Ruffer, I., Nobrega, C., & Wiewórowska-Domagalska, A. (2020). *The legal framework for e-commerce in the Internal Market* (Study for the committee on the Internal Market and Consumer Protection, Policy Department for Economic, Scientific and Quality of Life Policies). European Parliament. https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2020)652707

Smart Contracts Alliance (2018). *Smart Contracts: Is the Law Ready?* Chamber of Digital Commerce. https://digitalchamber.org/smart-contracts-whitepaper/

Súmar Albujar, O. (2012). Cinco errores frecuentes en la justificación de proyectos legislativos: una perspectiva económica. *THĒMIS-Revista De Derecho,* (62), 27-42.

Thorun C., & Diels, J. (2020). Consumer Protection Technologies: An Investigation Into the Potentials of New Digital Technologies for Consumer Policy. *Journal of Consumer Policy,* 43, 177-191. https://doi.org/10.1007/s10603-019-09411-6

Valdés, V. (9 de mayo 2016). Microchips en la ropa de Zara: Así se salvará la industria de la moda. *Vanity Fair*. https://www.revistavanityfair.es/lujo/articulos/microchips-zara-inditex-salvatore-ferragamo-moncler-industria-moda/22304

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS NORMATIVOS

Código de Protección y Defensa del Consumidor [CPDC], Ley 29571, Diario Oficial *El Peruano*, 1 de septiembre de 2010 (Perú).

Comisión de Protección al Consumidor 2 del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, 21 de setiembre 2015, Resolución Final 1632-2015/CC2, Expediente 181-2015/PS3 (Perú).

Comisión de Protección al Consumidor 2 del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, 7 de diciembre de 2016, Resolución Final 1971-2016/CC2, Expediente 308-2016/PS3 (Perú).

Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM (2020) 842 final (dic. 15, 2020).

Sala Especializada en Defensa de la Libre Competencia del Tribunal de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, 5 de agosto de 2020, Resolución 0084-2020/SDC, Expediente 0105-2018/CCD (Perú).

Sala Especializada en Protección al Consumidor del Tribunal de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, 2 de diciembre de 2015, Resolución 3816-2015/SPC-INDECOPI, Expediente 809-2014/CC2 (Perú).

Sala Especializada en Protección al Consumidor del Tribunal de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, 12 de noviembre 2020, Resolución 2107-2020/SPC-INDECOPI, Expediente 0037-2018/ILN-CPC-SIA (Perú).

10.18800/themis.202101.022

¿DESEA RECIBIR COMUNICACIONES PROMOCIONALES? UN ANÁLISIS DESDE LAS REGLAS DE PROTECCIÓN AL CONSUMIDOR Y DE DATOS PERSONALES

WOULD YOU LIKE TO RECEIVE ADS? AN ANALYSIS FROM CONSUMER AND DATA PROTECTION LAW

Fiorella Senno Vassallo*
Pontificia Universidad Católica del Perú

In this article, the author addresses the reform of the Consumer Protection and Defense Code carried out by Legislative Decree 1390, through which the Registry 'Gracias No Insista' was replaced by the rule of prior consent to receive mass communications with promotional purposes, which was aimed at harmonizing the consumer protection regulation with the one of personal data.

In this regard, the author develops a complete analysis of the regulation of promotional communications, both from the perspective of consumer protection rights and personal data protection; to later emphasize the successes and failures of the current regulation, at a legal and practical level. Likewise, the text proposes points of improvement to the current regulation and ends with practical recommendations on this matter to suppliers and consumers.

Keywords: Promotional communications; consumer protection; personal data protection; consent; advertising.

En el presente artículo, la autora aborda la reforma del Código de Protección y Defensa del Consumidor realizada mediante el Decreto Legislativo 1390, a través de la cual se reemplazó el Registro 'Gracias No Insista' por la regla del consentimiento previo para recibir comunicaciones masivas con fines promocionales, lo que tuvo por objetivo armonizar la normativa de protección al consumidor con la de datos personales.

Al respecto, la autora realiza un análisis completo de la regulación de las comunicaciones promocionales, tanto desde el enfoque de protección al consumidor como del de protección de datos personales; para posteriormente hacer énfasis en los aciertos y desaciertos de la regulación actual, a nivel legal y práctico. Asimismo, el texto propone puntos de mejora a la normativa vigente y finaliza con recomendaciones prácticas sobre la materia en cuestión dirigidas a proveedores y consumidores.

Palabras clave: Comunicaciones promocionales; protección al consumidor; protección de datos personales; consentimiento; publicidad.

* Abogada. Adjunta de docencia del curso Derecho Administrativo Económico en la Pontificia Universidad Católica del Perú. Asociada de Garrigues (Lima, Perú). Contacto: fiorella.senno@gmail.com

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 6 de julio de 2020, y aceptado por el mismo el 19 de julio de 2021.

I. INTRODUCCIÓN

> El Poder Ejecutivo, a propuesta del Indecopi, publica el Decreto Legislativo que modifica el Código de Protección y Defensa del Consumidor para que los ciudadanos no reciban promociones de productos y servicios no solicitados (Instituto Nacional de Defensa de la Propiedad Intelectual [Indecopi], 2018).

Este fue el titular del comunicado publicado por el Instituto Nacional de Defensa de la Propiedad Intelectual (en adelante, Indecopi) el 5 de setiembre de 2018, fecha en que se publicó el Decreto Legislativo 1390 que modificó el literal e) del artículo 58.1 del Código de Protección y Defensa del Consumidor (en adelante, CPDC), con el propósito de reemplazar el registro 'Gracias… No Insista' por la regla del consentimiento para recibir comunicaciones promocionales.

De esa manera, en búsqueda de armonizar el CPDC con la normativa de protección de datos personales, se estableció que únicamente sean blanco de llamadas, mensajes de texto y correos electrónicos masivos con fines promocionales, aquellas personas que previamente hubieren brindado su debido consentimiento; caso contrario, se configuraría una práctica prohibida por el CPDC: un método comercial agresivo. Sin embargo y paradójicamente, en el año 2019 el Perú fue el segundo país a nivel mundial en el que se realizaron más llamadas no deseadas o *spam* (Fai, 2019). Un año después las cosas variaron –pues el Perú pasó a ocupar el puesto catorce en el ranking del 2020–, aunque no tanto, porque se situó como el cuarto país de América Latina con más llamadas no deseadas (Fai, 2020).

Para abordar esta persistente realidad, no basta con realizar una lectura aislada del literal e) del artículo 58.1 del CPDC, por lo que revisaremos la regulación de las comunicaciones con fines promocionales sin consentimiento, tanto desde la perspectiva de protección al consumidor (como una práctica comercial agresiva prohibida) como desde la de protección de datos personales (en lo que respecta a su adecuado tratamiento), para así tener un panorama integral y diferenciar las comunicaciones prohibidas y las permitidas en dichos ámbitos. Posteriormente, identificaremos puntos de mejora respecto de los cuales plantearemos unas propuestas de modificación normativa. Por último, anotaremos unas recomendaciones para proveedores y consumidores.

II. PROTECCIÓN AL CONSUMIDOR

Sobre la base de la garantía constitucional de la defensa del interés de los consumidores, el CPDC ha reconocido que estos (incluyendo a los expuestos a una relación de consumo) tienen derecho a recibir información relevante sobre los productos y bienes que los proveedores ofrezcan en el mercado, para de esa manera, en virtud de la reducción de la asimetría informativa, estén en condiciones de tomar una adecuada decisión de consumo (Código de Protección y Defensa del Consumidor [CPDC], 2010). Dicha información deberá cumplir con ciertas características: ser veraz, suficiente, de fácil comprensión, apropiada, oportuna y fácilmente accesible.

Sin embargo, habrá que tener cautela sobre el modo en que se entrega la información de los productos y servicios a los consumidores, para no caer en empleo de métodos comerciales prohibidos, los que se clasifican en engañosos y agresivos. Serán engañosos, en el caso de conductas que puedan inducir a error al consumidor al adoptar una decisión sobre la transacción; mientras que, los métodos comerciales agresivos están referidos a las prácticas comerciales que mermen de forma importante la libertad de elección del consumidor mediante figuras como el acoso, la coacción, la influencia indebida y el dolo (Sánchez Barrios, 2012). En esta segunda clase de prácticas comerciales se han enmarcado a las comunicaciones con fines promocionales efectuadas masivamente y sin consentimiento.

Ante la compra de un producto o servicio derivada de la comisión de las prácticas comerciales prohibidas listadas en el artículo 58 del CPDC, en el artículo 59 se ha previsto el derecho del consumidor a la restitución inmediata de las prestaciones que fueron materia del contrato de consumo, el que únicamente deberá ser ejercido en un plazo de siete días calendario contados desde el día que se produjo la contratación del producto o servicio, o desde el día de su recepción o inicio de su ejecución, lo que ocurra con posterioridad (2010). Dicha disposición, conforme lo ha señalado la Sala Especializada en Protección al Consumidor del Indecopi, tiene por fin otorgarle al consumidor un periodo de reflexión sobre el bien adquirido o servicio contratado que le permita desistirse del contrato y obtener la restitución inmediata de lo que pagó, en caso de que el proveedor haya utilizado métodos comerciales agresivos en la contratación (Resolución 0728-2013/SPC-INDECOPI, 2013).

No obstante, el contar con un derecho de restitución y la posibilidad de reflexionar sobre la compra puede ser un arma de doble filo, pues se relativiza la prohibición de métodos comerciales agresivos, y en específico el consistente en realizar ofrecimientos por vía telefónica o electrónica sin el permiso de los consumidores. En palabras de Juan Espinoza Espinoza,

> aunque parezca paradójico, si bien el Código de Protección y Defensa del Consumidor (formalmente) prohíbe los denominados métodos comerciales agresivos o engañosos, en el fondo los permite, por el simple hecho que el derecho a la restitución tiene que ser ejercido por el consumidor: si no lo hace (dentro de un plazo de reflexión de 7 días), la venta será válida y producirá todos sus efectos (2010, p. 168).

De otro lado, hay que considerar que en este caso le corresponderá al consumidor acreditar la causal que sustenta su derecho a la restitución, con lo cual se busca que dicho pedido no se vacíe de contenido ni genere una situación perversa.

Dicho esto, pasemos a revisar el cambio normativo por el que ha atravesado la práctica comercial agresiva comentada. Veamos a continuación la regulación del Registro 'Gracias… No insista', para desarrollar los motivos de su derogación y su posterior reemplazo por la regla actual del consentimiento, y conocer cómo viene siendo aplicada.

A. Regla anterior: Registro 'Gracias… No insista'

En un principio, el derogado Decreto Supremo 006-2009-PCM, que aprobó el Texto Único Ordenado de la Ley del Sistema de Protección al Consumidor (en adelante, TUO de la LSPC) calificó en el literal f) del artículo 13 como un método comercial coercitivo al ofrecimiento de bienes o servicios por parte de proveedores a través de visitas, llamadas telefónicas o métodos análogos que fueren realizados de manera impertinente (2009). En concordancia con dicho precepto, la Quinta Disposición del Anexo de dicha norma estableció lo siguiente:

> Los proveedores que empleen *call centers*, sistemas de llamado telefónico, de envío de mensajes de texto a celular o de mensajes electrónicos masivos para promover productos y servicios, así como quienes presten el servicio de telemercadeo, **deberán excluir de entre sus destinatarios a todos aquellos números telefónicos y direcciones electrónicas que hayan sido incorporados a una lista que para dicho fin implementará el Indecopi**. **En dicha lista se podrán registrar los consumidores que no deseen ser sujetos de las modalidades de promoción antes indicadas** (Decreto Supremo 006-2009-PCM, 2009) [el énfasis es nuestro].

La referida lista fue implementada a través del Registro 'Gracias… No Insista' (en adelante, el Registro), en el cual podían inscribirse los consumidores para no recibir llamadas ni mensajes de empresas que promocionaran sus productos o servicios, esta era la regla. El Registro fue regulado por la Directiva 005-2009/COD-INDECOPI (2009), directiva de operación y funcionamiento del registro de números telefónicos y direcciones de correo electrónico excluidos de ser destinatarios de publicidad masiva, y de obligatorio cumplimiento a partir del 16 de setiembre de 2009.

Esta mecánica del registro para evitar recibir publicidad de empresas a las que no se les ha dado el consentimiento previo no fue una novedad peruana. Por ejemplo, en España existe la denominada 'Lista Robinson'[1], gestionada por la Asociación Española de Economía Digital, en la que se puede inscribir cualquier particular que desee manifestar su negativa u oposición al tratamiento de sus datos con fines comerciales (Beneyto, 2009), actualmente respaldada en el artículo 23 de la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (2018)[2].

Así, las personas que decidan inscribirse pueden elegir el canal de comunicación por el que no desean recibir publicidad (llamadas, correo electrónico, correo postal y SMS/MMA). Similar es el caso del 'National Do Not Call Registry'[3] de Estados Unidos, registro administrado por la Federal Trade Commission, al cual se inscriben las personas para no recibir llamadas no deseadas, salvo que se trate de llamadas con fines políticos, de caridad, cobros, encuestas y llamadas destinadas a proporcionar información en el marco de una relación contractual.

---

1 Para mayor información, véase Agencia Española de Protección de Datos (2021).

2 Artículo 23. Sistemas de exclusión publicitaria.

1. Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas. A tal efecto, podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los afectados. Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los afectados limiten la recepción de comunicaciones comerciales a las procedentes de determinadas empresas. […]

4. Quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo. A estos efectos, para considerar cumplida la obligación anterior será suficiente la consulta de los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente […] (Ley Orgánica 3/2018, 2018).

3 Para mayor información, véase Federal Trade Comission (2021).

Ahora bien, para el funcionamiento del Registro 'Gracias… No insista', era necesaria la inscripción de tanto (i) los consumidores que no querían recibir promociones (quienes podían registrar hasta cinco números telefónicos fijos, cinco celulares y cinco direcciones de correo electrónico); como de (ii) los proveedores que pretendiesen realizar promociones vía electrónica, telefónica o por mensaje de texto, quienes obtenían acceso a los números telefónicos y correos electrónicos registrados, mas no a otros datos personales de los consumidores.

De ese modo, los proveedores se encontraban obligados a excluir como destinatarios a los números telefónicos y direcciones electrónicas inscritos en el Registro antes de enviar cualquier comunicación para publicitar sus productos o servicios. Asimismo, en caso de que los proveedores hubieren contratado a terceros para que les presten servicios de *call center*, los primeros debían asegurarse de que los segundos adopten las medidas necesarias para que las remisiones efectuadas en su nombre obedezcan al marco normativo, sea exigiendo a la tercera proveedora que contara con la lista de direcciones excluidas o accediendo directamente a ella (Resolución Final 2092-2010/CPC, 2010).

Posteriormente, el TUO de la LSPC fue derogado por el CPDC, el cual entró en vigencia el 2 de octubre de 2010 y reguló en el artículo 58.1.e) como un método comercial agresivo el siguiente:

> Emplear centros de llamada (*call centers*), sistemas de llamado telefónico, envío de mensajes de texto a celular o de mensajes electrónicos masivos para promover productos y servicios, así como prestar el servicio de telemercadeo, a todos aquellos **números telefónicos y direcciones electrónicas que hayan sido incorporados en el registro implementado por el Indecopi** para registrar a los consumidores que no deseen ser sujetos de las modalidades de promoción antes indicadas [el énfasis es nuestro].

Seguidamente, la Directiva 005-2009/COD-INDECOPI fue modificada por la Resolución 159-2012-INDECOPI/COD, emitida por el Consejo Directivo del Indecopi, para adecuarla al CPDC, así como para relanzar el servicio del Registro mediante la variación y simplificación de ciertos aspectos del procedimiento de inscripción que ciertamente resultaban engorrosos, como la vigencia de la inscripción de los consumidores, que pasó de dos años renovables a ser indeterminada (2012). No obstante, conforme lo comentaremos a continuación, el fracaso del Registro 'Gracias… No insista' era inminente.

B. El fracaso del Registro 'Gracias… No insista'

Para noviembre de 2012, es decir, a los tres años de creación del Registro, eran tan solo 65 173 las personas registradas a nivel nacional, constaban inscritos 64 493 números de teléfonos celulares, 42 298 números de teléfonos fijos y 54 389 correos electrónicos; mientras que, únicamente 336 proveedores habían accedido al Registro a nivel nacional (Presidencia de Consejo de Ministros, 2012) antes de contactar a los consumidores. Ante esta situación, el Indecopi optó por reforzar su labor de supervisión y fomentar la denuncia por parte de los consumidores que hubiesen sido contactados, pese a su previa inscripción en el Registro. Sin embargo, a pesar de los esfuerzos, la gratuidad y la simplificación administrativa del procedimiento de inscripción; para diciembre de 2017, únicamente se encontraban inscritos 238 mil números de celulares y 119 mil teléfonos fijos, del total de 39.1 millones de líneas celulares y 2.9 millones de líneas fijas en el Perú para ese momento (Exposición de motivos del Decreto Legislativo 1390, 2018).

El evidente fracaso del Registro fue atribuido a tres causas: (i) el desconocimiento de su existencia, (ii) las restricciones de tiempo de los consumidores para registrarse y (iii) la falta de interés en la inscripción (Exposición de motivos del Decreto Legislativo 1390, 2018). Ahora bien, consideramos que principalmente, el fin del Registro habría obedecido a su intrínseca ineficiencia, pues si bien la inscripción era gratuita, lo cierto es que el CPDC colocaba en cabeza de los consumidores la carga de registrar su voluntad de no recibir comunicaciones promocionales, lo que principalmente implicaba el coste de oportunidad de su tiempo; mientras que los proveedores, además de registrarse, debían renovar periódicamente su inscripción. En resumen, una tediosa carga burocrática que no daba resultados prácticos.

Sin perjuicio de ello, existió otra razón también potente para derogar el Registro: la necesidad de concordar las normativas de protección al consumidor y de protección de datos personales, teniendo en cuenta la publicación de la Ley 29733, Ley de Protección de Datos Personales (en adelante, LDP) el 2 de julio de 2011, aún ajena o desconocida por muchos. Así, de acuerdo con la Exposición de Motivos del Decreto Legislativo 1390:

> La problemática encontrada luego de más de ocho años de vigencia del registro "Gracias…no insista" es, por un lado, que **estaría cumpliendo limitadamente su objetivo de que las empresas no puedan ofrecer propuestas comerciales a las personas que no deseen ser contactadas** y, por otro lado, el Código no se encuentra ade-

> cuado a lo señalado por la Ley de Protección de Datos Personales publicada en julio de 2011 (2018, p. 11) [el énfasis es nuestro].

Más adelante ahondaremos en dicha regulación; pero por lo pronto, tengamos en cuenta que la LDP tiene por objeto garantizar el derecho a la protección de los datos personales mediante el respeto de determinados principios como el del consentimiento, en virtud del cual, el tratamiento de los datos será lícito cuando su titular lo haya consentido libre, previa, expresa, informada e inequívocamente, para una finalidad específica.

C. Regla actual: el consentimiento

La regla del Registro cambió con la modificación del literal e) del artículo 58.1 del CPDC por el Decreto Legislativo 1390, vigente desde el 6 de septiembre de 2018. La regla se invirtió, ahora los consumidores solo deben recibir llamadas, mensajes de texto o correos electrónicos con fines promocionales siempre que previamente hayan manifestado su consentimiento. Así, de acuerdo con el vigente literal e) del artículo 58.1 del CPDC, califica ahora como un método comercial agresivo:

> Emplear centros de llamada (*call centers*), sistemas de llamado telefónico, envío de mensajes de texto a celular o de mensajes electrónicos masivos para promover productos y servicios, así como prestar el servicio de telemercadeo, **a todos aquellos números telefónicos y direcciones electrónicas de consumidores que no hayan brindado a los proveedores de dichos bienes y servicios su consentimiento previo, informado, expreso e inequívoco, para la utilización de esta práctica comercial**. Este consentimiento puede ser revocado, en cualquier momento y conforme a la normativa que rige la protección de datos personales (2018) [el énfasis es nuestro].

Según la Exposición de Motivos del Decreto Legislativo 1390,

> la Ley de Protección de Datos Personales señala como uno de sus principios rectores el del consentimiento, es decir, es necesario que las personas den su consentimiento expreso para que otros agentes económicos hagan uso de sus datos personales, como el número telefónico o correo (2018, p. 11).

En consecuencia, conforme lo señaló el Ministerio de Justicia, que es la Autoridad Nacional de Protección de Datos Personales (en adelante, ANDP) (Opinión Consultiva 12-2019-JUS/DGTAIPD, 2019), el Decreto Legislativo 1390 derogó tácitamente las disposiciones de la Ley 28493, coloquialmente conocida como la 'Ley Antispam', que permitía el envío de correos electrónicos comerciales sin consentimiento (*spam*), siempre que cumpliesen con ciertas características, como contener en el asunto la palabra 'PUBLICIDAD', incluir la denominación social, domicilio y correo electrónico del proveedor.

Este cambio de regla impulsado por el Indecopi buscó un escenario más eficiente del que se tuvo con el Registro y que se encuentre acorde con la regulación de protección de datos personales, uno en el que los consumidores *prima facie* se encuentren excluidos de recibir comunicaciones promocionales, salvo que así lo hubiesen autorizado. Es más, conforme se señala en la propia Exposición de motivos del Decreto Legislativo 1390, la prohibición del CPDC de efectuar comunicaciones a quienes se encontrasen inscritos en el Registro había sido tácitamente modificada con la parcial entrada en vigencia de la LDP en el año 2011 (2018); la que dispone en su artículo 13.5 que, salvo ley autoritativa al respecto, los datos personales solo pueden ser objeto de tratamiento con consentimiento de su titular, el que debe ser previo, informado, expreso e inequívoco (Ley 29733, 2011).

Asimismo, a través de esta nueva regulación, y conforme consta en la Exposición de motivos del Decreto Legislativo 1390, se buscó prevenir el acoso telefónico, con lo cual, los proveedores que hubiesen recibido un 'no' como respuesta, no deberían insistir. Sin embargo, ¿en realidad se está castigando el acoso telefónico (entendido como hostigamiento)? No precisamente, pues el literal e) del artículo 58.1 del CPDC no ha sido redactado en ese sentido; por lo cual, se entiende que la sola llamada o el solo envío de un correo electrónico sin consentimiento o sin que este haya sido emitido de conformidad con la regulación de protección de datos personales, ya calza como un método comercial agresivo, lo que consideramos cuestionable. En esa línea, habría que buscar que la interpretación sea menos restrictiva, pues consideramos que dichos actos aislados no calzan en la definición de métodos comerciales coercitivos y, más aún, considerando que tales actos ya se encuentran prohibidos por la normativa de datos personales –como lo revisaremos más adelante–, por lo que vemos que se pecó de sobrerregulación.

De otro lado, con el objeto de reforzar el rol fiscalizador del Indecopi sobre las comunicaciones promocionales sin consentimiento, la entidad habilitó a fines del 2018 el 'WhatsApp No Insista', que permite a los consumidores tener un canal sencillo y directo para reportar rápidamente las ofertas sobre productos y servicios que reciben sin haber brindado su consentimiento previo, o quienes, pese a haber manifestado su negativa,

continúen recibiendo dichas comunicaciones. De esa manera, el Indecopi se hace de información sobre presuntas infracciones y evalúa la correspondencia del inicio de un procedimiento administrativo sancionador por infracción al literal e) del artículo 58.1 del CPDC.

Así, el Indecopi ha impuesto sanciones que oscilan desde la amonestación hasta las 447.36 UIT (Resolución 0542-2021/SPC-INDECOPI, 2021) (incluyendo la remisión de la resolución final a la Autoridad Nacional de Protección de Datos Personales), considerando que la multa máxima es de 450 UIT; así como ha archivado procedimientos administrativos sancionadores tras haberse acreditado que los proveedores contaban con el consentimiento de los consumidores para realizar comunicaciones promocionales. Por ejemplo, Miducom Perú S.A. acreditó haber contado con el consentimiento de ciento veinticinco (125) consumidores para el envío de promociones a los números telefónicos y correos electrónicos que aquellos habían autorizado a través de la plataforma web de dicha compañía (Resolución Final 021-2020/CC3, 2020).

Entre los criterios jurisprudenciales que viene adoptando el Indecopi, la Comisión de Protección al Consumidor ha precisado que, cuando ante la vulneración del literal e) del artículo 58.1 del CPDC los proveedores incluyan a los consumidores en 'listas de no contactabilidad' para cesar el envío de mensajes sin consentimiento previo, esto no calificará como una subsanación voluntaria de la conducta; pues como bien indica, en este supuesto no hay conducta que subsanar dado que la afectación al derecho de los consumidores se concretó con las comunicaciones cursadas sin consentimiento (Resolución 288-2019/CC3, 2019). En consecuencia, en este escenario no nos encontramos ante una eximente de responsabilidad administrativa prevista en el artículo 257.1 del Texto Único Ordenado de la Ley de Procedimiento Administrativo General (en adelante, TUO de la LPAG) (Decreto Supremo 004-2019-JUS, 2019), sino frente a una atenuante, específicamente establecida en el artículo 112 del CPDC (2010).

Ahora bien, a fin de que una denuncia por infracción del literal e) del artículo 58.1 del CPDC tenga éxito, en el caso de llamadas telefónicas, por ejemplo, existen ciertos candados previstos por el Indecopi, ya que se debe acreditar: (i) la titularidad del denunciante sobre la línea telefónica; (ii) el ingreso de las llamadas efectuadas desde los números denunciados; (iii) el contenido publicitario de las llamadas (ofrecimiento de planes tarifarios para que cambie de operador); y (iv) la titularidad de la denunciada sobre los números indicados en el punto (ii) (Resolución 0943-2019/SPC-INDECOPI, 2019; Resolución Final 981-2020/CC2, 2020). No olvidemos que esto obedece al principio general del derecho, según el cual, 'quien alega un hecho debe probarlo'.

III. PROTECCIÓN DE DATOS PERSONALES

Al igual que la protección al consumidor, la protección de datos personales es un derecho fundamental, reconocido en el artículo 2.6 de la Constitución Política del Perú, según el cual las personas tienen derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar (1993). Esta garantía ha sido desarrollada por la LDP y su Reglamento (en adelante, RLDP), aprobado mediante el Decreto Supremo 003-2013-JUS (2013), para regular el adecuado tratamiento de datos personales, principalmente por parte de los titulares de bancos de datos o por terceros encargados de dicha tarea en virtud de una relación jurídica mantenida con los primeros. Para tal efecto, la ANDP cuenta con potestad normativa y orientativa, pero también fiscalizadora y sancionadora.

Cabe señalar que por datos personales entendemos a toda información (numérica, alfabética, gráfica, fotográfica o acústica) sobre hábitos personales, o de cualquier otro tipo respecto de una persona natural, que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados (Decreto Supremo 003-2013-JUS, 2013, art. 2.5). Así, de conformidad con la ANDP, la dirección de correo electrónico y el número telefónico son datos personales en tanto identifican indirectamente a una persona (Autoridad Nacional de Protección de Datos Personales, 2013). Asimismo, este concepto incluye a los datos sensibles, los que se encuentran referidos a las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental, u otras análogas que afecten su intimidad.

Mientras que, por tratamiento de datos personales se entiende a cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales (Decreto Supremo 003-2013-JUS, 2013, art. 2.19). En todos estos casos, quien recoge los datos, denominado 'titular del banco de datos', debe cumplir con determinadas obligacio-

nes en relación con el titular de los datos, como contar con su consentimiento para el uso de sus datos y obtener su debido consentimiento para fines específicos.

Una vez que los datos personales han sido recopilados por el titular del banco, con el consentimiento del titular de los datos, estos pueden ser tratados directamente por el primero o ser transferidos a terceros para que estos los traten, pero en ambos casos deberá de respetarse la finalidad por la cual fueron recogidos. Así por ejemplo, en caso de que las compañías subcontraten los servicios de *call centers* para que, a través de llamadas telefónicas a sus clientes, les proporcionen información sobre ofertas y campañas; será necesaria la autorización por parte del titular del banco de datos personales para tal fin (Decreto Supremo 003-2013-JUS, 2013, art. 37), quien, a su vez, debería haberlos obtenido con el consentimiento de los titulares de los referidos datos para su transferencia.

Ahora bien, cuando las compañías contratan *call centers* en el marco de un encargo de tratamiento para que realicen llamadas telefónicas a sus clientes con fines promocionales, la entrega de los datos personales del titular del banco de datos al *call center* no constituye una transferencia (Decreto Supremo 003-2013-JUS, 2013, art. 36). En ese sentido, no será necesario recabar el consentimiento de los titulares de los datos personales para su traspaso al *call center*. No obstante, este último solo podrá utilizarlos dentro del ámbito de dicho encargo; de manera que, para realizar tratamientos con fines distintos, primero deberá obtener el consentimiento del titular del dato personal (Oficio 146-2018-JUS/DGTAIPD, 2018). Así, en caso los datos personales no hubieren sido recogidos por el titular del banco para realizar comunicaciones con fines promocionales, será necesario recabar el consentimiento para tal finalidad.

Sin lugar a duda, los titulares de bancos de datos personales son agentes del mercado que reconocen el indiscutible valor comercial de la información como un recurso intangible. En la actualidad, evidentemente las empresas otorgan un alto valor al uso de los datos personales para fines publicitarios, para realización de campañas comerciales y para la prospección comercial (Biedma & Medina, 2012a), pues es indubitable que representa una ventaja para ofertar bienes y servicios a clientes actuales, así como para atraer potenciales clientes, incluso con una mayor motivación en un contexto de pandemia por el COVID-19 para superar la lamentable crisis económica generada.

Sin perjuicio de lo anterior, tal ejercicio empresarial deberá involucrar un apropiado tratamiento de los datos personales, lo que implica el respeto de determinados principios y derechos. De esa manera, se proporcionará tranquilidad a aquellos cuyos datos son correctamente tratados, se generará una imagen corporativa más valiosa y una mayor receptividad de clientes actuales y potenciales (Biedma & Medina, 2012b).

A. Principio del consentimiento

La LDP incluye un listado enunciativo de principios rectores del tratamiento de datos personales por parte de titulares de bancos de datos y de los encargados de su tratamiento, entre los que se encuentra el principio de consentimiento. La importancia del consentimiento reside en que materializa nuestra voluntad en ejercicio de nuestra libertad; por lo cual, la LDP y su Reglamento han previsto que, para ser debido, necesariamente deberá cumplir con las siguientes características:

(i) Libre: debe otorgarse sin que medie error, mala fe, violencia o dolo que pueda afectar la manifestación de voluntad del titular de los datos.

(ii) Previo: debe emitirse antes de la recopilación de datos, así como con anterioridad al tratamiento distinto a aquel por el cual se recopilaron.

(iii) Expreso e inequívoco: el consentimiento puede válidamente concederse de manera verbal (mediante una llamada telefónica) o escrita, sea con firma autógrafa o por medios digitales (con un *click* en la casilla 'He leído y estoy de acuerdo con la política de tratamiento de datos personales' de una página web, o mediante firma electrónica).

(iv) Informado: se le debe comunicar al titular de los datos personales, de manera clara, expresa, indubitable y con lenguaje sencillo, cuando menos, la existencia del banco de datos personales en el que se almacenarán, la identidad y domicilio del titular del banco, la finalidad del tratamiento de los datos, las transferencias de datos personales y sus destinatarios, y los canales para ejercer los derechos en calidad de titular de datos personales (Ley 29733, 2011; Decreto Supremo 003-2013-JUS, 2013).

De ese modo, para realizar cualquier tipo de tratamiento de datos personales, el titular del banco de datos personales o quien resulte como responsable del tratamiento, se encuentra obligado a conseguir el consentimiento para dicho fin. Sin perjuicio de ello, esta regla tiene excepciones, las

que se encuentran recogidas en el artículo 14 de la LDP: por ejemplo, cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público; cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento; cuando se hubiera aplicado un procedimiento de anonimización o disociación (Ley 29733, 2011). Por consiguiente, como regla general, cualquier clase de tratamiento de datos personales deberá realizarse si se cuenta con el consentimiento previo de su titular, salvo que exista una excepción prevista por la LDP.

Ahora bien, el contacto de consumidores para fines promocionales no se encuentra incluido como una excepción por el artículo 14 de la LDP, en consecuencia, será necesario que la empresa que pretenda enviar publicidad o comunicaciones promocionales dirigidas a terceros, cuente con su debido consentimiento para tal finalidad; el que, como vimos deberá ser libre, previo, informado, expreso e inequívoco.

B. Derechos de los titulares de datos personales

Adicionalmente, el correcto tratamiento de los datos personales involucra el respeto de los derechos de los titulares de datos personales conocidos como 'ARCO'; acrónimo de los derechos de acceso, rectificación, cancelación y oposición. Estos derechos, en virtud de las disposiciones generales del Título IV del RLDP, al ser de carácter personalísimo, exclusivamente pueden ser ejercidos por el titular de los datos personales, a través de procedimientos que deben caracterizarse por ser sencillos y proporcionados gratuitamente por los titulares de bancos de datos o responsables de su tratamiento (Decreto Supremo 003-2013-JUS, 2013).

(i) Acceso: derecho a obtener la información que sobre sí mismo sea objeto de tratamiento, lo que incluye el origen de la recopilación de sus datos, las razones que motivaron su recopilación y a solicitud de quién fue realizada, así como las transferencias de los datos efectuadas o que se prevén hacer.

(ii) Rectificación: derecho a que se modifiquen los datos personales cuando estos hubieren sido recopilados de manera inexacta o incompleta; o, si se hubiere advertido alguna omisión, error o falsedad. Además, abarca la actualización e inclusión de nuevos datos personales.

(iii) Cancelación: derecho a que se supriman los datos personales cuando estos hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recopilados, por el vencimiento del plazo establecido para su tratamiento, de haberse revocado el consentimiento para el tratamiento, así como en aquellos casos en los que no estén siendo tratados de conformidad con la LDP y el RLDP.

(iv) Oposición: derecho a que no se lleve a cabo el tratamiento de sus datos personales o este sea cesado, cuando no hubiere prestado su consentimiento para su recopilación por haber sido tomados de fuente de acceso al público; o cuando habiéndolo prestado, se pueden oponer por la existencia de motivos fundados y legítimos relativos a una concreta situación personal que justifiquen el ejercicio de este derecho (Decreto Supremo 003-2013-JUS, 2013, Título IV).

Según el artículo 55 del RLDP, para responder las solicitudes que fueren presentadas en ejercicio de los derechos ARCO, los titulares de bancos de datos personales o los responsables del tratamiento se sujetan a los siguientes plazos máximos, los que no consideramos eficientes por su amplitud:

(i) Ante el ejercicio del derecho de información, hasta ocho días contados desde el día siguiente de la presentación de la solicitud.

(ii) Ante el ejercicio del derecho de acceso, hasta veinte días contados desde el día siguiente de la presentación de la solicitud. Ahora bien, en caso de que la solicitud fuera estimada y el titular del banco de datos personales o responsable del tratamiento no acompañase a su respuesta la información solicitada, el acceso será efectivo dentro de los diez días siguientes a dicha respuesta. Lo que, en total, podría sumar un plazo de treinta días.

(iii) Ante el ejercicio de los derechos de rectificación, cancelación y oposición, hasta diez días hábiles para responder las solicitudes (Decreto Supremo 003-2013-JUS, 2013).

Tras la presentación de las solicitudes para el ejercicio de tales derechos, los titulares de bancos de datos personales o responsables del tratamiento únicamente podrán dar una respuesta total o parcialmente negativa si se encuentra debidamente justificada. En este último escenario, deberán señalar el derecho que les asiste para que, en todo caso, los titulares de los datos puedan recurrir

dicha decisión ante la ANDP. Asimismo, la prueba del cumplimiento del deber de respuesta le corresponderá al titular del banco de datos personales o responsable del tratamiento, debiendo conservar los medios para hacerlo.

De otro lado, hay casos en los que nos encontraremos frente a una recopilación de datos personales haciendo uso de medios fraudulentos, desleales o ilícitos, considerando que en nuestro país existe un gran mercado negro[4]. Esta conducta vulnera el principio de legalidad y ha sido calificada como una infracción muy grave por el RLDP (Decreto Supremo 003-2013-JUS, 2013, art. 132, numeral 2, literal e), pasible de ser sancionada con una multa desde 50 UIT hasta 100 UIT. Además, se suma a esto el tratamiento que pueda hacerse de ellos en ausencia del consentimiento de su titular, como su almacenamiento y utilización para la realización de comunicaciones promocionales. Dicho tratamiento sin consentimiento califica como una infracción grave, pasible de ser sancionada con una multa de 5 UIT hasta 50 UIT (Decreto Supremo 003-2013-JUS, 2013, art. 132, numeral 2, literal b).

IV. ENTONCES, ¿QUÉ TIENEN DE DIFERENTE LAS COMUNICACIONES PROMOCIONALES QUE RECIBÍAMOS ANTES DE LA MODIFICACIÓN DEL CPDC Y LAS QUE RECIBIMOS HOY?

Según la Exposición de Motivos del Decreto Legislativo 1390, la modificación del CPDC para reemplazar el Registro por la regla del consentimiento se sostenía en gran parte porque

> la Ley de Protección de Datos Personales señala como uno de sus principios rectores el del consentimiento, es decir, es necesario que las personas den su consentimiento expreso para que otros agentes económicos hagan uso de sus datos personales, como número telefónico o correo electrónico. Por lo que el Proyecto de Ley permitiría la adecuación del Código a dicha Ley (2018, p. 11).

Sin embargo, no habrá que perder de vista que la propia LDP ha previsto excepciones para la obtención del consentimiento (sin que esto impida el respeto de los demás principios previstos en la normativa). Así, de acuerdo con el artículo 14.2 de la norma, no se requiere el consentimiento del titular de datos personales para los efectos de su tratamiento, entre otros casos, cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público (Ley 29733, 2011). De acuerdo con el artículo 17 del RLDP, son consideradas fuentes accesibles al público, entre otros:

> 1. Los medios de comunicación electrónica, óptica y de otra tecnología, siempre que el lugar en el que se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general.
> 2. Las guías telefónicas, independientemente del soporte en el que estén a disposición y en los términos de su regulación específica.
> 3. Los diarios y revistas independientemente del soporte en el que estén a disposición y en los términos de su regulación específica.
> 4. Los medios de comunicación social.
> 5. Las listas de personas pertenecientes a grupos profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección postal, número telefónico, número de fax, dirección de correo electrónico y aquellos que establezcan su pertenencia al grupo.
> 6. […]
> 7. Los Registros Públicos administrados por la Superintendencia Nacional de Registros Públicos - SUNARP, así como todo otro registro o banco de datos calificado como público conforme a ley (Decreto Supremo 003-2013-JUS, 2013).

En esa línea, la ANDP, en respuesta a la consulta sobre el sentido del entonces proyecto de modificación del CPDC para reemplazar la regla de la inscripción en el Registro 'Gracias…no insista' por la del consentimiento del consumidor, manifestó lo siguiente:

> […] es preciso mencionar que **la obligación de obtener el consentimiento previo no significa la prohibición absoluta de contacto, siempre que el dato personal de contacto haya sido obtenido de una fuente accesible al público**, de acuerdo con lo señalado en el artículo

[4] Lamentablemente, como bien se expone en una investigación llevada a cabo por El Comercio (2015), en nuestro país existe un gran mercado negro en el que el producto estrella son precisamente los datos personales (nombres, números telefónicos, direcciones, correos electrónicos, sueldos, líneas de crédito y más). El tráfico de esta información sigue toda una cadena 'estratégica': (i) los datos son obtenidos de manera lícita y con el consentimiento de los clientes por empresas y por instituciones públicas a través de formularios virtuales, llamadas telefónicas o fichas impresas; (ii) la información ingresa a la base de datos de la empresa para un fin específico, como el informativo o publicitario; (iii) pero, los empleados de las compañías, ilícitamente copian las bases de datos y luego las venden, por ejemplo, en diferentes galerías del Centro de Lima; (iv) quienes las adquieren, copian las bases de datos en CDs o USBs y las venden, o las transfieren en 'la nube' (El Comercio, 2015). De esta manera, otras empresas terminan adquiriendo datos personales de manera ilegal, junto con las mafias dedicadas a la extorsión y el reglaje, lo que resulta aún más preocupante.

> 17 del Reglamento de la LDP. **En ese caso, el primer contacto debe estar orientado a informar al titular del dato personal sobre los tratamientos de datos personales adicionales y a obtener su consentimiento para los mismos** (Oficio 146-2018-JUS/DGTAJPD, 2018) [el énfasis es nuestro].

Por lo cual, con el bien intencionado Decreto Legislativo 1390 se buscaba que los consumidores que no deseasen ser contactados, no lo sean en virtud a una prohibición absoluta, sin necesidad de que registren previamente dicha voluntad en el Registro administrado por el Indecopi (prohibición relativa). No obstante, aquello es relativo, pues colisiona con la propia LDP en el sentido que, según lo expuesto por la ANDP, en tanto la recopilación de datos sea efectuada a través de fuentes de acceso público, será legal que los proveedores se comuniquen con los consumidores con la intención de ofertar sus productos y servicios, siempre que en la primera interacción con ellos se solicite su consentimiento para tal fin.

Luego, solo en caso de que la respuesta fuese afirmativa, se le podrá entregar la información con fines promocionales; caso contrario, si la respuesta fuese negativa y pese a ello se le entregue información promocional o se le volviese a contactar para el mismo fin, recién nos encontraríamos entonces en un incumplimiento de la normativa de datos personales, pues se habría quebrantado la voluntad del titular de los datos personales.

Es así como, luego de modificado el CPDC, el Indecopi, siguiendo lo expuesto por la ANDP, ha advertido en su propia jurisprudencia que no toda comunicación *per se* está prohibida, pues para obtener el consentimiento debe existir un primer contacto con el consumidor, siempre que el dato personal haya sido obtenido de una fuente de acceso al público. Esto es clave para entender por qué pese al cambio de regla del CPDC del que hablamos, legalmente continuamos recibiendo llamadas o mensajes.

Así, en el caso de comunicaciones telefónicas, cuando el proveedor haya tenido acceso al número telefónico y nombre del consumidor mediante fuentes de acceso público, en los primeros segundos de la llamada obligatoriamente se le deberá pedir su consentimiento para específicamente brindarle información promocional, y solo con su aceptación, se podrá proseguir con ello. Mientras que, en el caso de comunicaciones por mensaje de texto o correo electrónico, el primer mensaje que se envíe deberá servir para recabar el consentimiento, mas no para brindar directamente la información con fines promocionales.

En ese sentido, dado que las actuaciones de instrucción del procedimiento sancionador, tanto en el llevado a cabo por el Indecopi como por la ANDP, tienen por finalidad determinar si las comunicaciones contaban con el consentimiento del consumidor (y más allá de esto, que sea un consentimiento previo, informado, expreso e inequívoco), es de suma importancia que los proveedores posean los medios probatorios que lo sustenten, para así poder afrontar la carga de la prueba. Sin perjuicio de que, como vimos, no basta con que los consumidores afirmen haber recibido una comunicación promocional no consentida, es necesario que acrediten su recepción, siguiendo los criterios jurisprudenciales, indicados en la sección II.C. del presente escrito.

V. PROPUESTAS DE MEJORA

A. Sobre el riesgo del *non bis in ídem*

Hasta aquí tenemos que para que no se configure la práctica comercial agresiva prevista en el literal e) del artículo 58.1 del CPDC, se requerirá del consentimiento del consumidor, el que puede haberse obtenido básicamente de dos formas: de manera previa a la comunicación (sea directamente con el consumidor o indirectamente si existió una debida transferencia de datos) o como parte del primer contacto con el consumidor, si los datos personales se obtuvieron de una fuente pública (2010). Sobre esta última alternativa, opinamos que, si bien las expectativas de la modificación del CPDC no se condicen a cabalidad con la normativa de datos personales –lo que explica por qué los consumidores continúan recibiendo llamadas no deseadas pese al cambio normativo–, es cierto que no vulnera las normas de protección de datos personales ni de protección al consumidor, pues se busca un punto medio entre la libertad de empresa y el principio de consentimiento.

Ahora bien, habrá que ser muy cautelosos en la aplicación de los regímenes sancionadores, respecto de las comunicaciones promocionales sin consentimiento prohibidas por el CPDC y el tratamiento de datos personales sin consentimiento proscrito por la LDP y el RLDP. Recordemos que la infracción del CPDC se configurará con el envío masivo de comunicaciones promocionales sin consentimiento; por lo cual, en principio, el envío aislado de comunicaciones no debiera ser una conducta punible por dicha normativa, sino exclusivamente por la regulación de protección de datos personales. Sin embargo, consideramos que esto da cabida a un traslape normativo, bajo el cual en última instancia se sancionaría por lo mismo: ausencia de debido consentimiento.

En esa línea, cuando nos encontremos frente a este tipo de comunicaciones, nos preocupa el riesgo de que se inicien dos procedimientos sancionadores contra los agentes del mercado y que, como resultado, sean doblemente sancionados: por parte del Indecopi, por infracción del literal e) del artículo 58.1; y por parte de la ANDP, por vulneración del principio de consentimiento. Sobre este punto, debemos hacer un paréntesis para recordar que, la finalidad de la sanción no es solo la de castigar –ni mucho menos doblemente–, sino la de apuntar a la modificación de la conducta de los regulados con el objeto de que se cumplan las finalidades perseguidas por el derecho administrativo (Soto Delgado, 2017) y por el ordenamiento jurídico en general; lo que puede lograrse por medio de otras herramientas como la orientación y la imposición de medidas correctivas en el marco de fiscalizaciones, siguiendo un enfoque de regulación responsiva habilitado por la modificación de la TUO de la LPAG mediante el Decreto Legislativo 1272 (2016).

Al respecto, consideramos de suma importancia el respeto al principio de *non bis in* ídem, garantía del procedimiento administrativo sancionador recogida en el artículo 248.11 del TUO de la LPAG; en virtud del cual, no podrán imponerse dos sanciones administrativas por el mismo hecho cuando exista la triple identidad de sujeto, hecho y fundamento. Así, el *non bis in ídem* supone la colisión de dos leyes sobre un mismo hecho que podría ser sancionado por ambas (Carretero Pérez & Carretero Sánchez, 1995), lo que precisamente se busca evitar.

Usualmente, no hay mucho inconveniente en determinar la igualdad de hechos y actores, la dificultad llega cuando se analiza la identidad del fundamento, que muchas veces se niega, pero no siempre se justifica adecuadamente. Así, en este caso en concreto podría alegarse que las inconductas recogidas en el literal e) del artículo 58.1 del CPDC y en el artículo 132.2 del RLDP pueden poseer identidad de hechos y actores, pero no el mismo fundamento, bajo el argumento de que nos encontraríamos ante dos bienes jurídicos distintos: la protección al consumidor y la protección de los datos personales.

No obstante, en el fondo, sea el Indecopi o la ANDP, consideramos que el sustento para aplicar una sanción será el mismo: que se haya vulnerado el principio de consentimiento, por haber actuado en contra de la voluntad del titular de los datos personales (o consumidor). De esa manera, ambas instituciones, de acuerdo con la normativa vigente, se encuentran facultadas para sancionar a aquel que haya realizado una comunicación promocional que no haya obtenido el debido consentimiento del titular, para lo cual ambas velarán por determinar si se contó con el consentimiento, y si fue previo, informado, expreso e inequívoco. Por lo cual, no vemos plausible repetir el castigo por dos vías administrativas.

A fin de eliminar el riesgo de doble procedimiento administrativo sancionador y de doble sanción, consideramos que la mejor salida, de cara a una lectura más integral, coherente y razonable del ordenamiento jurídico, consiste en la modificación de la Séptima Disposición Complementaria Final de la LDP, relativa a las competencias del Indecopi[5]. En esta disposición se ha previsto que, sin perjuicio de la competencia asignada a la ANDP para salvaguardar los derechos de los titulares de información administrada por las Centrales Privadas de Información de Riesgos (CEPIRS) o similares; en materia de infracción a los derechos de los consumidores mediante la prestación de servicios e información brindados por las aquellas centrales, en el marco de las relaciones de consumo, son aplicables las normas sobre protección al consumidor, siendo el Indecopi el único competente para la supervisión de su cumplimiento.

Del mismo modo, dicha disposición contenida en la LDP podría establecer que, cuando se trate de infracciones cometidas al literal e) del artículo 58.1 del CPDC, tras haberse acreditado que los proveedores no contaban con el consentimiento de los consumidores para realizar comunicaciones promocionales, la competencia exclusiva sancionadora recaiga en el Indecopi; y que la ANDP no podrá sancionar nuevamente al proveedor por no haber contado con el consentimiento de los consumidores. Lo anterior no debiera implicar que la ANDP no pueda fiscalizar, iniciar procedimientos sancionadores y, de ser el caso, sancionar a aquellos proveedores que hayan cometido otras infracciones conexas, como haber recabado de manera ilegal los datos personales o haber obstaculizado el ejercicio de los derechos ARCO.

Una distinta alternativa sería que, en tanto una de las entidades ya haya ejercido su potestad sancionadora, la otra se abstenga de ejercer la propia; sin embargo, lo cierto es que esto traería grandes dificultades prácticas en su aplicación.

[5] Este asunto fue además evaluado por Asunción Ampuero Miranda y Paola Liliana Lobatón Fuchs, vocales de Sala Especializada en Protección al Consumidor. Véase la Resolución 32352015/SPCINDECOPI (2015) y Resolución 1931-2016-SPC-INDECOPI (2016).

B. Simplificación de los procedimientos para el ejercicio de los derechos ARCO

Consideramos que, si bien se ha avanzado en el camino de armonizar las normativas de protección de datos personales y la de protección al consumidor, aún queda un tramo por recorrer. Por ejemplo, si nos preguntamos cómo podrían hacer los consumidores para saber si el proveedor que los llama para ofrecerle sus servicios ha accedido legalmente (por medio del consentimiento o por fuentes públicas) o ilegalmente a sus datos personales, la respuesta parecería caer de madura: consultando en la llamada telefónica sobre el origen del consentimiento para tal efecto. Sin embargo, lo cierto es que el proveedor no está obligado a responder en ese momento y, si lo hace, por la premura o desconocimiento de los trabajadores, no siempre la respuesta será precisa.

Como lo hemos comentado, la LDP ha regulado un extenso plazo de hasta treinta días hábiles para que los proveedores atiendan las solicitudes de ejercicio del derecho de acceso, lo que dificulta que los consumidores puedan conocer o, de ser el caso, recordar, quién, cómo y con qué finalidad se recopilaron de sus datos. Acceder rápida y seguramente a dicha información facilitaría el ejercicio de otros derechos como la oposición, revocación de consentimiento, o bien la interposición de una denuncia ante la ANDP en caso no se reconociese una fuente de acceso legal.

Adicionalmente, según los artículos 49 y 50 del RLDP, la solicitud de acceso deberá dirigirse al titular del banco de datos personales o al responsable de su tratamiento; para lo cual, el consumidor deberá acreditar su identidad con una copia de su Documento Nacional de Identidad o a través de la firma digital (Decreto Supremo 003-2013-JUS, 2013). Estas exigencias dificultan aún más el ejercicio del derecho de acceso, lo que puede traducirse en: (i) la ausencia de denuncias que permitan detectar la comisión una práctica comercial prohibida y la vulneración del principio de legalidad; o bien, (ii) la presentación de reportes al 'Whatsapp No Insista' y de denuncias sin fundamento, cuando el acceso a los datos personales por los proveedores haya sido realizado de acuerdo con el principio del consentimiento o por el acceso a información pública. Lo cual genera ineficiencias en cuanto a costos y tiempo.

Así, la excesiva formalidad del RLDP dificulta el ejercicio del derecho de acceso y los otros derechos relacionados, lo que consiguientemente termina por afectar tanto los derechos de los consumidores que pueden no recibir una respuesta veraz y oportuna, así como a los intereses de los propios proveedores, quienes, de no revelar su fuente de manera correcta y con prontitud, se exponen a reclamos que eventualmente pueden culminar en el inicio de procedimientos administrativos sancionadores por parte del Indecopi o de la ANDP, algunos fundados y otros no, pero al final de cuentas, prevenibles.

Es más, el propio ejercicio del derecho de revocación debería ser lo más sencillo posible, debería bastar solo con ser ejercido telefónicamente o por mensaje, sin mayores formalidades. Sin embargo, si bien este es el espíritu del artículo 16 del RLDP, que dispone que la revocación del consentimiento puede realizarse en cualquier momento y sin justificación previa; este también dispone que para su revocación se deberá cumplir los mismos requisitos observados en su otorgamiento, pudiendo ser estos más simples, si así se hubiera señalado en tal oportunidad (Decreto Supremo 003-2013-JUS, 2013). De esta manera, se perdió la oportunidad de garantizar un eficiente y práctico ejercicio del derecho de revocación. Por ejemplo, en España, una llamada a un teléfono gratuito o a los servicios de atención al público del proveedor es suficiente para dejar de recibir comunicaciones con fines promocionales[6], de conformidad con el artículo 21.3 de la Ley Orgánica 3/2018, "cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines" (2018).

Para afrontar este escenario, proponemos una flexibilización de la regulación de datos personales antes comentada para que, en lugar de ser engorrosa, garantice el ejercicio simple y rápido del derecho de acceso, que les permita conocer a los consumidores, principalmente, la fuente de la cual el proveedor o un tercero recopiló sus datos; así como un ejercicio sencillo del derecho de revocación, que por su naturaleza, no debería contar con formalidad alguna. En ese sentido, sugerimos que en el mismo acto en el que el proveedor o tercero se comunique con los consumidores, además de pedir su consentimiento para ofrecerles promociones (de acuerdo con el criterio de la ANDP antes comentado), esté en condiciones de informar directamente la fuente de la cual recogió sus datos personales, especialmente cuando no se obtuvieron directamente, sino de manera indirecta

[6] Para mayor información, véase Agencia Española de Protección de Datos (2021).

por transferencia o por fuente de acceso público, como se ha regulado en la normativa española[7], por ejemplo. Asimismo, recomendamos dar trámite inmediato a las solicitudes de revocación e incluir a los solicitantes en una lista de 'no contacto', lo que además redunda positivamente en la reputación de la compañía.

De esa manera, no resultaría necesario activar el procedimiento de solicitud de ejercicio del derecho de acceso, el que al ser tan engorroso –sumado al desconocimiento– desincentiva su inicio por parte de los consumidores. Asimismo, esto propiciaría la reducción de incumplimientos al literal e) del artículo 58.1 del CPDC, se lucharía más firmemente contra el mercado negro de datos personales, se reduciría el número de denuncias infundadas e impulsaría la presentación de reclamos y denuncias fundamentadas.

VI. TÉNGASE PRESENTE

Brindaremos a continuación algunas sugerencias prácticas para el envío de comunicaciones con fines promocionales, así como para los consumidores.

A. Recomendaciones para proveedores

Sabemos que en el ámbito publicitario es imprescindible que el proveedor o el anunciante llegue a aquellas personas que puedan estar interesadas en sus productos o servicios; sin embargo, surge aquí una problemática derivada de la regulación de protección de datos personales (Fernando, 2005), si esta no es tomada en cuenta en el despliegue de dicha actividad. En ese sentido, es vital estar bien informados al respecto y tener presente las siguientes recomendaciones.

Revisar y contar con una política de privacidad que permita recabar el consentimiento de una manera clara y sencilla; y que posibilite que los consumidores puedan aceptar o rechazar recibir comunicaciones con fines promocionales. Esto incluye que, en los casos en los que los datos sean recopilados de fuentes públicas, se cuente con un protocolo para solicitar el debido consentimiento de los consumidores para la entrega de información promocional; así como asegurarse de aquello ocurra si se tercerizan los servicios de llamadas telefónicas, envío de mensajes de texto y correos electrónicos masivos.

En el supuesto anterior, de utilizarse mensajes de texto o correos electrónicos como medio de contacto, un primer correo deberá servir para recabar el consentimiento, el que, por ejemplo, podrá incluir *links* de suscripción para recibir promociones. En el caso de llamadas telefónicas, el primer contacto estará dirigido a requerir el consentimiento del consumidor, para lo cual será de utilidad contar con la información correcta sobre la fuente de origen de los datos personales, sea en el supuesto de que la haya obtenido de una fuente pública, mediante una transferencia consentida de datos o del propio consumidor.

Una vez que se cuente con el consentimiento para fines promocionales, será de suma importancia almacenar las pruebas o constancias, sea por medio de una grabación o, por ejemplo, guardando los correos electrónicos o suscripciones para recibir promociones. De ese modo, ante un eventual procedimiento sancionador, se podrá afrontar sin dificultades la carga de la prueba.

Por último, sugerimos mantener identificadas a las personas que negaron su consentimiento o lo revocaron, para de ese modo respetar su voluntad y evitar insistir.

B. Recomendaciones para los consumidores

¿Sueles leer o revisar las políticas de privacidad antes de comprar productos o contratar servicios? Probablemente la respuesta sea un tímido 'a veces' o un tajante 'no', y es que esta es una práctica generalizada entre los consumidores, muchas veces a causa de la rapidez de las operaciones comerciales y en otras, por desinterés. Esta situación produce el desconocimiento del propio consumidor, quien puede terminar por presentar una denuncia ante el Indecopi por vulneración del literal e) del artículo 58.1 del CPDC, en la que invertirá tiempo y posibles costos, pero que al final del día será declarada infundada si, en efecto, había otorgado su consentimiento previo para recibir comunicaciones promocionales, como al suscribirse a un concurso o registrado en una tienda *online*, pero no lo recordaba o no había revisado la política de privacidad que aceptó.

[7] De acuerdo con el artículo 11.3 de la Ley Orgánica 3/2018,

> Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 **facilitando a aquel la información básica** señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información. En estos supuestos, la información básica incluirá también:
>
> a) Las categorías de datos objeto de tratamiento.
>
> b) **Las fuentes de las que procedieran los datos** (2018) [el énfasis es nuestro].

En consecuencia, la recomendación más importante para los consumidores es leer. Solo de esa manera tendrán certeza respecto de qué están consintiendo y podrán manifestar su voluntad de manera adecuada; o en su defecto, asumir responsabilidad y aceptar que la ley no ampara el descuido. Como lo indica Alfredo Bullard González, asumir que el consumidor puede ser protegido en cualquier caso, sin importar su nivel de diligencia, es asumir que tendrán una suerte de seguro contra su propia irresponsabilidad brindado por los proveedores (2018). Este escenario claramente no es el deseado, pues, así como es relevante que los proveedores cumplan con las normas de protección al consumidor y de datos personales, también lo es que los consumidores lean la información que reciben y sean conscientes de lo que autorizan.

De otro lado, también es cierto que existe mucho desconocimiento sobre la normativa de protección de datos personales y sobre cómo pueden ser ejercidos los derechos ARCO, lo que puede acarrear que, en lugar de revocar el consentimiento para recibir promociones, se interponga una denuncia ante el Indecopi que carezca de fundamento, en lugar de solicitar la revocación de su consentimiento, por señalar un ejemplo. En atención a esta realidad, es imprescindible el rol que posee la ANDP de realizar campañas de difusión sobre la protección de datos personales, como la denominada '#YoCuidoMisDatosPersonales', que tuvo por objetivo orientar a la población, en especial a niños y adolescentes, sobre cómo proteger su información personal y mostrar las consecuencias negativas del uso inadecuado de las redes sociales.

Finalmente, queremos resaltar la importancia de fomentar una cultura de respeto al tratamiento de datos personales, tanto por parte de los consumidores, quienes deben procurar conocer y ejercer responsablemente sus derechos ARCO; como por parte de los agentes del mercado, quienes requieren desarrollar sus operaciones comerciales en un marco de libertad, pero en cumplimiento de la normativa de datos personales y protección al consumidor, lo que incluso redundará en una mejor imagen corporativa en el mercado.

REFERENCIAS

Agencia Española de Protección de Datos (2021). Publicidad no deseada. https://www.aepd.es/es/areas-de-actuacion/publicidad-no-deseada

Autoridad Nacional de Protección de Datos Personales (2013). *El Derecho Fundamental a la Protección de Datos Personales.* https://cdn.www.gob.pe/uploads/document/file/1401558/El%20derecho%20fundamental%20a%20la%20protecci%C3%B3n%20de%20datos%20personales.pdf

Beneyto, R. (2009). La protección de los datos personales de los consumidores: las listas Robinson. *Computing España, 30.*

Biedma, J., & Medina, J. (2012a). La normativa sobre protección de datos personales: una visión práctica para la empresa. *Revista Partida doble*, (240), 72-85.

(2012b). La normativa sobre protección de datos personales (II): explotación legítima de datos personales. *Revista Partida doble*, (241), 56-69.

Bullard González, A. (2018) ¿Es el Consumidor un Idiota? El Falso Dilema entre el Consumidor Razonable y el Consumidor Ordinario. *Revista de la Competencia y la Propiedad Intelectual*, *6*(10), 5-57.

Carretero Pérez, A., & Carretero Sánchez, A. (1995). *Derecho Administrativo Sancionador*. Editorial de Derecho Reunidas.

El Comercio (24 de enero del 2015). Un imperio de la ilegalidad que vulnera la vida privada de limeños. *El Comercio*. https://cde.3.elcomercio.pe/doc/0/1/0/4/8/1048400.pdf

Espinoza Espinoza, J. (2010). Primeras reflexiones a propósito del Código de Protección y Defensa del Consumidor. *Ius et Veritas*, *20*(41), 164-169.

Fai, K. (3 de diciembre de 2019). Truecaller Insights: Top 20 countries Affected by Spam Salls & SMS in 2019. *Truecaller*. https://truecaller.blog/2019/12/03/truecaller-insights:-top-20-countries-affected-by-spam-calls-&-sms-in-2019/

(8 de diciembre de 2020). Truecaller Insights: Top 20 countries Affected by Spam Calls & SMS in 2020. *Truecaller*. https://truecaller.blog/2020/12/08/truecaller-insights-top-20-countries-affected-by-spam-calls-in-2020-2/

Federal Trade Comission (2021). National Do Not Call Registry FAQs. https://www.consumer.ftc.gov/articles/national-do-not-call-registry-faqs

Fernando, M. (2005). La protección de datos personales en el ámbito de la publicidad en la legislación española. *Revista Chilena de Derecho*, (7), 97-109. http://dx.doi.org/10.5354/0717-9162.2005.10764

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual [Indecopi] (5 de setiembre de 2018). El Poder Ejecutivo, a propuesta del Indecopi, publica DL que modifica el Código de Protección y Defensa del Consumidor para que ciudadanos no reciban promociones de productos y servicios no solicitados [Nota de prensa]. https://repositorio.indecopi.gob.pe/bitstream/handle/11724/6400/NP%20180905%20Mejoras%20al%20C%c3%b3digo%20para%20no%20recibir%20llamadas%20promocionales.pdf?sequence=1&isAllowed=y

Presidencia de Consejo de Ministros (27 de noviembre de 2012). INDECOPI relanza servicio "Gracias… No insista". http://www2.pcm.gob.pe/Prensa/ActividadesPCM/2012/Noviembre/27-11-12-a.html

Sánchez Barrios, M. (2012). *Estudios Sobre Consumo*. Tirant lo Blanch.

Soto Delgado, P. (2017). Sanciones administrativas como medidas de cumplimiento del derecho: un enfoque funcional y responsivo aplicado al régimen sancionatorio ambiental. *Ius et Praxis, 22*(2), 189-226.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Código de Protección y Defensa del Consumidor [CPDC], Ley 29571, Diario Oficial El Peruano, 1 de septiembre de 2010 (Perú).

Comisión de Protección al Consumidor sede Lima Sur, 3 de septiembre de 2010, Resolución Final 2092-2010/CPC, Expediente 2878-2009/CPC (Perú).

Comisión de Protección al Consumidor 3 sede Central, 20 de noviembre de 2019, Resolución 288-2019/CC3, Expediente 067-2019/CC3 (Perú).

Comisión de Protección al Consumidor 3 sede Central, 12 de febrero de 2020, Resolución Final 021-2020/CC3, Expediente 083-2019/CC3 (Perú).

Comisión de Protección al Consumidor 2 sede Central, 4 de agosto de 2020, Resolución Final 981-2020/CC2, Expediente 1112-2019/CC2 (Perú).

Consejo Directivo del Indecopi, 18 de octubre de 2012, Resolución 159-2012-INDECOPI/COD (Perú).

Constitución Política del Perú [Const.] (1993) (Perú).

Decreto Legislativo 1272, Decreto Legislativo que modifica la Ley del Procedimiento Administrativo General y deroga la Ley del Silencio Administrativo, Diario Oficial *El Peruano*, 21 de setiembre de 2016 (Perú).

Decreto Legislativo 1390, Decreto Legislativo que modifica el Código de Protección y Defensa del Consumidor, Diario Oficial *El Peruano*, 5 de setiembre de 2018 (Perú).

Decreto Supremo 006-2009-PCM, Decreto Supremo que aprueba el Texto Único Ordenando de la Ley del Sistema de Protección al Consumidor, Diario Oficial *El Peruano*, 30 de enero de 2009 (Perú).

Decreto Supremo 003-2013-JUS, Decreto Supremo que aprueba el Reglamento de la Ley de Protección de Datos Personales, Diario Oficial *El Peruano*, 22 de marzo de 2013 (Perú).

Decreto Supremo 004-2019-JUS, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley del Procedimiento Administrativo General, Diario Oficial *El Peruano*, 25 de enero de 2019 (Perú).

Directiva 005-2009/COD-INDECOPI, Directiva de Operación y Funcionamiento del Registro de Números Telefónicos y Direcciones de Correo Electrónico Excluidos de ser destinatarios de publicidad Masiva "Registro Gracias… No Insista", 16 de setiembre de 2009 (Perú).

Exposición de Motivos del Decreto Legislativo 1390, 05 de septiembre de 2018 (Perú).

Ley 29733, Ley de Protección de Datos Personales, Diario Oficial *El Peruano*, 2 de julio de 2011 (Perú).

Ley Orgánica 3/2018, Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (B.O.E. 2018, 3) (Esp.).

Ministerio de Justicia y Derechos Humanos, 14 de marzo de 2018, Oficio 146-2018-JUS/DGTAIPD (Perú).

Ministerio de Justicia y Derechos Humanos, 19 de febrero de 2019, Opinión Consultiva 12-2019-JUS/DGTAIPD (Perú).

Sala Especializada en Protección al Consumidor sede Lima Sur, 25 de marzo de 2013, Resolución 0728-2013/SPC-INDECOPI, Expediente 40-2012/CPC (Perú).

Sala Especializada en Protección al Consumidor sede Lima Sur, 13 de octubre de 2015, Resolución 32352015/SPCINDECOPI, Expediente 643-2014/CC2 (Perú).

Sala Especializada en Protección al Consumidor sede Junín, 30 de mayo de 2016, Resolución 19312016/SPCINDECOPI, Expediente 592015/CPCINDECOPIJUN (Perú).

Sala Especializada en Protección al Consumidor sede Lima Sur, 8 de abril de 2019, Resolución 0943-2019/SPC-INDECOPI, Expediente 1459-2017/CC2 (Perú).

Sala Especializada en Protección al Consumidor sede Lima Sur, 10 de marzo de 2021, Resolución 0542-2021/SPC-INDECOPI, Expediente 0174-2019/CC3-SIA (Perú).

10.18800/themis.202101.023

GOBIERNO CORPORATIVO EN TIEMPOS DE *VENTURE CAPITAL*

CORPORATE GOVERNANCE IN TIMES OF VENTURE CAPITAL

José Miguel Porto Urrutia*
Exmiembro de THĒMIS
Porto Legal

The importance of having good corporate governance policies that respond to the particularities of the company is indisputable, especially in capital structures (such as startups), whose special dynamics in the industry (of venture capital) generate a high risk of harming the interests of disadvantaged groups (such as minority shareholders). In addition, there is a risk of unduly influencing management, due to the privileged position that certain groups hold (such as investors with a high financial capacity).

In this order of ideas, this article exposes the challenges and complexities that the venture capital industry is going through, mainly in the Peruvian startup market. Likewise, the author analyzes some proposals for good corporate governance, in order to outline a starting point in the search for practices and policies that allow the consolidation of the figure in the country.

Keywords: Venture capital; startups; partnership; board of directors; management; shareholders.

Es indiscutible la importancia de contar con políticas de buen gobierno corporativo que respondan a las particularidades de la sociedad; sobre todo, en estructuras de capital (como las startups*), cuya dinámica especial en la industria (del* venture capital*) genera un alto riesgo de vulnerar los intereses de grupos en desventaja (como lo son los accionistas minoritarios). Así como también, existe el riesgo de influenciar indebidamente la gestión en razón de la posición privilegiada que determinados grupos detentan (como lo son los inversionistas con alta capacidad financiera).*

En ese orden de ideas, el presente artículo expone los retos y complejidades que atraviesa la industria del venture capital*, fundamentalmente en el mercado de* startups *peruano. Asimismo, el autor analiza algunas propuestas de buen gobierno corporativo, a efectos de trazar un punto de partida en la búsqueda de prácticas y políticas que permitan la consolidación de la figura en el país.*

Palabras clave: Capital de riesgo; startups*; sociedad; directorio; gerencia; accionistas.*

* Abogado. Master of Laws (LL.M.) por la Universidad de Chicago. Socio fundandor de Porto Legal (Lima, Perú). Contacto: jporto@porto.legal

Nota del Editor: Este artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 10 de enero de 2021, y aceptado por el mismo el 4 de agosto de 2021.

I. INTRODUCCIÓN

La industria de capital de riesgo (*venture capital*) continúa madurando en el mercado peruano y sus particularidades nos hacen preguntarnos sobre las mejores prácticas de gobierno corporativo que debieran aplicarse a la misma. Las *startups*, que se encuentran al centro de esta industria, cuentan con una dinámica y estructura de capital especiales que las diferencian de las estructuras convencionales; situándose entre el modelo corporativo americano con capital difundido, y el modelo peruano con capital concentrado y familiar. En este artículo, nos referiremos a los retos y complejidades que se presentan en la industria de *venture capital* peruana. Además, revisaremos algunas propuestas para incorporar criterios de buen gobierno corporativo que sirvan para incrementar la eficiencia, competitividad y valorización de las *startups;* así como facilitar los esfuerzos de levantamiento de capital.

II. LA RUTA DEL FINANCIAMIENTO

El mercado peruano muestra una particularidad: la disponibilidad de financiamiento en estadios tempranos del emprendimiento, como es el caso de las rondas de inversionistas previos a las series A (usualmente lideradas por fondos de *venture capital* y por montos en exceso de un millón de dólares americanos)[1]. Sumado a ello, el Perú cuenta con una población de dimensiones atractivas (ni muy pequeña como la chilena, ni muy grande como México o Brasil) y centralizada (la mayor parte de la actividad económica se encuentra concentrada en Lima y otras pocas ciudades de la costa). Esto hace atractivo al Perú para emprender, porque el nivel de inversión para obtener un producto mínimo viable que resulte escalable es menor que en otras plazas latinoamericanas con poblaciones mayores y economías descentralizadas.

Naturalmente, al demostrar la viabilidad de un producto o servicio en el mercado peruano, el siguiente paso es el escalamiento en Perú y luego a otros mercados con gran masa de consumidores (como podrían ser México y Brasil). Estas características deberían determinar que la actividad de las *startups* continúe incrementándose en el país.

No obstante, la deficiencia del mercado peruano es la escasez de fondos de *venture capital*[2] con operaciones locales y dispuestas a invertir en *startups* constituidas en el Perú. Por ello, el camino de las *startups* peruanas tiende a llevarlas hacia Estados Unidos (específicamente Delaware, que es la jurisdicción de preferencia de los fondos de *venture capital*) para constituir una matriz como vehículo donde se reciben las inversiones en series A y posteriores.

A medida que la *startup* avanza a lo largo de la 'ruta del financiamiento', completará hitos (la etapa de validación, temprana, crecimiento, consolidación y salida) y, con cada fase, la valorización de la *startup* incrementará, al igual que la capacidad de sus fundadores para levantar financiamiento adicional en lo que se denominan 'rondas de inversión'. Con cada levantamiento de capital, los fundadores verán diluida proporcionalmente su participación en el capital social. Es por ello que la ruta del financiamiento es también una carrera contra la dilución, donde los fundadores deben diluirse estratégica y voluntariamente para lograr levantar capital en estadios posteriores.

En cada ronda de inversión tendremos inversionistas que financiaron la *startup*, ya sea con instrumentos de deuda, opciones o inversiones de capital, que requerirán a cambio, entre otros, mejoras en las políticas de gobierno corporativo, como la conformación de directorios con participación de los inversionistas. Es así que, a medida que los fundadores van levantando capital y siguen la ruta de financiamiento, el gobierno corporativo de la *startup* tendrá que robustecerse, no solo para mantenerse competitiva y acceder a financiamiento, sino también por exigencia de los inversionistas. El Gráfico 1 detalla la ruta del financiamiento.

III. LA ESTRUCTURA DE CAPITAL DE LAS *STARTUPS*

A medida que el emprendimiento navega por las complejidades de la ruta del financiamiento, los fundadores se van diluyendo en el capital social y entran nuevos inversionistas. Esto genera una dinámica particular en las *startups* que vale la pena considerar:

---

1 Si bien, de acuerdo a la terminología de Crunchbase (2021), una serie A es aquella entre los uno a treinta millones de dólares, en nuestro mercado las rondas de inversión son más modestas y se tiene que una serie A es aquella en la que se obtiene financiamiento por encima del millón de dólares. Véase la definición en la página web de Crunchbase.

2 En este sentido, se vienen realizando esfuerzos a través del gobierno peruano para cerrar esta brecha. Un primer paso fue el otorgamiento a Salkantay Partners de fondos no reembolsables para lanzar el primer fondo de *venture capital* peruano. Asimismo, también se encuentra el lanzamiento de parte de la Corporación Financiera de Desarrollo (COFIDE) del Fondo de Capital para Emprendimientos Innovadores (FCEI), el cual invertirá en fondos de capital de riesgo en la Alianza del Pacífico.

Gráfico 1: La ruta del financiamiento

Fuente: Elaboración propia

(i) El capital se encontrará concentrado en las manos de los fundadores.

(ii) Los fundadores mantendrán el control y la administración de la *startup*.

(iii) A diferencia de estructuras como el modelo corporativo peruano, en donde la propiedad y la administración se encuentran en manos de grupos familiares adinerados, en la *startup*, los fundadores, en la mayoría de los casos, no cuentan con los recursos económicos para financiar personalmente el crecimiento de la *startup* a lo largo de la ruta del financiamiento. Asimismo, la *startup* usualmente tampoco estará en capacidad de generar crecimiento orgánico con fondos propios (existe un periodo de tiempo necesario para que la misma madure, llegue a un punto de equilibrio y, aun cuando lo logre, no se sabe si los flujos serán suficientes para continuar con el proceso de expansión y crecimiento agresivo que suelen tener las *startups*).

(iv) Los inversionistas usualmente tendrán un rol pasivo.

(v) Usualmente la *startup* no tendrá un directorio, salvo en los casos en los que exista un inversionista que realice una inversión considerable y exija encontrarse representado en el directorio.

(vi) Los inversionistas, ya sea que se trate de fondos de *venture capital* o inversionistas ángeles, tienen una ventana de tiempo de inversión, pero, en cualquier caso, buscan liquidar sus posiciones en el corto plazo para hacer una ganancia.

(vii) Algunos inversionistas (como podrían ser los corporativos) podrían estar buscando liquidar posiciones (a cambio de una ganancia) o estar interesados en invertir en *startups* como mecanismo para encontrarse vigentes, cerca de los avances tecnológicos y disruptivos de la industria, así como para conocer, de la mano de la *startup*, las complejidades que se presentan en la transición del mundo analógico al digital.

Esta estructura de capital en donde no hay una clara división entre la propiedad y la administración hace que los fundadores puedan vulnerar los intereses de los accionistas minoritarios (inversionistas). Sin embargo, al ser los inversionistas quienes tienen acceso al capital para continuar financiando la *startup*, se genera una dinámica especial de cierta dependencia en donde resulta importante que los inversionistas no utilicen su privilegiada posición financiera para influenciar indebidamente en la gestión de la *startup*, más aún cuando cuenten con sitios en el directorio.

IV. GOBIERNO CORPORATIVO Y LOS PROBLEMAS DE AGENCIA

El gobierno corporativo es la forma cómo la sociedad distribuye los roles y responsabilidades, así como el sistema de chequeos y balances entre el directorio, la gerencia, los accionistas y cualquier otro grupo con legítimo interés en la empresa para producir una compañía de funcionamiento eficiente, orientada idealmente a generar valor en el largo plazo (Loncharich, 2005). Las principales instituciones involucradas son los accionistas (reunidos en junta general), el directorio (designado por los accionistas) y la gerencia (designada por el directorio de la sociedad).

Al centro de las discusiones sobre la implementación de políticas de buen gobierno corporativo, se encuentran los problemas de agencia, que típicamente se generan cuando un agente debe velar por los intereses de terceros. Al respecto, los economistas Michael Jensen y William Meckling argumentaron que los gerentes profesionales quienes trabajan como agentes de los propietarios de la empresa, tienen incentivos para cuidarse a sí mismos en lugar de a los propietarios. La gerencia, por ejemplo, podría prodigarse beneficios que no favorecen directamente a la empresa, ni a sus propietarios reales (O'Reilly, 2017, pp. 240-241).

Coincidimos con Martínez Ortiz (2014) cuando señala que el gobierno corporativo tiene dos dimensiones del problema de agencia: la **dimensión vertical** y la **dimensión horizontal**. La dimensión vertical se presenta en el modelo capitalista, en específico en Estados Unidos, donde existe una clara separación entre la propiedad y el control de las sociedades. Allí el capital se encuentra diluido entre una gran cantidad de accionistas, donde ninguno de ellos muestra incentivos por supervisar, fiscalizar o monitorear a los administradores de la sociedad (sea que se trate del directorio o la gerencia).

De otro lado, la dimensión horizontal refiere a problemas de agencia generados cuando no existe una clara separación entre la propiedad y el control, donde los socios mayoritarios toman control del directorio y la gerencia, actuando en perjuicio de los accionistas minoritarios. En estos casos se advierte que la propiedad y el control recaen en manos del accionista controlador, siendo, en el caso peruano, un grupo familiar con una importante capacidad adquisitiva (Martínez Ortiz, 2014, pp. 99-100).

V. DE LA ADMINISTRACIÓN DE LAS *STARTUPS*

Las *startups* generalmente se constituyen como sociedades anónimas cerradas (sin directorio) y solo cuando sus inversionistas lo exigen se crea un directorio. La administración de una *startup* se rige por lo establecido en el artículo 152 de la Ley 26887, Ley General de Sociedades (en adelante, LGS), el cual señala que: "**[l]a administración de la sociedad está a cargo del directorio y de uno o más gerentes, salvo por lo dispuesto en el artículo 247**[3]" (1997) [el énfasis es nuestro].

Como señala Salas Sánchez, "[n]o se aprecia una clara delimitación de las competencias de uno y otro órgano social, salvo las referidas a la jerarquía y a la atribución del gerente general respecto de los actos y contratos ordinarios" (2005, p. 3). En ese mismo sentido, el Anteproyecto de la Ley General de Sociedades[4] (en adelante, el Anteproyecto) y el Código de Buen Gobierno Corporativo para las Sociedades Peruanas señalan que resulta necesario asignarle al directorio de las sociedades un rol estratégico y estructural de la sociedad, el cual supervise y controle a la gerencia; delegando en la gerencia la gestión ordinaria de la sociedad (Ministerio de Justicia y Derechos Humanos, 2021, p. 283; 2013).

En ese sentido, el principio 16 del Código de Buen Gobierno Corporativo para las Sociedades Peruanas propone que

> **El Directorio tiene como función aprobar y dirigir la estrategia corporativa de la sociedad; establecer objetivos, metas y planes de acción, incluidos los presupuestos anuales y los planes de negocios; controlar y supervisar la gestión; así como encargarse del gobierno y la administración de la sociedad**. Es función del Directorio supervisar las prácticas de buen gobierno corporativo y establecer las políticas y medidas necesarias para su mejor aplicación (2013) [el énfasis es nuestro].

Luego, el principio 24 del mismo código señala que: "[e]xiste separación entre la administración o gobierno ejercido por el Directorio, **la gestión ordinaria a cargo de la Alta Gerencia y el liderazgo del gerente general**, mediante una política clara de delimitación de funciones […]" (Código de Buen Gobierno Corporativo para las Sociedades Peruanas, 2013) [el énfasis es nuestro].

De acuerdo a ello, se sugiere que una adecuada estructura de buen gobierno corporativo delimite claramente la responsabilidad de cuestiones estratégicas de la sociedad en el directorio, mientras que la gerencia se ocupará de la gestión ordinaria del negocio.

A. Del comportamiento de los directores

Nuestra LGS detalla ciertos deberes que los directores de la sociedad deben tener al ejercer su cargo.

---

3 Artículo 247.- Directorio facultativo

En el pacto social o en el estatuto de la sociedad se podrá establecer que la sociedad no tiene directorio. Cuando se determine la no existencia del directorio todas las funciones establecidas en esta ley para este órgano societario serán ejercidas por el gerente general (Ley 26887, 1997).

4 El Anteproyecto es un trabajo liderado desde el año 2014 por el Ministerio de Justicia y Derechos Humanos, y elaborado por un grupo de trabajo de destacados profesionales. Este fue presentado el pasado 27 de mayo de 2021 con el objetivo de realizar ciertos ajustes y modificaciones a la actual LGS.

El artículo 171 de la LGS establece que

> **Los directores desempeñan el cargo con la diligencia de un ordenado comerciante y de un representante leal.** Están obligados a guardar reserva respecto de los negocios de la sociedad y de la información social a que tengan acceso, aun después de cesar en sus **funciones** (Ley 26887, 1997) [el énfasis es nuestro].

Como señala Elías Laroza, la LGS no define ni desarrolla el significado de ejercer el cargo con la "**diligencia de un ordenado comerciante**" y tampoco de **"representante leal"**, señalando que se encuentran referidas a normas de conducta que los directores deberán cumplir (1998, p. 343) [el énfasis es nuestro]. Adicionalmente, el Anteproyecto señala que el director debe tener un nivel de dedicación adecuado para la responsabilidad que asume (Ministerio de Justicia y Derechos Humanos, 2021). Se concluye así que los directores tienen dos deberes de conducta a seguir: el deber de diligencia y el de lealtad.

1. Deber de diligencia

Tratándose de una norma de conducta, no nos encontramos ante una norma de resultado. El director no es responsable por las malas decisiones que tome y su diligencia no es definida por el resultado de las mismas, sino por la forma cómo se tomaron las decisiones al interior de la sociedad. La LGS no requiere que los directores sean infalibles, sino que trabajen diligente y ordenadamente, como lo haría un comerciante, valga la redundancia, 'diligente y ordenado'. Así, lo más relevante no es el resultado final de las decisiones del directorio (acertadas o no), sino que se analiza la forma cómo los directores adoptaron la decisión.

Otra forma de ver el deber de diligencia es como mecanismo de protección. Un director que toma una mala decisión no estaría infringiendo su deber de diligencia, si procuró obtener la mayor información disponible y veraz sobre la decisión a tomar (reconociendo las limitaciones de tiempo e información disponible que siempre se producen al tomar decisiones); si existió un debate riguroso donde el directorio exploró diversas opciones, en el que se debatieron los puntos a favor y en contra de la decisión; si se recurrió a la opinión de expertos en la materia cuando el tema o decisión así lo requería, entre otros. Opinamos que el fondo de las decisiones adoptadas por el directorio no merece revisión, y que cualquier disputa con los acuerdos del directorio se debería centrar en la forma en cómo se adoptó el acuerdo y no en el acuerdo *per se,* salvo cuando el fondo sea contrario a ley.

2. Deber de lealtad

¿A quién le debe lealtad el director? Esta no es una respuesta sencilla, ya que la sociedad tiene diversos actores a los cuales el director podrá deberles lealtad. ¿Acaso son los accionistas, la sociedad, los trabajadores, sus proveedores, el medio ambiente o la comunidad? Veamos algunos modelos a continuación.

a. *El modelo norteamericano*

Milton Friedman, ganador del Premio Nobel de Economía, ensayó la doctrina de primacía de los accionistas, en virtud de la cual las sociedades tienen como fin último maximizar el retorno de los accionistas. La Corte Suprema del Estado de Delaware, en el caso Revlon (*Revlon, Inc. c. MacAndrews & Forbes Holdings*, 1986), estableció que los intereses de los accionistas siempre deben prevalecer por sobre los intereses de cualquier otro, salvo en procesos de quiebra o disolución, en donde se debe considerar los intereses de terceros ajenos a los accionistas (citada en Cole, 2019, p. 9).

Como las sociedades se encuentran en el centro del modelo capitalista, el modelo planteado por Friedman genera descontento al incentivar un modelo económico que pudiera resultar codicioso, egoísta o corrupto (Collier, 2018, p. 77). De esta manera, muchos cuestionan si el modelo de primacía de los accionistas es el más adecuado para el modelo capitalista. En ese sentido, el precedente es cuestionado por producir excesos en el modelo capitalista cuando el fin último del directorio, y por ende de las sociedades, es maximizar los retornos para los accionistas sin consideraciones adicionales.

Bajo este modelo, podría argumentarse que un directorio que destine recursos para proteger el medio ambiente, los derechos de los trabajadores o a la comunidad en la ejecución de sus negocios podría afectar adversamente los ingresos de los accionistas y ser sujeto a una acción por incumplimiento al deber de lealtad.

b. *El modelo peruano*

En nuestra legislación, el artículo 173 de la LGS establece que

> Cada director tiene el derecho a ser informado por la gerencia de todo lo relacionado con la marcha de la sociedad. Este derecho debe ser ejercido en el seno del directorio y de manera de no afectar la gestión social.
>
> **Los directores elegidos por un grupo o clase de accionistas tienen los mismos deberes para**

> **con la sociedad y los demás accionistas que los directores restantes y su actuación no puede limitarse a defender los intereses de quienes los eligieron** (Ley 26887, 1997) [el énfasis es nuestro].

Claramente, el legislador ha establecido que los directores no pueden limitarse a defender los intereses de los accionistas que los eligieron y tienen un deber de lealtad hacia todos los accionistas de la sociedad; con lo cual sus decisiones no pueden limitarse a beneficiar al grupo de accionistas que los designó. Notemos que dicho artículo señala además que los directores tienen un deber fiduciario hacia la sociedad.

Ello es ratificado luego por el artículo 180 de la LGS que establece que

> **Los directores no pueden adoptar acuerdos que no cautelen el interés social sino sus propios intereses o los de terceros relacionados**, ni usar en beneficio propio o de terceros relacionados las oportunidades comerciales o de negocios de que tuvieren conocimiento en razón de su cargo. No pueden participar por cuenta propia o de terceros en actividades que compitan con la sociedad, sin el consentimiento expreso de ésta […] (Ley 26887, 1997) [el énfasis es nuestro].

El artículo 180 de la LGS establece, entonces, una obligación de no hacer, de manera que en ningún caso el director puede adoptar acuerdos que perjudiquen los intereses sociales, aun si estos acuerdos pueden beneficiar a los accionistas de la sociedad (y no solo a aquellos que los designaron). Así, los directores podrán defenderse contra cualquier acción individual de responsabilidad por parte de los accionistas que consideren vulnerados sus intereses, siempre que justifiquen su decisión de acuerdo con los mejores intereses de la sociedad.

En conclusión, el director debe velar en primera instancia por los intereses de la sociedad, no pudiendo en ningún caso adoptar acuerdos que perjudiquen el interés social. En ese sentido, nuestra LGS se aleja del principio de primacía de los accionistas que sostenía Milton Friedman y que la comunidad internacional viene cuestionando. En segunda instancia, el director debe velar por los intereses de todos los accionistas, y no únicamente de los accionistas que lo designaron[5].

c. *Las nuevas tendencias*

Existe una tendencia en el sector empresarial americano que rechaza la doctrina de primacía de los accionistas, para encontrar sostenibilidad en el largo plazo mediante la incorporación de los intereses de terceros distintos a los accionistas de la sociedad. Iniciativas como el Business Roundtable[6] procuran integrar al desarrollo social los intereses de los consumidores, los proveedores, los trabajadores, la comunidad y el retorno de los accionistas en el largo plazo[7]. Parece ser que la visión empresarial y social está cambiando, que la doctrina de primacía de los accionistas ha generado amplia insatisfacción y que resulta conveniente explorar nuevas opciones de gobierno corporativo.

En esa misma línea, se viene produciendo un cambio dramático hacia la incorporación del criterio Environmental, Social and Governance (en adelante, ESG) como enfoque de inversiones, en donde los fondos haciendo inversiones buscan medir y reportar factores ambientales, sociales y de buen gobierno corporativo en las empresas en las cuales invierten (Palacios, 2021).

Estas nuevas tendencias parecieran ir más allá de la primacía de los accionistas o de velar por los intereses sociales para dar cada vez mayor importancia a intereses ajenos a la sociedad, como podría ser el impacto que tienen las empresas principalmente en el medio ambiente y en la sociedad. Esto resulta relevante, dado que, si los fondos de inversión incorporan estos criterios en sus políticas de inversión, el impacto sería inmediato en las em-

---

5 En la misma línea, el Anteproyecto establece en el artículo 148 que

1. El director desempeña el cargo con la lealtad de un representante leal, obrando de buena fe y en el mejor interés de la sociedad, procurando evitar incurrir en conflicto de interés. […]
3. Cada director tiene el mismo deber de lealtad para con la sociedad con independencia del accionista o accionistas con cuyo voto haya sido elegido. 4. La actuación del director no debe estar destinada a promover o defender los intereses de los accionistas que los eligieron o de las personas vinculadas a estos o al propio director (Ministerio de Justicia y Derechos Humanos, 2021).

6 Véase Business Roundtable Corporation (2020).

7 En ese sentido, Tim Cook, en una entrevista en The David Rubenstein Show, señaló que ellos "manejan Apple a largo plazo" (Bloomberg, 2018). Por otro lado, en una edición de la revista The Economist dedicada a Negocios, se señaló que Walmart, que encarnó la doctrina de la primacía de los accionistas, "acabó con una reputación de precios bajos para los consumidores y maltrato a los proveedores y trabajadores" (2020) [traducción libre]. Así, Walmart ha buscado limpiar esa imagen procurando defender otros intereses como podrían ser los de la comunidad gay y migrar hacía energías renovables. Walmart también acabó con la venta de municiones y armas luego de un tiroteo en una de sus tiendas y

presas invertidas, las cuales tendrían que adecuar sus modelos de gobierno corporativo para proteger intereses que van más allá del de los accionistas y de la sociedad, y asegurar que, al hacerlo, no vulneren las disposiciones de las leyes locales aplicables.

3. De la responsabilidad de los directores

La LGS establece ciertas responsabilidades para aquellos directores que no cumplan con el deber de lealtad y diligencia. Al respecto, el artículo 177 de la LGS establece que

> **Los directores responden, ilimitada y solidariamente, ante la sociedad, los accionistas y los terceros por los daños y perjuicios que causen por los acuerdos o actos contrarios a la ley, al estatuto o por los realizados con dolo, abuso de facultades o negligencia grave** [...] (Ley 26887, 1997) [el énfasis es nuestro].

Si concluimos que, si un director adopta un acuerdo en beneficio de los accionistas, el cual vulnera los intereses de la sociedad, resulta contrario a lo establecido en el artículo 180 de la LGS, y, por ende, corresponde que dicho director responda en forma ilimitada y solidariamente ante la sociedad por los daños y perjuicios causados; entonces cualquiera que asume el rol de director en una sociedad debe estar seguro de contar con la asesoría legal adecuada para asesorarse ante este tipo de contingencias.

B. Del comportamiento de los gerentes y los accionistas

Nótese que bajo la LGS no se exigen estándares de conducta a los gerentes, ni a los accionistas de la sociedad. De esta manera, ni el accionista ni el gerente deben a la sociedad un deber de lealtad ni de diligencia como el que resulta aplicable a los directores. En ese sentido, los accionistas sí pueden votar en junta general de accionistas para defender sus intereses propios, y en contra del interés social y de terceros sin perjuicio alguno.

En el caso de la gerencia, si bien no existe un estándar de conducta que resulte aplicable, la LGS establece en su artículo 190 que "**el gerente responde ante la sociedad, los accionistas y terceros, por los daños y perjuicios que ocasione por el incumplimiento de sus obligaciones, dolo, abuso de facultades y negligencia grave**" (Ley 26887, 1997) [el énfasis es nuestro]. En otras palabras, el gerente no tiene un deber de lealtad ni de diligencia como parámetro de conducta para sus actividades y solo resulta responsable cuando la sociedad esté en capacidad de acreditar que incumplió sus obligaciones, abuso de sus facultades, o actuó con dolo o negligencia grave.

Para cubrir dicho vacío, el principio 24 del Código de Buen Gobierno Corporativo para las Sociedades Peruanas extiende los deberes de diligencia, lealtad y reserva del directorio a los gerentes (2013). En ese sentido, el Anteproyecto, en su artículo 166, extiende a los gerentes los deberes de lealtad y diligencia aplicables a los directores (Ministerio de Justicia y Derechos Humanos, 2021).

VI. PROBLEMÁTICA DE BUEN GOBIERNO CORPORATIVO EN LA INDUSTRIA DE VENTURE CAPITAL

Las disposiciones de buen gobierno corporativo deben ajustarse a las necesidades del mercado y la industria. No cabe duda de que la implementación de prácticas y procedimientos que reflejen un buen gobierno corporativo son importantes para lograr la competitividad de la empresa en el sector, maximizar el potencial de la sociedad para alcanzar metas y objetivos trazados, incrementar la valorización de la sociedad, y acceder a fuentes de financiamiento en las mejores condiciones.

Como señalan algunos, en el mundo corporativo peruano, en donde no existe una clara diferencia entre la propiedad y el control, los principales problemas de agencia se manifiestan como problemas horizontales, en los que el énfasis parte por proteger a los accionistas minoritarios de los accionistas que controlan y administran las sociedades (Martínez Ortiz, 2014, p. 102). En el caso de *venture capital*, mientras las *startups* operen sin la presencia de una casa matriz en Delaware, vale la pena discutir un marco de buen gobierno corporativo que debiera incorporarse en documentos que vinculen a la sociedad y a los administradores con los demás accionistas. Creemos que la evaluación y maduración de la *startup* requerirá que las políticas de buen gobierno corporativo se vayan ajustando a medida que la *startup* va avanzando en la ruta del financiamiento y va levantando capital.

A. Etapa de validación

Como suele ocurrir en este estadio, las inversiones individuales no son significativas y los inversionis-

procurando que el gobierno incremente el control en la venta de armas, todo ello en contra del *lobby* del National Rifle Association en USA (una de las asociaciones más poderosas de los Estados Unidos) (The Economist, 2020).

tas no tienen incentivos suficientes para dedicar tiempo a la supervisión de la administración de la *startup*. Los inversionistas suelen ser personas cercanas a los fundadores como amigos y familiares. Desde el punto de visto del gobierno corporativo, las principales complejidades son: (i) lograr el involucramiento de inversionistas en la gestión de la *startup*; (ii) que la sociedad mantenga debidamente informados a los inversionistas sobre la gestión de la sociedad; y (iii) la defensa de los intereses de los accionistas minoritarios (inversionistas) ante los accionistas controladores y administradores (fundadores). En esta etapa, los problemas de agencia son principalmente horizontales y pueden ser atendidos mediante los siguientes mecanismos:

(i) ***Smart-money***: Al levantar financiamiento, la *startup* debe buscar un perfil de inversionista que desee involucrarse en el proceso de toma de decisiones o que traiga experiencia previa en la industria que se pudiera apalancar.

(ii) **Acceso a información**: Que la *startup* tenga un sistema de reportería periódico entre inversionistas con los principales indicadores de la industria específica y demás información relevante del mercado para inversionistas.

(iii) **Comité de gestión**: La *startup* debería contar con un comité de gestión con representación de los inversionistas, donde los fundadores puedan discutir los principales retos y acciones a tomar. Sería un espacio de retroalimentación de los inversionistas para los fundadores y, a su vez, un espacio informal donde los fundadores rendirán cuenta sobre sus acciones y decisiones a los inversionistas.

(iv) **Código de conducta**: En la medida de que los fundadores continuarán desarrollando un negocio con dinero de terceros, es importante fortalecer sus deberes fiduciarios a fin de garantizar que también se adhieran a los deberes de conducta de diligencia y lealtad que resultan aplicables a los directores de las sociedad. De esta manera, se podrá mitigar potenciales situaciones de conflicto, en donde se privilegien los intereses de los fundadores controladores por encima de los accionistas minoritarios o inversionistas. Esto podría lograrse mediante la aprobación de un código de conducta de la *startup* al cual se adhieren los colaboradores y que los guíe en la gestión ordinaria de la sociedad.

B. Etapa temprana

En la etapa previa a la entrada de fondos de *venture capital* en el capital social de la sociedad, advertimos la presencia de inversionistas ángeles e inversionistas capitalistas más sofisticados en la *startup*. También encontramos inversionistas corporativos que incrementan cada vez más su participación en la inversión en *startups*. Sobre la base de los montos financiados, aquel que lidere la ronda de inversión y para inversiones que pudieran resultar materiales (usualmente mayor a US$ 500 000), vemos la exigencia de los inversionistas por participar en los directorios de la sociedad, o en su defecto, participar de manera más activa en el proceso de toma de decisiones de la *startup*.

Para aquellas *startups* que lleguen a esta etapa habiendo implementado las medidas de reportería y de rendición de cuentas a los inversionistas contempladas en la sección V.A, gran parte del trabajo estará completado. Sin embargo, el punto de mayor fricción pudiera ser la entrega de sitios en el directorio a los inversionistas.

En aquellos casos donde los inversionistas solicitan sitios en el directorio de la *startup*, advertimos que algunos emprendedores muestran preocupación por concederlos. Si bien los acuerdos en directorio se adoptan por mayoría, no se debe subestimar la influencia que pueden tener directores sofisticados. No debemos olvidar una dinámica particular en las *startups* y es que los inversionistas podrían estar en capacidad de financiarlas, y utilizar su disponibilidad de recursos para influenciar indebidamente la gestión para beneficio propio. Así, creemos que la preocupación tiene mérito en la medida que consideremos que esos directores designados por los inversionistas empujen agendas propias en perjuicio de la sociedad[8].

Cada directorio tiene una dinámica especial. Es posible que un director con el conocimiento y las relaciones adecuadas influya en el proceso de toma de decisiones, al ser el directorio el lugar indicado

[8] Este es un problema que se repite en todas las industrias como podremos advertir de los casos de Disney y de inversionistas activistas que citamos a continuación:

Caso Disney: Cuenta Robert Iger que cuando asumió el cargo de CEO de Disney, las relaciones entre Disney y Pixar estaban muy deterioradas. La disputa, más que corporativa, era personal entre Steve Jobs (CEO de Pixar y Apple por aquel entonces) y Michael Eisner, por aquel entonces CEO de Disney. Cuando Iger asume el cargo de CEO de Disney en reemplazo de Eisner, acuerda con Steve Jobs la adquisición de Pixar por parte de Disney. Eisner se opuso firmemente a la adquisición alegando, entre otras cosas, que Steve Jobs tendría una influencia perjudicial en el directorio de Disney

para influir en la toma de decisiones de la sociedad sin asumir un rol gerencial.

Por ejemplo, en los Estados Unidos los inversionistas activistas, aun sin contar con mayoría en el directorio, designan directores sofisticados con un alto conocimiento de la industria y experiencia corporativa previa en el manejo de relaciones dentro del directorio (entre el directorio y los principales inversionistas, así como entre el directorio y la gerencia), para promover los cambios y mejoras estructurales necesarios, así como un equipo de trabajo que los respalda en el procesamiento de información antes de las sesiones de directorio (Walker, 2016, pp. 169 & 208), pudiendo estar mejor informados que otros directores que no cuentan con ese soporte para sustentar sus puntos de vista y convencer a los otros directores.

En cualquier caso, estamos a favor de la representación de inversionistas en los directorios, así como de terceros independientes. Sin perjuicio de ello, para evitar posibles interferencias perjudiciales de los inversionistas, sugerimos la implementación de las siguientes medidas:

(i) **Reglamento del directorio**: Alineado con la recomendación del principio 18 del Código de Buen Gobierno Corporativo para las Sociedades Peruanas (2013), es recomendable contar con un reglamento de directorio que contenga las políticas y procedimientos de funcionamiento, de cumplimiento obligatorio, y que permita sancionar o reemplazar, mediante proceso expeditivos, a directores que incumplan con los deberes de diligencia y lealtad establecidos en la ley. Se tendrá que evaluar la posibilidad de que la sociedad también tome en consideración intereses de terceros, como es el caso de la incorporación de las ESG en el proceso de toma de decisiones.

(ii) **Independencia de los directores**: Los directores designados por los inversionistas se encontrarán ante situaciones complejas, dado que, por un lado, los inversionistas que los designaron esperan que ellos protejan sus intereses en la *startup*, y por el otro, los deberes de diligencia y lealtad que la ley les impone no les permiten privilegiar los intereses de estos inversionistas. La situación más compleja que se presenta es cuando un inversionista designa como su representante en un directorio a uno de sus trabajadores. Evidentemente, aquel director designado, por su relación de dependencia con el inversionista, solo puede proteger, bajo los términos de su relación laboral, los intereses de su empleador. Queda claro el conflicto de interés que se produce en estos casos, por lo que siempre debe procurarse que los representantes de los inversionistas en el directorio sean, de preferencia, terceros ajenos a la organización del inversionista[9]. Lo ideal sería que los inversionistas pudieran designar a un tercero independiente que los pudiera representar en el directorio de la *startup* y así mitigar potenciales conflictos de interés.

(iii) **De la función del directorio en una *startup***. Creemos importante tener en cuenta que el directorio tiene que trabajar para el fundador, gerente general o CEO. Si bien la estrategia de la sociedad debe recaer en el directorio, es el fundador, gerente general o CEO quien se encuentra en la gestión ordinaria de la *startup*, en el día a día del negocio, tomando decisiones sobre la marcha para hacer

Así, aun cuando Eisner ya no era CEO ni director de Disney, seguía teniendo mucha influencia en las decisiones de Disney. La transacción se llevó a cabo y Steve Jobs, por aquel entonces uno de los empresarios más influyentes en el mundo, se convirtió en el mayor accionista de Disney y se le asignó un sitio en el directorio de Disney (los sitios en el directorio son preciados). La entrega de un solo sitio a Steve Jobs en un directorio de nueve directores de Disney bloqueó la fusión entre Pixar y Disney por 6,400 millones de dólares (Iger, 2019).

Caso inversionistas activistas: Cuando el directorio o los ejecutivos de las sociedades americanas tienen resultados deficientes, la sociedad podría convertirse en el objetivo de inversionistas activistas, quienes procurarán intervenir para obtener cambios estructurales o sitios en el directorio. Usualmente los cambios propuestos por los inversionistas activistas son la venta de negocios deficitarios, cambios en la compensación de los ejecutivos o en el gobierno corporativo, o el mejor uso de los recursos de la sociedad (como podrían ser el pago de dividendos y recompras de acciones). Luego de advertir un objetivo, el inversionista activista iniciará un proceso de compra de acciones de dicha sociedad, hasta llegar a obtener una participación del 5% aproximadamente. Habiendo obtenido dicha participación, promoverá la elección de su candidato al directorio de la sociedad, y cuando no es aceptado por la sociedad, inicia un proceso, donde el inversionista activista y el directorio de la sociedad procurarán obtener poderes de representación de otros accionistas para votar en representación de ellos en la junta general, y a favor de sus respectivos candidatos. Este proceso para obtener poderes de representación se llama *proxy fight*. Los inversionistas activistas hacen inversiones sustanciales para adquirir el 5% del capital social y luego llevar adelante el *proxy fight* con el solo objetivo de lograr que su director candidato sea designado miembro del directorio (Walker, 2016).

9 En el caso de los fondos de *venture capital*, esta preocupación se mitiga, porque, si bien ellos también designan a funcionarios del fondo en los directorios de las s*tartups*, existe un riesgo reputacional de por medio para velar por los intereses de la *startup* y así continuar desplegando fondos en otras *startups*.

que la *startup* salga adelante con la ayuda de su equipo. Así, el éxito o fracaso de esta descansa en los hombros del fundador, gerente general o CEO. El directorio, por tanto, debe estar ahí para cuestionar, traer nuevos puntos de vista, pero ultimadamente lograr que el fundador, gerente general o CEO sea exitoso (y así consecuentemente la *startup* y los accionistas) (Feld & Ramsinghani, 2014, p. 160). En la medida que el fundador advierta que el directorio trabaja para él y que los directores reconozcan que trabajan para el fundador, las metas deberían estar alineadas e, indistintamente de quien designe al director, el directorio será la herramienta de gobierno corporativo ideal para que la sociedad cumpla con sus objetivos.

Poco se ha discutido sobre gobierno corporativo en las *startups* y si bien este trabajo no aspira a ser un análisis exhaustivo sobre las medidas de buen gobierno corporativo a ser implementadas en las mismas, pretendo que sea un punto de partida para continuar desarrollando las mejores prácticas y políticas que nos permitan ayudar a las *startups* peruanas a consolidarse en el país y continuar su crecimiento hacia otros mercados latinoamericanos.

REFERENCIAS

Bloomberg (13 de junio de 2018). The David Rubenstein Show: Tim Cook [video]. https://www.bloomberg.com/news/videos/2018-06-13/the-david-rubenstein-show-tim-cook-video

Business Roundtable Corporation (2020). *Statement on the Purpose of a Corporation*. https://s3.amazonaws.com/brt.org/BRT-StatementonthePurposeofaCorporationOctober2020.pdf

Cole, T. (2019). *CEO Leadership: Navigating the New Era in Corporate Governance*. University of Chicago Press.

Collier, P. (2018). *The Future of Capitalism: Facing the New Anxieties*. Harper.

Crunchbase (2021). Glossary of Funding Types. https://support.crunchbase.com/hc/en-us/articles/115010458467-Glossary-of-Funding-Types

Elías Laroza, E. (1998). *Ley General de Sociedades Comentada*. Normas Legales.

Feld, B., & Ramsinghani, M. (2014). *Startup Boards: Getting the Most Out of your Board of Directors*. Wiley.

Iger, R. (2019). *The Ride of a Lifetime: Lessons Learned from 15 Years as CEO of the Walt Disney Company*. Random House.

Loncharich, I. (2005). En beneficios de todos Gobierno Corporativo. *Jurídica: Suplemento de análisis legal del Diario El Peruano*, (28).

Martínez Ortiz, J. (2014). Gobierno corporativo en el Perú: contribución para re-enfocar el concepto. Apuntes. *Revista De Ciencias Sociales*, (56/57), 95-114. https://doi.org/10.21678/apuntes.56/57.550

Ministerio de Justicia y Derechos Humanos (2021). *Anteproyecto de la Ley General de Sociedades.* https://cdn.www.gob.pe/uploads/document/file/1914635/Anteproyecto%20de%20la%20Ley%20General%20de%20Sociedades.pdf.pdf

O'Reilly, T. (2017). *WTF? What's the Future and Why It's Up to Us*. HarperCollins Publishers.

Palacios, E. (2021). EGS toma un rol central en las inversiones de private equity. *Industria Legal*, (4), 16-17.

Salas Sánchez, J. (2005). Las funciones del directorio y de la gerencia. *Jurídica: Suplemento de análisis legal del Diario El Peruano*, (28).

The Economist (17 de septiembre de 2020). What is stakeholder capitalism?. https://www.economist.com/business/2020/09/17/what-is-stakeholder-capitalism

Walker, O. (2016). *Barbarians in the Boardroom. Activist investors and the battle for control of the world's most powerful companies*. Pearson.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Ley 26887, Ley General de Sociedades, Diario *El Peruano*, 9 de diciembre de 1997 (Perú).

Código de Buen Gobierno Corporativo para las Sociedades Peruanas, 4 de noviembre de 2013 (Perú).

10.18800/themis.202101.024

LAS PLATAFORMAS DIGITALES Y LA PARTICULARIDAD DE SU PAPEL EN EL MERCADO: SU ACTIVIDAD ECONÓMICA Y LAS IMPLICANCIAS LABORALES QUE SE GENERAN COMO CONSECUENCIA DE SU INCORRECTA IMPLEMENTACIÓN

DIGITAL PLATFORMS AND THE PARTICULARITY OF THEIR ROLE IN THE MARKET: THEIR ECONOMIC ACTIVITY AND THE LABOR IMPLICATIONS THAT ARE GENERATED AS A CONSEQUENCE OF THEIR INCORRECT IMPLEMENTATION

Cecilia Calderón Paredes*
Cornejo & Santiváñez Laboralistas

In the context of Bill 4243/2018-CR, the Law of Decent Employment that regulates workers on Digital Platforms, the existence of a new business reality dominated by the phenomenon of digital platforms is undeniable. This new dynamic challenges the classic parameters of labor law and puts into debate the existence or not of an employment relationship between the agents participating in it.

In this article, and from a commercial-labor perspective, the author outlines the existence of a new 'platform economy', identifies the actors involved in it and the dynamics that it incorporates in the market. In the same way, she examines the new signs of employment that could arise in this scenario, as they have been recognized by the Spanish Supreme Court in one of its last decisions regarding the matter: the Glovo case.

Keywords: Collaborative economy; platform economy; digital platforms; uberization; signs of employment; labor relationship distortion.

En el contexto del Proyecto de Ley 4243/2018-CR, Ley del Empleo Digno que regula a los trabajadores de Plataformas Digitales, es innegable la existencia de una nueva realidad empresarial dominada por el fenómeno de las plataformas digitales. Esta nueva dinámica reta los parámetros clásicos del derecho laboral y coloca en debate la existencia o no de un vínculo de naturaleza laboral entre los agentes partícipes de ella.

En el presente artículo, y bajo una visión mercantil-laboral, la autora destaca la existencia de una novedosa economía de plataformas, identifica a los actores intervinientes en ella y la dinámica que esta incorpora en el mercado. De igual manera, examina los nuevos indicios de laboralidad que podrían surgir en este escenario, conforme han sido reconocidos por el Tribunal Supremo español en un último pronunciamiento referido al tema: el caso Glovo.

Palabras clave: Economía colaborativa; economía de plataformas; plataformas digitales; uberización; indicios de laboralidad; desnaturalización laboral.

* Abogada. Máster en Derecho de las Transacciones Internacionales por el Centro de Estudios Garrigues y la Universidad Antonio de Nebrija, España. Candidata a Magíster en la Maestría de Derecho del Trabajo y de la Seguridad Social en la Pontificia Universidad Católica del Perú. Asociada senior de Cornejo & Santiváñez Laboralistas (Lima, Perú). Contacto: cecilia.calderonp@gmail.com

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 10 de enero de 2021, y aceptado por el mismo el 18 de marzo de 2021.

I. INTRODUCCIÓN

Cuando en nuestro medio abordamos la problemática vinculada a las plataformas digitales, lo primero que salta a la vista es la facilidad con que el común de las personas –e, inclusive, los legisladores– simplifica o restringe el objeto social presente en estos negocios, equiparándolo con la actividad ofrecida a través de ellas. Sucede así, por ejemplo, en el proyecto de ley denominado Ley del Empleo Digno que regula a los trabajadores de Plataformas Digitales, el que denomina a los "trabajadores" de las plataformas digitales como "repartidores, conductores" (Proyecto de Ley 4243/2018-CR, 2019, art. 1). Realidad curiosa si recordamos que, en el mercado peruano, las más conocidas y difundidas plataformas digitales son empresas en las que se ofrecen servicios de transporte y reparto.

Desde nuestra experiencia, las empresas que tienen a las plataformas digitales como principal activo no se dedican a la prestación del servicio que se ofrece a través de ellas. Su objeto social es, en realidad, el desarrollo de la plataforma y, como tal, su actividad empresarial gira en torno al diseño, creación, puesta en marcha, soporte técnico, mejoramiento, publicidad y administración de esta.

La plataforma o *app* es un medio que permite la interconexión digital y facilita a sus usuarios perfeccionar transacciones entre ellos. A través de esta, usuarios proveedores (ajenos a la empresa que desarrolla el aplicativo) ofrecen al mercado distintos tipos de bienes y servicios y, en uso de la misma, otros usuarios, clientes, concretan negocios con ellos.

El presente artículo aborda, bajo una visión mercantil-laboral, el fenómeno de las plataformas digitales, distinguiendo los distintos servicios involucrados y el papel que adoptan sus actores. Bajo este contexto, y tras reconocer que los vínculos jurídicos que debieran ser ejecutados de forma independiente pueden verse afectados por una distorsión en la práctica, finalizamos nuestra aproximación examinando los indicios de laboralidad que podrían surgir en esta nueva economía, conforme han sido reconocidos en una de las más recientes sentencias expedidas por el Tribunal Supremo español para el caso Glovo.

II. LAS PLATAFORMAS DIGITALES COMO ACTORAS EN EL MERCADO

A. Un nuevo concepto: la economía de plataformas

La evolución en la tecnología ha permitido la paulatina aparición de nuevas formas de organización empresarial, abriendo las puertas a modelos de negocio que permiten la comercialización de bienes y servicios a través de medios digitales.

La denominación utilizada para este fenómeno varía en función de cuál es la dinámica que se produce a partir de la oferta[1]. No obstante, en términos generales y para efectos del presente artículo, nos referiremos de forma genérica a la 'economía de plataformas', que es aquella que aprovecha la utilización de una plataforma digital para el perfeccionamiento de una transacción (comúnmente, la venta de bienes o la contratación de un servicio).

En la economía de plataformas, distintos usuarios se registran en ella –ya sea como usuarios que proveen bienes o servicios o como usuarios que requieren de los mismos– con el fin de que, a través de esta, logren enlazar una oferta abierta a un requerimiento específico.

En consecuencia, el éxito en este tipo de negocios reside en la dimensión de la oferta que alberga la plataforma y, desde luego, en qué tan masivo es el uso de ella. Efectivamente, se trata de un círculo que se retroalimenta; así, mientras más oferta de bienes o servicios se encuentre en una plataforma, más probable es que una mayor cantidad de usuarios se registre en ella. Es la cantidad y variedad de ofertantes lo que aumenta considerablemente la posibilidad de satisfacer prontamente una necesidad. Y sucede lo mismo en sentido inverso; es decir, mientras más grande sea la preferencia de los consumidores por determinada plataforma, más atractiva resultará esta para quienes ofertan

[1] Conceptualmente, se habla de *gig economy*, **economía a demanda**, **economía colaborativa**, entre otros. Brevemente, podemos señalar que el término *gig economy* representa el **género**, pues alude a una forma de organización del mercado de trabajo que se caracteriza por la prevalencia de labores autónomas de corta duración; por su parte, la **economía a demanda** y la **economía colaborativa** son dos manifestaciones de esta, es decir, las **especies** del género *gig economy*. Para más información sobre el tema, véase la página web Gig Economy Data Hub, desarrollada en asociación por Cornell University y el Aspen Institute (https://www.gigeconomydata.org/basics).

Así, como lo sintetiza Valerio De Stefano en su artículo titulado La *gig economy* y los cambios en el empleo y la protección social, mientras en la economía colaborativa las micro tareas se llevan a cabo a distancia y, por ello, las partes no se encuentran ni ejecutan actividades de forma "presencial" (toda la interacción se realiza de forma virtual), en la economía a demanda el internet sirve para "poner en común la oferta y la demanda de actividades […] para que estas puedan ejecutarse **a nivel local**" (2016, p. 152) [el énfasis es nuestro], es decir, de forma presencial.

bienes o servicios, pues, al existir un mayor número de usuarios, más probable será que ellos –como ofertantes– concreten negocios al conseguir público consumidor.

En este contexto y conforme al modelo de negocio, el servicio que presta la empresa titular de la plataforma digital consiste en ser una intermediaria entre la oferta y la demanda que se encuentra libre en el mercado, permitiendo la conexión entre quien provee el bien o servicio y quien lo requiere (comúnmente conocido como 'usuario final'). Nos encontramos, pues, frente a una empresa que opera como intermediaria entre necesidades, la cual gestiona la oferta y demanda de determinado servicio a través de una plataforma digital.

Ahora bien, es importante considerar que las empresas de la economía de plataformas tienen una infraestructura digital que les permite la posibilidad de facilitar la celebración de acuerdos referidos a los servicios que se ofrecen a través de ellas, ello pensando en el beneficio de los usuarios finales. En efecto, las plataformas o *apps*, al conectar distintos tipos de usuarios y funcionar como lugar de encuentro entre los agentes del mercado, se nutren de la información de estos, lo que resulta un elemento clave para facilitar la celebración de las transacciones.

Así, el servicio prestado por la plataforma consiste no solo en agrupar ofertas para ser expuestas, sino también en ser un canal que almacena y centraliza los datos que sirven para perfeccionar acuerdos con la inmediatez de un *click*, sin necesidad de que ninguna de las partes tenga que trasladarse físicamente, encontrarse en un mismo ambiente, reiterar información proporcionada previamente para su suscripción como usuario de la plataforma, o negociar condiciones económicas asociadas al servicio que se prestará.

Efectivamente, gracias a la infraestructura digital, quienes participan de una transacción pueden conocer la identidad de su contraparte, contactarlo telefónicamente, ubicarlo físicamente e, inclusive, no requerirán invertir tiempo en negociar los términos y condiciones de una operación –entre ellos, el precio de lo que se comercializa–, pues estos se encontrarán predeterminados en la plataforma. Las posibles ventajas son tales que, de requerirse, la tecnología asociada a las plataformas logra evitar el uso de dinero físico, debido a que permite el pago por canales digitales.

Como se observa, bajo el amplio paraguas de estas facilidades, las empresas de la economía de plataformas pueden continuar transformándose y ser no solo un ente que intermedia entre servicios y necesidades, sino también uno que, hasta cierto punto, apoya a los usuarios estructurándolos. Sobre este particular, conviene destacar lo señalado por la Comisión Europea, la que reconoce que las empresas titulares de las plataformas pueden ejecutar actividades auxiliares al servicio que se ofrece a través de ellas (*e.g*. modalidades de pago, cobertura de seguro, servicio posventa) y que esto "no constituye por sí mismo una prueba de influencia y control por lo que respecta al servicio subyacente" (2016, p. 7).

Para cerrar este apartado, no quisiéramos dejar de mencionar el siguiente aspecto relevante: de la mano de los avances tecnológicos y la proliferación del uso del internet, el mercado de consumo de bienes y servicios ha evolucionado, respondiendo a un modelo de sociedad en la que el ahorro de tiempo y esfuerzo son vitales y representan bienes deseados.

Así, la inmediatez que permiten las plataformas digitales satisface la creciente necesidad de disfrutar de experiencias de consumo rápido, simple y eficiente, características que, por tanto, serán el eje y la meta de las empresas que participan en este modelo de negocio.

B. Antecedentes administrativos expedidos por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual que reconocen que las empresas de la economía de plataformas tienen como objeto social el servicio de intermediación entre personas

En el Perú, la casuística por la que se conoce a la economía de plataformas se encuentra vinculada a cuestionamientos sobre la supuesta prestación directa del servicio de transporte público de pasajeros por parte de las empresas que comercializan aplicaciones como los mundialmente conocidos Uber y Cabify (Resolución 074-2015/CD1-INDECOPI, 2015), o empresas más locales como Taxi Satelital (Resolución 100-2015/CD1-INDECOPI, 2015) o Solo para Ellas (Resolución 075-2015/CD1-INDECOPI, 2015).

Al respecto, es importante señalar que, a la fecha, los pronunciamientos referidos a la economía de plataformas han sido emitidos en vía administrativa por el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (en adelante, Indecopi), existiendo, además, algunos informes emitidos por el Ministerio de Transporte y Comunicaciones, entidad competente para la regulación del sector transporte (que es la actividad más cuestionada por vía legal en esta industria). Estos pronunciamientos

destacan que en el Perú existe un vacío legal respecto de la actividad de las empresas de la economía de plataformas, la que finalmente califican de "prestación de un servicio de intermediación" (Resolución 084-2020/SDC-INDECOPI, 2020, numeral 108).

Ciertamente, desde aproximadamente el año 2015, la Comisión de Fiscalización de la Competencia Desleal Número 1 del Indecopi se ha pronunciado de forma reiterada y sostenida ante supuestos actos de competencia desleal y publicidad engañosa, señalando que las empresas que comercializan los aplicativos donde se ofertan servicios de transporte privado no ejecutan ese servicio, sino que ofrecen la "colocación" del transporte que es provisto por un tercero ajeno a ellas (Resolución 099-2015/CD1-INDECOPI, 2015; Resolución 100-2015/CD1-INDECOPI, 2015).

Así, por ejemplo, tras analizar la información contenida en el sitio web y redes sociales de la empresa Easy Taxi, el Indecopi concluyó que

> [...] Del referido sitio web y redes sociales, podemos verificar información suficiente sobre **la naturaleza del servicio que brinda la imputada**, el cual, conforme se ha señalado anteriormente, **permite, mediante el uso de una aplicación móvil, la colocación de servicio de taxi al usuario que lo solicite**, **de manera rápida y automática y, no la prestación del servicio de transporte** […] (Resolución 099-2015/CD1-INDECOPI, 2015, numeral 4.2.3) [el énfasis es nuestro].

De igual manera, señaló que la empresa conocida como Taxi Satelital se publicitaba de manera clara y expresa como una plataforma que permite una conexión "automática y rápida" entre usuarios, que son quienes –por una parte– requieren y –por la otra– prestan el servicio de transporte (Resolución 100-2015/CD1-INDECOPI, 2015, numeral 4.2.3).

Más recientemente, la Sala Especializada en Defensa de la Competencia del Indecopi (en adelante, la SDC) se pronunció respecto de una denuncia interpuesta por la Asociación de Consumidores Indignados Perú contra Uber Perú S.A. y Uber B.V., en la que se alegaba un supuesto incumplimiento de las normas que prohíben la competencia desleal (Resolución 084-2020/SDC-INDECOPI, 2020, sección Antecedentes). De acuerdo con la asociación, estas empresas estarían prestando el servicio de taxi (transporte público de pasajeros) sin haber obtenido las autorizaciones, licencias o títulos necesarios, así como en inobservancia de las normas laborales y fiscales, lo que les generaría una gran ventaja competitiva.

Sobre el particular, tras un detallado análisis, la SDC procedió a confirmar la resolución de primera instancia, en la que, entre otros, se reconocía que la empresa Uber B.V. se dedica exclusivamente a conectar usuarios taxistas con usuarios solicitantes del servicio de transporte, lo cual no constituye la prestación directa del servicio. Este pronunciamiento acogió la defensa de la denunciada, la que alegaba que su modelo de negocio consistía en facilitar el intercambio de bienes y servicios entre particulares a través del uso de tecnologías o medios digitales, enlazando la oferta y demanda de las personas.

Para tales efectos, la SDC desarrolló un apartado denominado economía de plataformas y, entre los numerales 66 y 78, conceptualizó el modelo de negocio al que nos venimos refiriendo, verificando y validando la forma cómo se estructura y describiéndolo, tal y como ha sido expuesto en el apartado precedente.

Así, la SDC denomina "plataforma de dos lados" a los aplicativos de la economía de plataformas, señalando que son un espacio virtual provisto por un agente económico –en estos casos, la empresa que las desarrolla–, que es el que facilita la interacción entre distintos grupos de personas, permitiéndoles no solo contactarse sino también realizar a través de ella sus transacciones (Resolución 084-2020/SDC-INDECOPI, 2020, numeral 66).

Además, este pronunciamiento tiene la particularidad de que resalta las ventajas o beneficios económicos que genera la economía de plataformas para el mercado, los que sintetiza en dos:

a) El ahorro en los costos de transacción, los que incluyen el costo de búsqueda, negociación del contrato y coordinación para su cumplimiento; y

b) Las "externalidades de red indirectas", que no es otra cosa que el incremento del valor de la plataforma producido como consecuencia del incremento en el número de usuarios contraparte (Resolución 084-2020/SDC-INDECOPI, 2020).

Este último ítem, aludido en el apartado precedente, significa que los usuarios valorarán más una plataforma mientras más usuarios contraparte puedan encontrar en ella: es la retroalimentación de oferta y demanda.

Es importante señalar que, para efectos de definir la economía de plataformas y delimitar el servicio que prestan las empresas en ella, la SDC se nutre también de lo señalado por la Comisión Europea

en el documento denominado Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Una Agenda Europea para la Economía Colaborativa (Resolución 084-2020/SDC-INDECOPI, 2020, numeral 72). Este reconoce que en la economía de plataformas intervienen tres tipos de actores, quienes son:

a) El administrador o intermediador, es decir, la empresa que desarrolla la plataforma;

b) Los proveedores de productos o prestadores de servicios, quienes hacen uso de la plataforma para ofertarlos; y

c) Los usuarios finales de los productos o servicios, quienes demandan los mismos y buscan satisfacer su necesidad encontrando ofertas a través de la plataforma (Resolución 084-2020/SDC-INDECOPI, 2020, numeral 72).

Es sobre la base de estos antecedentes teóricos y de un análisis detallado tanto de los términos y condiciones del aplicativo Uber, como de la información disponible en la página web y en el contrato privado suscrito entre Uber Perú S.A. y Uber B.V.[2], que la SDC concluye que el aplicativo Uber "[...] es una plataforma digital de transporte de dos lados que permite conectar a socios conductores (taxistas) con usuarios solicitantes (pasajeros)" (Resolución 084-2020/SDC-INDECOPI, 2020, numeral 102), ofreciendo dos productos diferentes a dos demandas distintas.

La SDC es enfática en señalar, pues, que los usuarios de la plataforma son de dos tipos: unos que ofertan y otros que demandan un servicio. Reconoce expresamente en el mismo apartado que:

> [...] De un lado, se ubican los conductores [quienes] demandan que potenciales pasajeros se pongan en contacto con ellos –a través del aplicativo– a fin de poder realizar un servicio de transporte […] del otro lado, se ubican los **usuarios**, quienes, por medio del aplicativo, demandan **contactar** con los **socios conductores**, **a fin de que estos les brinden un servicio de transporte a cambio de una contraprestación** […] (Resolución 084-2020/SDC-INDECOPI, 2020, numeral 102) [el énfasis es nuestro].

Ahora bien, aunque para efectos del análisis que nos congrega nos encontramos ante pronunciamientos administrativos que no tienen como fin determinar si existe o no naturaleza laboral en la forma cómo se provee el servicio, queremos destacar el reconocimiento que hacen respecto de la nueva realidad empresarial sobre la que venimos refiriéndonos.

Esta no genera por sí misma una vulneración a las bases del derecho laboral ni precariedad laboral en los vínculos jurídicos de los que se nutre. Se trata, desde nuestro entendimiento, de un modelo de negocio relativamente novedoso, cuyo desarrollo es aún muy incipiente en el mercado peruano y que, como sucede en muchos otros casos, con ocasión de su puesta en marcha, puede haberse visto afectado por distorsiones.

C. La expansión de los negocios que se concretan gracias a la economía de plataformas como evidencia del *core business* de las empresas que actúan en el marco de esta

Conforme anticipamos en la introducción del presente artículo, la economía de plataformas es un modelo de negocio que aprovecha la implementación de una infraestructura digital que permite la conexión de distintos tipos de necesidades. En nuestro país, de momento, las empresas que participan en ella se concentran en permitir la prestación de servicios vinculados al transporte privado de personas y al transporte o reparto de bienes, lo que ha generado que muchos equiparen su objeto social a la ejecución de dichos servicios.

No obstante, es importante considerar que existen algunas empresas de la economía de plataformas que ya 'piensan fuera de la caja' y actúan en el mercado bajo un concepto más comprehensivo. Se trata, principalmente, de empresas como Glovo y Rappi que, en la práctica, vienen demostrando al mercado cuál es la real naturaleza de esta novedosa forma de organización y de hacer negocios. Aunque se les suele identificar con la interconexión para el reparto de bienes (*delivery*), ambas vienen empleando sus plataformas para que, a través de ellas, bancos pertenecientes a dos de los grupos económicos más importantes del país ofrezcan productos propios del sistema financiero.

Efectivamente, tal y como fue anunciado a fines del 2020, el Banco de Crédito del Perú (en adelante, BCP) y el banco Interbank han celebrado alianzas con Glovo y Rappi para que, en aprovechamiento de sus plataformas digitales, se facilite servicios

[2] Contrato suscrito para que la primera brinde servicios de soporte y publicidad a la segunda, la que es en realidad la titular del aplicativo y quien, de acuerdo con esta realidad empresarial particular, presta el servicio de intermediación entre usuarios.

financieros a los usuarios de estos aplicativos (Gestión, 2020; Perú21, 2020).

De acuerdo con las notas de prensa, el BCP ha desarrollado un plan piloto que tiene como objetivo concretar préstamos económicos a restaurantes y empresas afiliadas a Glovo. Lo que lleva a cabo es una evaluación de la situación crediticia de aquellas a partir de información económica referida a los ingresos y/o facturación generada por las ventas concretadas a través del *app*. Esto lo realiza fácilmente aprovechando que esta información se encuentra almacenada por la compañía como consecuencia del uso de su plataforma.

Se trata, pues, de una forma novedosa de ejecutar la evaluación crediticia en un sistema financiero acostumbrado a operar por canales clásicos (agencia) y se logra a partir de una sinergia entre empresas. Por un lado, la plataforma digital que tiene como principal activo el manejo de información clave de empresas usuarias que ofrecen sus servicios a través de ella; y, por otro lado, la entidad financiera que ahorra en costos de transacción, agilizando la forma cómo accede a información relevante sin invertir recursos humanos, tiempo y esfuerzo en que los potenciales clientes se acerquen a una sede propia o utilicen diferentes medios virtuales para entregarle documentación que respalde su solicitud de crédito.

La alianza de Rappi con Interbank es muy similar, con la precisión de que su objetivo sería mucho más ambicioso, pues pretendería 'bancarizar' el mercado peruano en diferentes niveles y productos, permitiendo que a través de la plataforma digital se pueda, además de otorgar créditos, crear cuentas de ahorro.

Esta nueva forma de hacer negocios representa la materialización de la vocación de las empresas que desarrollan plataformas digitales: el aprovechamiento de una infraestructura digital 'neutra' para conectar necesidades en diferentes sectores económicos. En particular, nos parece interesante el uso que se ha dado de las plataformas o *apps* para beneficiar mercados tan tradicionales como la banca, que ninguna relación tiene con el servicio de reparto o *delivery* con el que se ha pretendido identificar a las empresas de la economía de plataformas que operan en nuestro país.

Estas nuevas alianzas, a nuestro parecer, demuestran que la actividad económica de las empresas de la economía de plataformas **no** consiste en la prestación del servicio que se ofrece a través de ellas (en este caso, se trata de un servicio de naturaleza financiera, actividad estrictamente regulada en nuestro país y que, por tanto, de ninguna manera podría ser ejecutada por Rappi o Glovo en tanto no se trata de empresas autorizadas), sino que es, en realidad, la prestación de un servicio de sola interconexión. En los ejemplos expuestos, por un lado, existen personas naturales o jurídicas con la necesidad de integrarse al sistema financiero o de obtener un crédito y, por otro lado, se encuentran los bancos, cuyo objetivo es cubrir la mayor cantidad del mercado con sus productos y que aprovechan la data derivada del uso de las plataformas digitales para acercarse a un público objetivo al que, quizás, no hubieran podido contactar tan fácilmente sin el uso de los aplicativos Glovo y Rappi.

Finalmente, es sumamente relevante considerar el contexto social en el que la diversificación del uso de las plataformas digitales está sucediendo: la propagación de la pandemia del COVID-19, la que durante el año 2020 y previsiblemente, durante el 2021, generará que el Gobierno peruano mantenga un conjunto de medidas destinadas a garantizar el distanciamiento social entre las personas. Así, pues, se limitaron las libertades de tránsito, de reunión e, inclusive, de empresa, prohibiéndose la circulación de personas, estableciéndose distintos horarios de inmovilización en domicilio y limitándose no solo los aforos, sino también las actividades económicas autorizadas a operar presencialmente.

Esta situación, sin lugar a duda, contribuye a la valorización de las empresas de la economía de plataformas pues, dado su principal activo, podrían servir para conectar distintos tipos de necesidades no vinculadas al transporte de personal o de bienes[3] en un contexto en el que diversos sectores económicos requieren urgentemente de interconexión digital.

Recordemos que, como bien lo ha resaltado la Comisión Europea, la economía de plataformas crea nuevas oportunidades y "[...] puede, por lo tanto, contribuir de manera importante al empleo y el

[3] En este ámbito, la propia Rappi se encuentra ya un paso adelante, pues desde hace algún tiempo permite que a través de su plataforma se a) concreten pedidos en distintos establecimientos comerciales, bajo la modalidad 'Recojo', lo que significa que el usuario canaliza su necesidad a través de Rappi pero no hace uso del servicio de interconexión para reparto; o b) se realicen donaciones –en este caso, a Aldeas Infantiles Perú–, servicio que, evidentemente, únicamente sirve para fines filántropos mas no para que el usuario obtenga un bien o servicio de aprovechamiento propio.

crecimiento [...] si se fomenta y desarrolla de manera responsable" (2016, p. 1).

III. LA DESNATURALIZACIÓN DE LOS VÍNCULOS INDEPENDIENTES PROPIOS DE LA ECONOMÍA DE PLATAFORMAS

A. Dos realidades distintas: la empresa de la economía de plataformas como agente intermediador y como empleador y la posibilidad de una distorsión

Habíamos señalado que, de acuerdo con el modelo de negocio de la economía de plataformas, las empresas que se desenvuelven en este mercado tienen como finalidad la creación de una plataforma digital o *app* que conecta la oferta y la demanda relacionadas a determinado bien o servicio, los que pueden ser diversos.

Bajo este entendido, estas empresas actuarán en dos dimensiones: una, como empleador frente a sus trabajadores –es decir, a quienes contratan para el desarrollo y gestión de la plataforma digital–; y otra, como actor en el mercado, ofreciendo el servicio de interconexión a los distintos tipos de usuario interesados en su producto, con los que celebrarán acuerdos de naturaleza mercantil.

Los contratos de trabajo que celebren se dirigirán, entonces, a posiciones clave del negocio o, inclusive, a puestos de orden administrativo, que cubren necesidades del día a día de toda empresa. Así, se podrán suscribir contratos laborales con, por ejemplo, los ingenieros de *software* que diseñan el algoritmo y el interfaz de la plataforma y solucionan cualquier defecto o falla que pudiera ocurrirle; o con personal de las áreas de administración, contabilidad, recursos humanos, entre otros. No obstante, para relacionarse con los usuarios que prestan servicios ofertándolos en la plataforma, la naturaleza de los contratos será diferente, totalmente ajena a la laboral. ¿Por qué? Porque estas personas ejecutan –en principio– servicios por cuenta propia y utilizan el aplicativo únicamente como un medio para ofrecerlos.

Lo relevante en este apartado es tener presente que las empresas de la economía de plataformas no son empresas que deban calificarse, automáticamente, como informales para la óptica laboral, pues detrás de ellas existe personal que, bajo contratos de trabajo, presta servicios a su favor en actividades propias de su giro de negocio.

Ahora bien, los principales problemas que se presentan cuando analizamos a las empresas de la economía de plataformas son, por un lado, la ya mencionada identificación del objeto social de la compañía con el servicio que los terceros ofertan a través de ellas; y, por otro lado, la tendencia a trasladar la distorsión propia de determinadas experiencias a la totalidad de los posibles participantes en este modelo de organización. Sobre este último aspecto es que nos queremos referir a continuación.

Efectivamente, tal y como sucedió en los inicios de la regulación de tercerización laboral –e inclusive, previamente, con la intermediación de servicios–, el mercado suele recibir con sospecha a las empresas que se desenvuelven de forma distinta al modelo imperante.

Hoy en día estamos acostumbrados a que quien presta un servicio lo ofrezca directamente; pese a ello, la economía de plataformas trabaja de manera distinta: quien presenta la oferta a los posibles consumidores no es, en realidad, quien ejecutará el servicio y, por ello, esta nueva forma de operar genera suspicacias.

Sumado a ello, se trata de una estructura de negocio que, en la práctica, puede conllevar a una desnaturalización de los vínculos independientes que la alimentan, ello como consecuencia de una inadecuada ejecución de las atribuciones de las partes: es una realidad que algunas de las empresas –pese a alegar que no proporcionan el servicio requerido por los consumidores– se reservan algunas facultades que resultan muy intrusivas y exceden de los simples 'arreglos' de aspectos accesorios en beneficio del usuario final (lo que la Comisión Europea ha llamado 'servicios auxiliares', como se ha mencionado antes), lo que genera una gran distorsión en el modelo.

En este contexto, ya sea porque no se conoce la dinámica de su funcionamiento o porque, lamentablemente, se ha tenido una mala experiencia con alguna empresa específica, se tiende a atribuir una carga negativa al modelo de negocio desarrollado en la economía de plataformas.

Desde nuestra experiencia, es importante recordar que la existencia o no de un vínculo de naturaleza laboral dependerá de las circunstancias y características que lo rodean. Por ello, al ser la economía de plataformas una estructura de negocios válida y diferente a la común no debiera generalizarse señalándose que alguna distorsión identificada en la casuística descalifica todo el sistema, máxime si es sabido que no todas las empresas de la economía de plataformas celebran acuerdos con los proveedores bajo las mismas reglas y condiciones.

B. De la posibilidad de encontrarnos frente a relaciones regidas por el derecho del trabajo entre las empresas de la economía de plataformas y los usuarios proveedores: la desnaturalización de sus relaciones y la subordinación como elemento diferenciador de un vínculo de naturaleza laboral

Habíamos señalado que las empresas de la economía de plataformas son entidades que se dedican a desarrollar *apps* o plataformas digitales que sirven de intermediarias para la concreción de transacciones entre usuarios proveedores y usuarios finales. En este contexto, las empresas no solo implementan las plataformas, sino que también las administran, lo que identificamos como su papel **gestor**.

Como se ha expresado previamente, como parte de su gestión, las empresas establecen ciertas condiciones uniformes que ayudan a configurar las transacciones que los usuarios concretan a través de la plataforma, lo que denominaremos papel **estructurador**.

Esta distinción es relevante porque, según vemos, es en este último ámbito que podría analizarse la posibilidad de que se presente una distorsión que convierta en laboral un vínculo que nació con vocación de ser autónomo o independiente. ¿Por qué podría suceder ello? Porque la empresa titular de la plataforma determina ciertas condiciones del servicio a ejecutarse y, muchas veces, se reserva ciertas facultades o derechos, lo que podría llegar a evidenciar la existencia de subordinación entre ella y el proveedor.

Así, conforme a lo indicado en el apartado previo, a nivel de doctrina y jurisprudencia comparada se ha podido identificar que no solo por las facultades y derechos que la empresa titular de una plataforma se reserva, sino también por la forma cómo se comporta en relación con el proveedor, algunas jurisdicciones se han pronunciado ya reconociendo la desnaturalización que se produce en los vínculos que suscriben los usuarios proveedores y aquellas. La desnaturalización, desde luego, implicará que estos vínculos, supuestamente independientes, deban reconocerse como trabajo por cuenta ajena.

A partir de un análisis jurisprudencial[4], verificamos que el examen de las diferentes Cortes ha generado como resultado algunos elementos en común, que no son más que un conjunto de indicios que ayudarían a determinar cuándo el vínculo jurídico entre un prestador de servicios y una empresa de la economía de plataformas se encuentra desnaturalizado.

Desde nuestra perspectiva, todos ellos parten de un mismo núcleo, es decir, son manifestaciones de la **subordinación** como elemento diferenciador del contrato de trabajo.

Al respecto, de conformidad con lo dispuesto en el artículo 4 del Decreto Supremo 003-97-TR, Texto Único Ordenado de la Ley de Productividad y Competitividad Laboral, en toda relación laboral se pueden identificar tres elementos esenciales, a saber: a) la prestación personal de servicios; b) la remuneración; y, c) la subordinación (1997). Por el contrario, las relaciones independientes o autónomas son aquellas en las que quienes prestan el servicio trabajan sin encontrarse bajo poder de dirección alguno (Arce Ortiz, 2008, p. 84).

Vemos, pues, cómo el elemento diferenciador entre un contrato de trabajo y un contrato de prestación de servicios independientes (contrato de locación de servicios) es la **subordinación**. En palabras del maestro Neves Mujica, aquella representa

> [...] un vínculo jurídico entre el deudor y el acreedor de trabajo, en virtud del cual el primero le ofrece su actividad al segundo y le confiere el poder de conducirla. Sujeción de un lado y dirección del otro, son los dos aspectos centrales del concepto [...]. (2012, p. 36).

Sobre este particular, la doctrina ha señalado que el concepto de subordinación se construye a partir del elemento de **dependencia**. De acuerdo con lo señalado por el profesor Alfredo Montoya Melgar, ello significa identificarla con el "[...] sometimiento a las órdenes e instrucciones del empresario" (1999, p. 60).

En este mismo sentido, para el Tribunal Constitucional peruano, la diferencia entre una relación de naturaleza laboral y una civil consiste en que en esta última no se presenta el elemento de dependencia o sujeción *i.e*. no existe subordinación. Así, ha señalado que

> [...] el contrato de locación de servicios ha sido definido en el artículo 1764º del Código Civil como aquél acuerdo de voluntades por el cual

[4] Para mayor referencia, véase Calderón Paredes (2019), en el que hemos desarrollado un breve resumen, acompañado de algunos comentarios, respecto de jurisprudencia emitida previamente en relación a las empresas Uber, Glovo y Deliveroo por tribunales españoles y anglosajones, así como por el propio Tribunal de Justicia de la Unión Europea (Corte de Luxemburgo).

> 'el locador se obliga, sin estar subordinado al comitente, a prestarle sus servicios por cierto tiempo o para un trabajo determinado, a cambio de una retribución' [por lo que] es evidente que, de la definición dada por el Código Civil, se desprende que lo que caracteriza a este contrato es la **independencia del locador frente al comitente en la prestación de sus servicios, siendo este el elemento diferenciador entre ambos contratos** (Expediente 9197-2006-AA-TC, 2007, fundamento 5) [el énfasis es nuestro].

Luego, al ser la subordinación el elemento central que define la existencia de un vínculo laboral, conviene preguntarnos por sus particularidades. Para ello, es preciso recordar que, de acuerdo con las definiciones brindadas, la subordinación implica sujeción, sometimiento, obediencia y, por ello, se encuentra estrechamente vinculada a la existencia de facultades de dirección, fiscalización y sanción por parte del empleador, las que le permiten organizar activamente la prestación del servicio y corregirla en caso la misma se apartase de las instrucciones impartidas.

Así, en palabras de los profesores Palomeque y Álvarez:

> El contrato de trabajo está inmerso en un ámbito donde una de las partes, el empresario, **tiene la facultad de organizar el sistema de producción de bienes y servicios** que libremente ha decidido instalar; esta **capacidad organizativa se concreta en la ordenación de las singulares prestaciones laborales**.
>
> La **potestad para organizar y ordenar el trabajo**, inicialmente y durante toda la ejecución del contrato, **recibe el nombre de poder de dirección** (dirección y control de la actividad laboral) (2008, p. 530) [el énfasis es nuestro].

Conforme a lo señalado, el elemento de subordinación que diferencia a un contrato de trabajo o una relación laboral de otras de naturaleza civil abarcará todas aquellas actitudes y facultades que permiten que quien contrata el servicio pueda organizarlo y dirigirlo, manifestándose tradicionalmente, entre otros, en la posibilidad de determinar el lugar y horario de prestación del servicio, el método a seguir, el control y corrección del trabajo realizado.

Ahora bien, es relevante tener presente que, como lo señala el maestro Neves Mujica, la subordinación conlleva un poder jurídico cuyo ejercicio no es obligatorio para quien lo ostenta, por lo que el empleador "[...] puede decidir si lo ejerce o no y en qué grado, según las necesidades de la empresa y la diversidad de trabajadores [...]" (2012, p. 38). En igual sentido, el profesor Sanguineti Raymond ha indicado que "[...] la forma de operar [un vínculo de jerarquía y subordinación] puede asumir en la práctica una gran variedad de matices y grados, debido a la presencia de una serie de factores externos que inciden sobre ella, contribuyendo a modularla" (1997, p. 50).

Al respecto, es necesario tener presente que, conforme a este último autor, al ser el empleador el titular del poder de dirección, este "[...] puede optar por hacer uso de él en mayor o menor intensidad, en función de lo que considere más adecuado para la satisfacción de su interés" (Sanguineti Raymond, 1997, p. 50), lo que además de ser una manifestación de sus facultades, regulará en mayor o menor medida la posibilidad de que la subordinación se manifieste.

Esta característica, sin embargo, de ninguna manera limitará la configuración de un vínculo de naturaleza laboral pues, en realidad, el elemento de subordinación debe ser analizado **desde el solo hecho de ser latente**: si la subordinación y el poder de dirección del empleador **pueden** presentarse en una relación, así sea de forma **potencial**, configurarán un vínculo de trabajo.

Esto es sumamente relevante, pues en muchos casos, con el fin de descartar la existencia de un vínculo de naturaleza laboral, se alega que, en la práctica, las facultades aludidas no se ejercen y que, por ello, en supuesta aplicación del principio de primacía de la realidad, debiera descartarse un vínculo de naturaleza laboral.

No obstante, en atención a lo indicado, lo relevante será siempre analizar todas y cada una de las facultades que las empresas se reservan respecto de determinada prestación de servicios, pues aunque las mismas no se ejecuten, el simple hecho de existir como una potestad representa un derecho que no se pierde por su 'no uso' y puede servir para demostrar la naturaleza del vínculo suscrito entre las partes.

IV. LOS INDICIOS DE LABORALIDAD EN EL CONTEXTO DE LA ECONOMÍA DE PLATAFORMAS: DE LOS CLÁSICOS A LOS MÁS NOVEDOSOS

A. Los indicios de laboralidad como manifestación del principio de primacía de la realidad y su necesaria adaptación a la nueva realidad empresarial

Los rasgos o indicios de laboralidad son hechos o situaciones fácticas que evidencian la ausencia de autonomía en la prestación de un servicio. En este sentido, la aplicación de indicios de laboralidad

pretende la vigencia de la presunción de laboralidad establecida en el artículo 4[5] del Decreto Supremo 003-97-TR (1997) antes mencionado, pues materializan la presencia de alguno de los tres elementos esenciales de la relación de trabajo, principalmente de la subordinación que, como venimos señalando, es el elemento diferenciador de la misma.

Bajo este entendido se ha pronunciado el Tribunal Supremo español, el que afirma que la valoración de indicios de laboralidad está estrechamente vinculada con la verificación de la existencia de autonomía, señalando que "[...] la calificación de la relación como laboral ha de hacerse en cada caso en atención a los indicios existentes, valorando principalmente el margen de autonomía del que goza quien presta el servicio [...]" (S.T.S. 637/2015, 2015, p. 4).

Al respecto, conviene tener en consideración que los indicios de laboralidad deben ser siempre analizados de forma conjunta, pues es la concurrencia acumulada de ellos lo que permite al juzgador generar convicción sobre la naturaleza laboral de un servicio. Luego, la identificación de uno o algunos pocos no significará que, de manera automática, deba procederse al reconocimiento de una relación de trabajo, sino que, cuando corresponda, el juzgador sopesará los hechos acreditados en el caso y, observándolos en su conjunto, decidirá el valor probatorio que les otorga.

Es importante señalar, además, que, según Villavicencio Ríos y Vieira, los indicios de laboralidad son los elementos que apoyan a la concreción y aplicación del principio de primacía de la realidad, pues buscan que prevalezca la real prestación subordinada de servicios, incluso cuando las partes han celebrado un contrato de otra naturaleza (1999, p. 10). Recordemos que, de conformidad con lo establecido por el Tribunal Constitucional peruano, el principio de primacía de la realidad es aquel que obliga a que, "[...] en caso de discordancia entre lo que ocurre en la práctica y lo que fluye de los documentos, deb[a] darse preferencia a lo primero; es decir, a lo que sucede en el terreno de los hechos [...]" (Expediente 1944-2002-AA/TC, 2003, fundamento 3).

A nivel nacional, los rasgos o indicios de laboralidad se han desarrollado casuísticamente y, ciertamente, suelen presentarse únicamente como enunciados, sin que los jueces o tribunales se detengan a desarrollarlos a profundidad. Así, por ejemplo, el Tribunal Constitucional ha establecido las siguientes condiciones como indicios de la existencia de una relación de trabajo encubierta: a) control sobre la prestación o la forma en que esta se ejecuta; b) integración del demandante en la estructura organizacional de la emplazada; c) prestación ejecutada dentro de un horario determinado; d) prestación de cierta duración y continuidad; e) suministro de herramientas y materiales a la demandante para la prestación del servicio; f) pago de remuneración a la demandante; y g) reconocimiento de derechos laborales, tales como las vacaciones anuales, las gratificaciones y los descuentos para los sistemas de pensiones de salud (Expediente 03917-2012-PA/TC, 2015, fundamento 24).

Por su parte, a nivel internacional, en una de las últimas y más importantes sentencias recaídas sobre la materia, el Tribunal Supremo español ha resuelto un recurso de suplicación interpuesto con la finalidad de dar unificación de doctrina. En él, se pronuncia para determinar si existe o no relación laboral dependiente entre un demandante y la empresa Glovoapp23 S.L., señalando que, en principio, "[...] la dependencia no implica una subordinación absoluta, sino sólo la inserción en el círculo rector, organizativo y disciplinario de la empresa [...]" (S.T.S. 2924/2020, 2020, p. 10).

Conforme a ello, este Tribunal recopila un conjunto de indicios a los que clásicamente ha recurrido para determinar la existencia de una relación laboral, todos los cuales han sido desarrollados en diferentes pronunciamientos propios expedidos en distintas causas, los que hemos agrupado en dos tipos de inicios y pasamos a mencionar brevemente:

a) **Indicios de dependencia**: a) la asistencia al centro de trabajo o al lugar de trabajo designado por el empresario y el sometimiento a horario; b) el desempeño personal del trabajo; c) la inserción de la persona en la organización de trabajo del empresario, que se encarga de programar su actividad; y d) la ausencia de organización empresarial propia de la persona (S.T.S. 2924/2020, 2020, pp. 10-11).

b) **Indicios de ajenidad**: a) la entrega o puesta a disposición del empresario por parte del prestador, de los productos elaborados o de los servicios realizados; b) la adopción por parte del empresario y no del prestador de las decisiones concernientes a las relaciones

[5] Artículo 4 del Decreto Supremo N 003-97-TR: "En toda prestación personal de servicios remunerados y subordinados, **se presume la existencia de un contrato de trabajo** a plazo indeterminado [...]" (1997) [el énfasis es nuestro].

> de mercado o de las relaciones con el público, como fijación de precios o tarifas, selección de clientela o indicación de personas a atender; c) el carácter fijo o periódico de la retribución del trabajo; y d) el cálculo de la retribución o de los principales conceptos de la misma con arreglo a un criterio que guarde una cierta proporción con la actividad prestada, sin el riesgo y sin el lucro especial que caracterizan a la actividad del empresario o al ejercicio libre de las profesiones (S.T.S. 2924/2020, 2020, p. 11).

Desde nuestra perspectiva, es importante tomar en consideración que cada uno de estos enunciados ha sido extraído de contextos específicos y que, por ello, podrán servir de guía para analizar un caso sometido a examen, más no para ser aplicados como una suerte de *checklist* sin mayor estudio del caso.

Figura entre estos indicios, por ejemplo, el de una supuesta ausencia de organización empresarial propia de la persona que provee el servicio, algo que es relativo si se piensa que no todas las actividades que se ejecutan ofreciéndose a través de una plataforma permiten el establecimiento de una estructura compleja por detrás.

De igual forma, se menciona el hecho de que sea la empresa titular de la plataforma quien adopta decisiones concernientes a las relaciones de mercado del servicio que ejecuta el tercero, tales como la fijación de precios o tarifas o la determinación de la clientela a atender.

En estos casos, aunque sujeto a un análisis del caso en concreto, creemos que existe una posibilidad válida de que estos aspectos sean determinados por el algoritmo de la plataforma como parte del servicio auxiliar que esta proporciona a los prestadores de servicios, pues, recordemos, entre las bondades de este modelo de negocio está que la información centralizada en la plataforma digital ayude a que esta evite costos de transacción.

Lo relevante en estos casos estará, según entendemos, en verificar si los parámetros de eficiencia utilizados por la plataforma responden a elementos objetivos (brindar un valor a la escasez de la oferta de un servicio en determinado momento o considerar la distancia y el tráfico, por ejemplo) o si, por el contrario, manifiestan alguna forma de subordinación a la empresa por parte del prestador de servicios. En este punto, es importante tener en consideración que, para ello, no bastará con la experiencia de uno o un conjunto de usuarios, sino que será necesario que el juzgador logre conocer la lógica que sigue el algoritmo de la plataforma digital para sus asignaciones, algo que se podría determinar, por ejemplo, aplicando una pericia de carácter informática.

B. Los indicios de laboralidad derivados de la verificación de una nueva realidad

Habíamos señalado que el Tribunal Supremo español reconoce que los indicios de laboralidad resultan aplicables en aquellos casos en los que se desea determinar si existe una relación laboral encubierta y que, para ello, ha desarrollado un conjunto de indicios que buscan probar que, en la práctica, los elementos del contrato de trabajo son identificables en determinada situación.

En este contexto, el mismo Tribunal Supremo español ha sostenido que existe la necesidad de adaptar el concepto de dependencia o subordinación, principal elemento diferenciador de un contrato laboral, atendiendo a que el desarrollo de la tecnología ha impactado en la forma cómo se configuran hoy en día las relaciones. Así, afirma que

> [...] en la sociedad postindustrial la nota de dependencia se ha flexibilizado. Las innovaciones tecnológicas han propiciado la instauración de sistemas de control digitalizados de la prestación de servicios. **La existencia de una nueva realidad productiva obliga a adaptar las notas de dependencia y ajenidad a la realidad social del tiempo en que deben aplicarse las normas** [...] (S.T.S. 2924/2020, 2020, p. 10) [el énfasis es nuestro].

Esta situación ha recibido igual reconocimiento por parte de la doctrina, tal y como lo evidencian los planteamientos de los profesores Óscar Ermida Uriarte y Óscar Hernández Álvarez. Ambos juristas afirmaron hace casi dos décadas que el elemento de subordinación, que es la "piedra fundamental del sistema Laboral, pues determina su aplicación", venía siendo discutido –entre otros– por presuntas necesidades tecnológicas y que "[...] el cuestionamiento de este instituto específico [...] adquiere una significación mucho mayor que la de otros aspectos del Derecho del Trabajo" (Ermida Uriarte & Hernández Álvarez, 2002, p. 285), generando una imperante necesidad de adaptación de cara a las nuevas formas organizativas.

En el año 2020, el Tribunal Supremo español aprovechó uno de sus más recientes pronunciamientos sobre el tema para desarrollar brevemente los que podríamos considerar **nuevos indicios de laboralidad**, los que se encuentran adaptados a la prestación del servicio de transporte de mercancías ofrecido a través de una determinada plataforma digital (Glovo).

Estos nuevos indicios, insistimos, han sido determinados en función a un conjunto de características vinculadas a un caso concreto y, por ello, si bien podrán servir como elementos de análisis de otras realidades empresariales, sugerimos sean abordados con prudencia.

1. El medio de producción relevante en este tipo de economía

De conformidad con lo señalado por el Tribunal Supremo español,

> [...] Había ajenidad en los medios, evidenciada por **la diferencia entre la importancia económica de la plataforma digital y los medios materiales del demandante:** un teléfono móvil y una motocicleta. **Los medios de producción esenciales en esta actividad no son el teléfono móvil y la motocicleta del repartidor sino la plataforma digital** de Glovo, en la que deben darse da alta restaurantes, consumidores y repartidores, al margen de la cual no es factible la prestación del servicio [...] (S.T.S. 2924/2020, 2020, p. 18) [el énfasis es nuestro].

Al respecto, nos parece relevante destacar que el análisis del Tribunal parece confundir cuál es el servicio prestado por cada actor de este tipo de economía.

Recordemos, pues, que tal y como lo ha reconocido la propia Comisión Europea, el modelo de economía de plataformas lleva inherente la prestación de dos servicios plenamente diferenciados: a) el que ofrece la empresa titular de la plataforma digital, que es la interconexión de usuarios; y b) el que presta el usuario que ofrece sus servicios a través de la plataforma (2016).

En este contexto, es cierto que en este tipo de economía los medios esenciales para la actividad principal no serán los que provee el prestador de servicios, pues, en este nivel de análisis, el servicio que se está examinando es el de interconexión que ofrece la plataforma digital a sus usuarios (proveedores y público en general).

A partir de ello y para esa relación jurídica, los medios que fuesen a emplear los proveedores –en cualesquiera fuesen los servicios que se ofrecieren a través de la plataforma– serán siempre accesorios.

2. La prestación de un servicio bajo la denominada 'marca ajena'

Tras señalar lo indicado en el numeral precedente, el Tribunal Supremo español concluye, de manera inmediata y sin mayor desarrollo ni sustento, que, en ese caso, los proveedores de servicio "[...] realizaba[n] su actividad bajo una marca ajena" (S.T.S. 2924/2020, 2020, p. 18).

El concepto de la 'ajenidad en la marca' propone que los prestadores de servicios en la economía de plataformas actúan en el mercado amparados por una marca (la de la plataforma) y que "[...] con su prestación de servicios [...] no ponen en juego, ni para bien ni para mal, otra cosa que la marca [de la empresa] [...] siéndoles por tanto totalmente ajeno el impacto de su actividad ya que el mismo repercute en [aquella] [...]" (S. Juz. Soc. 193/2019, 2019).

Desde nuestra perspectiva, esta afirmación no genera, de forma determinante, la existencia de un indicio de laboralidad. En efecto, muchas de las plataformas digitales materia de análisis tienen como usuarios prestadores del servicio a individuos anónimos. Esto se debe, básicamente, al tipo de labor fungible que ejecutan, la que no les permite desarrollar una 'marca personal/individual'.

Pese a ello, es también cierto que el propio tipo de negocio, es decir, el uso de una plataforma digital como medio de interconexión de necesidades, puede generar servicios más individuales, en los que los usuarios se inclinen o prefieran a determinado prestador, seleccionándolo o requiriéndolo específicamente al momento de hacer uso del aplicativo.

En estos casos, el servicio materia de comercio seguirá siendo prestado de forma autónoma por el prestador de servicios y la plataforma digital seguirá sirviendo de medio o catálogo para que estos oferten al mercado, pero la dinámica variará, pues los usuarios podrían requerir prestadores específicos, atendiendo al servicio que brindan.

Esta situación podría producirse, por ejemplo, en plataformas donde se ofrecen servicios de nanas o de limpieza de hogar, donde la cercanía del prestador al ambiente personal y familiar del usuario que solicita el servicio podría generar una suerte de 'marca personal/individual'; esto, sobre la base de la experiencia, se crea una preferencia por un prestador específico, solicitándolo con regularidad.

La posibilidad de desarrollar una 'marca' no depende de que la misma se registre o esté vinculada a un logo, colores o frase comercial, sino que se centra en la posibilidad de distinguir y/o diferenciar a quien ejecuta el servicio, el que por su propia naturaleza y sin perjuicio de la plataforma donde se ofrezca, sigue siendo independiente, con la particularidad de poder ser más o menos 'fungible' para el usuario que lo requiere.

3. El establecimiento de un método de fiscalización y sanción a través del sistema de puntuación que asignan los usuarios

De conformidad con lo señalado por el Tribunal Supremo español,

> [...] Glovo tiene establecido un sistema de puntuación de los repartidores clasificándolos en tres categorías: principiante, junior y senior [...] La puntuación del repartidor se nutre de tres factores: la valoración del cliente final, la eficiencia demostrada en la realización de los pedidos más recientes, y la realización de los servicios en las horas de mayor demanda, denominadas por la Empresa «horas diamante».
>
> Existe una penalización de 0,3 puntos cada vez que un repartidor no está operativo en la franja horaria previamente reservada por él. Si la no disponibilidad obedece a una causa justificada, existe un procedimiento para comunicarlo y justificar dicha causa, evitando el efecto penalizador.
>
> Los repartidores que tienen mejor puntuación gozan de preferencia de acceso a los servicios o recados que vayan entrando. No existía pacto de exclusividad [...] (S.T.S. 2924/2020, 2020, p. 15).

Al respecto, consideramos pertinente señalar que, a diferencia de los anteriores **nuevos indicios**, en este caso encontramos no solo más información (que es la que sustenta y permite comprender la decisión adoptada), sino, además, elementos de interferencia en la prestación del servicio por parte de la empresa titular de la plataforma que son mucho más evidentes.

Por ello, consideramos que, para el caso descrito en la sentencia, sí existían elementos que permitían señalar que nos encontrábamos ante una relación laboral encubierta, en la que la empresa titular de la plataforma ejecutaba facultades que son manifestación del poder de dirección que corresponde a un empleador.

Ahora bien, contrariamente a lo que expone el Tribunal Supremo español, no consideramos que los tres factores que determinan el otorgamiento de puntuación sean elementos de interferencia, que signifiquen fiscalización o sanción del repartidor por parte de la plataforma.

En todos los casos –*i.e.* valoración del usuario que requirió el servicio, la eficiencia demostrada en la realización de los pedidos y la realización de los servicios en las horas de mayor demanda–, nos encontramos ante elementos objetivos, que apuntan a favorecer la experiencia del consumidor (usuario final), lo que, finalmente, favorecerá a todos los usuarios de la plataforma pues, como ya se ha explicado, oferta y demanda se retroalimentan.

Inclusive, la propia Comisión Europea ha señalado que "[...] la oferta de mecanismos de evaluación o calificación tampoco es, **por sí misma**, una prueba de influencia o control significativos" (2016, p. 7) [el énfasis es nuestro], opinión para la cual considera que la evaluación y calificación las realiza el usuario final y no la plataforma, por lo que podrían calificar como **herramientas o servicios que califica de auxiliares**.

Sin perjuicio de lo indicado, insistimos en que, del texto de la sentencia, para el caso específico se identificaban aspectos contrarios a la existencia de una relación independiente por parte del prestador. Así, las consecuencias para él derivan no de cómo el usuario final percibe su servicio ni del reconocimiento objetivo a su eficiencia (rapidez, número de servicios diarios, por ejemplo), sino de la verificación de incumplimientos a los términos y condiciones de su relación contractual con la plataforma, elemento adicional a la sola posibilidad de que los usuarios finales calificasen el servicio recibido.

En efecto, si como parte del algoritmo que regula la plataforma se estableciesen penalidades que buscan corregir el quebrantamiento de reglas de conducta impuestas por la empresa al proveedor de servicios en el marco de los términos y condiciones del contrato que las vincula, corresponde que se analice dichas condiciones.

Así, imponer una penalidad por ausencia –específicamente, por "no estar operativo en la franja horaria previamente reservada", situación descrita por el Tribunal Supremo español (S.T.S. 2924/2020, 2020, p. 15)– o por haber cancelado o abandonado un servicio luego de que hubiera sido asignado o aceptado (según sea el caso), parece evidenciar vigilancia, control y subordinación respecto del prestador.

Se trata, ciertamente, de una situación que resulta contradictoria, máxime si consideramos que nos encontramos analizando una relación jurídica en la que, teóricamente, existe amplia libertad para que el prestador decida cuándo ejecutar los servicios que ofrece a través del aplicativo.

En este contexto, al establecer una consecuencia negativa, la empresa se encontrará ejecutando las facultades de dirección (los prestadores de servicios son instruidos de qué deben y qué no deben

hacer), fiscalización (de forma directa, se realiza un control sobre esas incidencias) y sanción de los prestadores (pues, siempre que se presenten las incidencias, la plataforma penaliza al prestador de servicios, por incumplir las reglas de conducta), algo que no es compatible con una relación de servicios independientes.

En el primer caso, consideramos que la ausencia de un prestador no debiera generar impacto en su calificación, pues la libertad de decisión que debe mantener un independiente respecto de su disponibilidad es irrestricta y, de condicionarse, nos encontraríamos ante el establecimiento de una jornada de trabajo, poder que es exclusivo de un empleador.

Por su parte, el 'abandono' o 'cancelación' de un servicio por parte del prestador es un aspecto que puede ser cubierto con la calificación que haga el usuario que se perjudicó con ellos, por lo que la posibilidad de que estos asignen puntuaciones para retroalimentar a otros usuarios con su experiencia cubre de por sí este tipo de situaciones, no siendo necesario que la empresa que administra la plataforma intervenga, pues al hacerlo se encontraría fiscalizando la ejecución, algo que no le compete.

4. El control empresarial permanente a través de la geolocalización por GPS

De conformidad con lo señalado por el Tribunal Supremo español, aunque se tiene como hecho no controvertido que los prestadores de servicios podían elegir libremente la ruta a seguir en cada trayecto,

> [l]a geolocalización por GPS del demandante mientras realizaba su actividad, registrando los kilómetros que recorría, es también un indicio relevante de dependencia en la medida en que **permite el control empresarial en tiempo real del desempeño de la prestación**. Los repartidores están sujetos a un permanente sistema de control mientras desarrollan la prestación del servicio (S.T.S. 2924/2020, 2020, p. 17) [el énfasis es nuestro].

Sobre el particular, llama nuestra atención el evidente salto en la argumentación y la conclusión a la que llega el Tribunal sobre un supuesto control permanente por parte de la plataforma.

De una revisión integral de los considerandos, no se desprende que el GPS hubiere sido utilizado para controlar de manera permanente la ubicación de la persona con un fin distinto al que podría ser administrar las solicitudes de servicios y su asignación más eficiente. Tampoco se acredita que hubiere servido para sancionar al prestador de algún modo.

Efectivamente, ni los antecedentes del pronunciamiento ni los hechos probados indican, por ejemplo, que la empresa se sirviese del uso del GPS para validar que los prestadores de servicios no se aparten de una ruta establecida por ella; de hecho, la sentencia es clara en señalar que el establecimiento de las rutas es libre. Tampoco se indica, por otro lado, que el GPS fuese empleado para calcular el tiempo que toma prestar el servicio y sancionar una supuesta demora.

En este sentido, parece drástico señalar que existe sujeción a un sistema de control permanente cuando, finalmente, la ruta adoptada o el lugar donde se les ubique en determinado momento no les generará consecuencias negativas.

Inclusive, encontramos que el pronunciamiento omite señalar un aspecto relevante en este tipo de economías: el GPS es uno de los componentes esenciales con los que opera la plataforma. Recordemos que la conexión entre oferta y demanda requiere que los usuarios conozcan la ubicación física de ambas partes; inclusive, en los casos en los que la designación se deja al algoritmo y no al usuario, es el GPS el que permite una designación eficiente.

V. CONCLUSIONES

a) La economía de plataformas es un modelo de negocio que implica la prestación de un servicio de interconexión de usuarios, aprovechando para ello la infraestructura digital que sustenta a una plataforma o *app*. A la fecha, no existe en nuestro país legislación dirigida a regularla.

b) Los bienes o servicios que se pueden ofrecer a través de las plataformas digitales son amplios y, contrariamente a la idea que impera en nuestro país, no se limitan a la prestación del servicio de transporte de personas o bienes.

c) Es necesario tener presente que la actividad económica que ejecutan las empresas de la economía de plataformas no es la prestación del servicio que se ofrece a través de su plataforma o *app*.

d) Estas empresas son un intermediario que facilita la concreción de negocios entre sus usuarios: la plataforma virtual es, pues, un espacio donde la oferta y demanda de un

bien o servicio confluyen, facilitando el perfeccionamiento de transacciones.

d) Últimamente y con ocasión de la creciente necesidad de conexión virtual que se ha evidenciado a partir de la pandemia del COVID-19, la potencialidad de las empresas de la economía de plataformas ha salido a relucir: han celebrado alianzas con entidades bancarias para que estas, en aprovechamiento de las *apps* y de la información que se genera con su uso cotidiano, ofrezcan productos del sistema financiero.

Esto ha hecho más evidente que las empresas de la economía de plataformas tienen como finalidad interconectar necesidades de terceros y que son estos terceros quienes celebran y ejecutan negocios jurídicos por su cuenta, siendo ellas totalmente ajenas al servicio ofrecido.

e) En la práctica, los vínculos independientes suscritos entre la empresa titular de la plataforma digital y quienes ofrecen sus servicios a través de ellas pueden desnaturalizarse. Esto dependerá de cómo se ejecuta esta relación y no, de forma automática y predeterminada, del hecho de que nos encontremos ante una empresa de la economía de plataformas.

f) Muchas de las situaciones calificadas como indicios de laboralidad identificados en el contexto de la economía de plataformas no implican, necesariamente, la existencia de un vínculo desnaturalizado pues su existencia responde a situaciones objetivas, que no desdibujan el vínculo autónomo.

No obstante, siempre será necesario evaluar cada caso en concreto y, por ello, la vigencia de los denominados indicios clásicos y los nuevos indicios de laboralidad deberá validarse en cada contexto.

g) A pesar de que reconocemos que los beneficios que pueden generarse en el marco de la economía de plataformas son amplios, es también cierto que las ventajas de este nuevo modelo de negocios no deberán significar, de ninguna forma, el favorecimiento de la precariedad laboral.

Por ello, deberá vigilarse cómo se desarrollan los vínculos contractuales que la conforman para velar por la vigencia de la legislación nacional, lo que incluye no solo las normas laborales sino también fiscales y administrativas.

REFERENCIAS

Arce Ortiz, E. (2008). *Derecho Individual del Trabajo en el Perú: desafíos y deficiencias.* Palestra Editores.

Calderón Paredes, C. (2019). El impacto de las nuevas formas organizativas propias de la economía basada en medios tecnológicos en el mundo del trabajo. *THĒMIS-Revista de Derecho*, (75), 237-253. https://doi.org/10.18800/themis.201901.017

Comisión Europea (2016). *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones - Una Agenda Europea para la Economía Colaborativa*. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016DC0356&from=ES

De Stefano, V. (2016). La "gig economy" y los cambios en el empleo y la protección social. *Gaceta Sindical: reflexión y debate*, (27), 149-172.

Ermida Uriarte, O. & Hernández Álvarez, O. (2002). Crítica de la subordinación. *Ius et Veritas*, (25), 281-295.

Gestión (2 de diciembre de 2020). Restaurantes afiliados a aplicativo de delivery tendrán facilidades para acceder a crédito. https://gestion.pe/economia/restaurantes-afiliados-a-aplicativo-de-delivery-tendran-facilidades-para-acceder-a-creditos-glovo-bcp-nndc-noticia/?ref=gesr

Montoya Melgar, A. (1999). Sobre el trabajo dependiente como categoría delimitadora del Derecho del Trabajo. En J. Cruz Villalón (ed.), *Trabajo subordinado y trabajo autónomo en la delimitación de fronteras de derecho del trabajo: Estudios en homenaje al profesor José Cabrera Bazán* (pp. 57-72). Tecnos.

Neves Mujica, J. (2012). *Introducción al Derecho del Trabajo* (2da ed.). ARA Editores.

Palomeque, M. & Álvarez, M. (2008). *Derecho del Trabajo* (16ta ed.). Centro de Estudios Ramón Areces, S.A.

Perú21 (23 de setiembre de 2020). Interbank y Rappi firman alianza ofrecer mejores servicios financieros digitales en Perú. https://peru21.pe/economia/delivery-interbank-y-rappi-firman-alianza-ofrecer-mejores-servicios-financieros-digitales-en-peru-noticia/?ref=p21r

Sanguineti Raymond, W. (1997). *Contrato de trabajo y nuevos sistemas productivos*. ARA Editores.

Villavicencio Ríos, A. & Vieira, M. (1999). *La protección de los trabajadores en el Perú*. Organización Internacional del Trabajo.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Comisión de Fiscalización de la Competencia Desleal 1 del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, 5 de agosto de 2015, Resolución 074-2015/CD1-INDECOPI, Expediente 212-2014/CCD (Perú).

Comisión de Fiscalización de la Competencia Desleal 1 del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, 5 de agosto de 2015, Resolución 075-2015/CD1-INDECOPI, Expediente 213-2014/CCD (Perú).

Comisión de Fiscalización de la Competencia Desleal 1 del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, 19 de agosto de 2015, Resolución 099-2015/CD1-INDECOPI, Expediente 211-2014/CCD (Perú).

Comisión de Fiscalización de la Competencia Desleal 1 del Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual, 19 de agosto de 2015, Resolución 100-2015/CD1-INDECOPI, Expediente 214-2014/CCD (Perú).

Decreto Supremo 003-97-TR, Decreto Supremo que aprueba el Texto Único Ordenado del Decreto Legislativo 728, Ley de Productividad y Competitividad Laboral, Diario Oficial *El Peruano*, 27 de marzo de 1997 (Perú).

Proyecto de Ley 4243/2018-CR, Ley del Empleo Digno que regula a los trabajadores de Plataformas Digitales, presentado el 16 de abril de 2019 (Perú).

S. Juz. Soc. Barcelona Sec. 31, 11 de junio de 2019, (No. 193/2019) (Esp.)

S.T.S., 20 de enero de 2015, (No. 637/2015) (Esp.).

S.T.S., 25 de septiembre de 2020, (No. 2924/2020) (Esp.).

Sala Especializada en Defensa de la Competencia del Tribunal de Defensa de la Competencia y Propiedad Intelectual, 5 de agosto de 2020, Resolución 084-2020/SDC-INDECOPI, Expediente 0105-2018/CCD (Perú).

Tribunal Constitucional [T.C.], 28 de enero de 2003, sentencia recaída en el Expediente 1944-2002-AA/TC (Perú).

Tribunal Constitucional [T.C.], 6 de noviembre de 2007, sentencia recaída en el Expediente 9197-2006-AA-TC (Perú).

Tribunal Constitucional [T.C.], 8 de julio de 2015, sentencia recaída en el Expediente 03917-2012-PA/TC (Perú).

10.18800/themis.202101.025

LAS NUEVAS TECNOLOGÍAS Y LA PROTECCIÓN DE DATOS EN EL ENTORNO LABORAL: RETOS Y PERSPECTIVAS LEGALES

NEW TECHNOLOGIES AND DATA PROTECTION IN THE WORKPLACE: CHALLENGES AND LEGAL PERSPECTIVES

Iván Blume Moore*
Rodrigo, Elías & Medrano

Information and communications technologies, known as ICT, have undoubtedly contributed to the development of societies through the multiplication of data processing and storage in everyday relationships. At the same time and notwithstanding, it is not possible to ignore the risks that these have caused, in relation to the lack of security of personal data. This situation has generated the development of regulatory frameworks aimed at counteracting such risks. Among these regulations, there are the ones relating to the workplace.

In this article, the author reviews the novelties brought about by the entry into force of the Personal Data Protection Law (Law 29733) in Peruvian law. Subsequently, he points out and describes the basic concepts involved in the topic of personal data protection. In a third section, he develops the obligations of employers regarding the protection of personal data and the challenges that this faces in the face of global changes. Finally, he illustrates all this through cases of jurisprudence.

Keywords: Personal data protection; Information and Communication Technologies; Personal Data Protection Law; employer; worker; employment relationship.

Las tecnologías de información y comunicación, conocidas como TIC, han aportado, sin duda alguna, al desarrollo de las sociedades a través de la multiplicación del procesamiento y almacenamiento de datos en las relaciones cotidianas. Sin perjuicio de ello, y en contrapartida, no es posible desconocer los riesgos que, al mismo tiempo, aquellas han causado, relativos a la falta de seguridad de los datos personales. Esta situación ha generado el desarrollo de marcos normativos destinados a contrarrestar tales riesgos. Entre esta normativa, se encuentra aquella relativa al ámbito laboral.

En el presente artículo, el autor revisa las novedades que trajo consigo la entrada en vigencia de la Ley de Protección de Datos Personales (Ley 29733) en el ordenamiento peruano. Posteriormente, señala y describe los conceptos básicos que intervienen en el tópico de la protección de datos personales. En una tercera sección, desarrolla las obligaciones de los empleadores frente a la protección de datos personales y los desafíos que ello enfrenta ante los cambios globales. Por último, ilustra todo ello a través de casos de la jurisprudencia.

Palabras clave: Protección de datos personales; tecnologías de información y comunicación; Ley de Protección de Datos Personales; empleador; trabajador; relación laboral.

* Abogado. Máster en Relaciones Industriales y Laborales por la Universidad de Cornell. Asociado en el Estudio Rodrigo, Elías & Medrano (Lima, Perú). Contacto: iblume@estudiorodrigo.com

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 1 de febrero de 2021, y aceptado por el mismo el 16 de junio de 2021.

I. INTRODUCCIÓN

La multiplicación del procesamiento y almacenamiento de datos a partir de las relaciones e interacciones cotidianas es una de las muchas formas en que las tecnologías de información y comunicación (en adelante, TIC) han transformado nuestras vidas. Al tiempo que nos han facilitado la vida cotidiana y ampliado el acceso a la información, también han generado riesgos relacionados principalmente con el uso incontrolado y la falta de seguridad de los datos personales. Esto a su vez ha llevado al surgimiento de marcos normativos para hacerle frente a esos riesgos, de los que se desprenden relativamente nuevas obligaciones y responsabilidades legales para quienes intervienen en el tratamiento de datos personales.

En el ámbito laboral, por ejemplo, la mediación de dichas tecnologías incluye procesos tan diversos como la gestión de personal, las comunicaciones internas y externas y las formas de monitoreo y control del trabajo, entre otras. Por efecto de todo ello, los empleadores captan, procesan y almacenan una gran cantidad de datos e información sobre sus trabajadores. En todos esos procesos deben asegurarse de cumplir con lo dispuesto en las normativas sobre protección de datos.

En el Perú se cuenta desde el 3 de julio de 2011 con la Ley 29733, Ley de Protección de Datos Personales (en adelante, LPDP), que define los conceptos básicos que se deben tener en cuenta en esta materia. Sin embargo, el desarrollo legislativo y jurisprudencial no logra ir siempre al paso de los avances de las TIC, ni de los dilemas que surgen de sus aplicaciones en todos los ámbitos de las relaciones sociales, incluyendo al trabajo. Ello plantea una serie de retos jurídicos y tecnológicos sobre cómo garantizar de manera efectiva el derecho a la protección de datos de los trabajadores, así como sobre sus alcances y límites frente a otros derechos y obligaciones que emergen de las relaciones laborales.

En este artículo nos proponemos revisar algunos de esos retos a partir de desarrollos normativos y jurisprudenciales recientes sobre el alcance de la protección de datos personales en casos específicos de aplicaciones tecnológicas que se enmarcan o son relevantes dentro del contexto laboral. Examinaremos estos casos a la luz de los principios consagrados en el marco legal vigente y de los criterios básicos sobre las obligaciones frente al derecho a la protección de los datos personales que se desprenden de la legislación nacional. Asimismo, nos ocuparemos en especial de las orientaciones generales formuladas por la Organización Internacional del Trabajo (en adelante, OIT) y de la guía recientemente publicada por la Agencia Española de Protección de Datos (en adelante, AEPD) sobre la protección de datos en las relaciones laborales. El propósito no es hacer un estudio comparado de la legislación internacional, sino ofrecer un panorama general de los conceptos fundamentales que se deben tener en cuenta al abordar estos temas dentro del ámbito laboral, así como llamar la atención sobre algunos temas novedosos o poco desarrollados que merecen mayor atención en nuestro país.

Con este fin, dividimos este artículo en cuatro secciones. En la primera, nos referiremos a las novedades que introdujo la LPDP en el ordenamiento jurídico peruano y los antecedentes en los desarrollos jurídicos nacionales e internacionales que llevaron a su adopción. En la segunda sección, a partir de las definiciones contenidas en la LPDP y en su correspondiente reglamento, presentamos los conceptos básicos que fundamentan la regulación de la protección de los datos personales. La tercera se ocupa específicamente de las obligaciones de los empleadores frente a la protección de los datos personales de sus trabajadores y revisa los principales desafíos ante los cambios globales, no solo tecnológicos, sino sociales. Finalmente, en la última sección revisaremos tres casos que ilustran la aplicación de los principios generales presentados en las secciones anteriores a situaciones y aplicaciones tecnológicas específicas.

II. LA LEY DE PROTECCIÓN DE DATOS PERSONALES Y SUS ANTECEDENTES

Con la expedición de la LPDP, el Congreso peruano reconoció explícitamente la protección de datos personales como un derecho fundamental y se propuso regular su adecuado tratamiento tanto por las entidades públicas, como por las instituciones privadas (Ley 29733, 2011). Las disposiciones de esta ley y su correspondiente reglamento constituyen normas de orden público y de cumplimiento obligatorio[1].

Antes de la aprobación de la LPDP, el principal referente para la resolución de los conflictos en torno al tratamiento de datos personales era el inciso 6

[1] La LPDP establece lo siguiente:

Artículo 1.- Objeto de la ley

La presente ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen (Ley 29733, 2011).

del artículo 2 de la Constitución Política que consagra el derecho de las personas "a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar" (Constitución Política del Perú [Const.], 1993). El inciso 7 del mismo artículo, además de consignar el derecho "al honor y a la buena reputación, a la intimidad personal y familiar", establece el derecho "a la voz y a la imagen propias" (Const., 1993). Adicionalmente, el inciso 4 del artículo 200 establece el proceso de *habeas data* para garantizar la protección de este derecho (Const., 1993).

Es decir, desde principios de los noventa el constituyente había identificado los potenciales riesgos que se derivaban de la capacidad de registro y almacenamiento de los datos personales por parte de medios audiovisuales e informáticos, pero enmarcaba la protección frente a dichos riesgos como una cuestión pertinente al derecho a la intimidad. Con la aprobación de la LPDP, no solo se desarrollan con mayor claridad las disposiciones constitucionales, sino que se introduce en el ordenamiento jurídico peruano la noción del derecho a la protección de datos como un derecho autónomo con un alcance que va más allá de la protección de la intimidad. Recoge así un concepto que ya había sido plasmado en la legislación de otros países y al que, incluso, ya habían hecho referencia algunas decisiones a nivel local.

Por ejemplo, el Tribunal Constitucional (en adelante, TC), en la sentencia sobre el proceso de *habeas data* tramitado bajo el Expediente 1797-2002-HD/TC, había señalado lo siguiente:

> […] aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar […]. Ello se debe a que mientras que este protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen (2003, fundamento 3).

Como veremos, esta facultad de todo individuo de controlar sus datos personales es el principio básico de las normativas sobre protección de datos personales. La insuficiencia del derecho a la intimidad para garantizar dicha protección en el contexto tecnológico actual la explica Castro Cruzatt:

> […] en el contexto del creciente desarrollo informático y tecnológico se advirtió también que el registro indiscriminado de datos personales, su interrelación y posterior transmisión descontrolada, confiere un alto poder de control sobre los titulares de dichos datos, llegando a representar una nueva forma de dominio social a la que le ha denominado Poder Informático (2008, p. 261).

Es decir, hoy es tan extendido el uso la tecnología informática que los requerimientos de protección no pueden solamente limitarse a la necesidad de resguardar la intimidad, pues existen una serie de riesgos relacionados al uso masivo de la información de las personas que van desde el perfilamiento hasta los fraudes bancarios que hacen especialmente necesario la protección de los datos personales.

A este contexto busca precisamente responder el desarrollo normativo y jurisprudencial sobre la protección de datos personales. En Perú, el marco legal está conformado principalmente por la LPDP y su reglamento, aprobado por Decreto Supremo 003-2013-JUS (2013) (en adelante, Reglamento). Se han emitido además directivas sobre seguridad de la información y sistemas de videovigilancia[2].

III. CONCEPTOS BÁSICOS

La aplicación de la anterior normativa a casos específicos requiere tener clara una serie de conceptos básicos definidos por la LPDP y por su Reglamento. Presentamos a continuación un resumen de los conceptos más relevantes a modo de preguntas y respuestas.

A. ¿Qué es un dato personal?

Lo primero que se debe tener claro es la amplitud de esta denominación. Dentro de ella se incluye, según el inciso 4 del artículo 2 del Reglamento, "información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales o de cualquier tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que pueden ser razonablemente utilizados" (Decreto Supremo 003-2013-JUS, 2013). Así, la LPDP solo protege los datos de personas naturales. Los datos de personas jurídicas no son parte de su ámbito de aplicación.

Los desarrollos tecnológicos han ido ampliando el listado de datos que pueden caber dentro de esta

[2] Véase, Resolución Directoral 019-2013-JUS/DGPDP, del 11 de octubre de 2013, y Resolución Directoral 02-2020-JUS/DGTAIPD, del 14 de febrero de 2020.

definición. Actualmente, por ejemplo, un dato personal de gran relevancia es la información de geolocalización. La Autoridad Nacional de Protección de Datos Personales (en adelante, ANPDP), en la Resolución Directoral 008-2017-JUS/DGPDP (2017), ha concluido que la geolocalización es un dato personal. Al respecto, ha señalado que

> […] debido al rápido desarrollo tecnológico que viene dándose en nuestra sociedad, los teléfonos móviles inteligentes o dispositivos electrónicos de naturaleza similar permiten la geolocalización y con ello la identificación de una persona, ya que con ellos se conoce el desplazamiento de un determínalo individuo. Esto último se da pues estos teléfonos móviles inteligentes o dispositivos electrónicos de naturaleza similar se mantienen cerca de la persona desde su bolsillo hasta la mesa de noche que se encuentra en su habitación. En consecuencia, la identificación de una persona que se da a través de la información generada por la ubicación de un teléfono móvil inteligente o dispositivo electrónico de naturaleza similar constituye un dato personal, siendo de aplicación las disposiciones contenidas en la LPDP y su Reglamento (p. 14).

Los datos sensibles son objeto de especial protección (Ley 29733, 2011, art. 3). Dentro de estos se incluyen: información biométrica que permita la identificación de una persona; datos sobre identidad racial o étnica; información sobre la situación económica (ingresos, patrimonio, deudas, etc.); opiniones o adscripciones políticas o religiosas; afiliación sindical; datos sobre la salud física o mental; hechos que correspondan a la vida afectiva, familiar o a la esfera más íntima de las personas; entre otros.

En estos casos, el consentimiento debe ser otorgado por escrito y debe ser clara la justificación para recolectar, almacenar y tratar datos sensibles. Asimismo, de acuerdo con el Reglamento, la finalidad debe ser legítima, concreta y acorde con las actividades o fines explícitos del titular del banco de datos personales (Decreto Supremo 003-2013-JUS, 2013).

B. ¿Qué es un banco de datos o base de datos personales?

Banco de datos es un *"*conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera sea la forma o modalidad de su creación, formación, almacenamiento, organización y acceso*"* (Ley 29733, 2011, art. 2 inciso 2). El titular de la base de datos personales puede ser una "persona natural o jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad" (Ley 29733, 2011, art. 2 inciso 15).

Sin que necesariamente sean conscientes de las obligaciones que se desprenden de ello, los empleadores son titulares de bases de datos con la información personal de sus trabajadores que recolectan y tratan en las diferentes etapas de la relación laboral. Son bases de datos típicas del entorno laboral los legajos de los trabajadores, la información de candidatos para los procesos de selección, la información de salud ocupacional de los trabajadores, los sistemas de videovigilancia, entre otros.

C. ¿Qué constituye un tratamiento de datos?

La LPDP y el Reglamento de la LPDP se aplican a toda modalidad de tratamiento de datos personales, ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado, e independientemente del soporte en el que se encuentren (Decreto Supremo 003-2013-JUS, 2013, art. 3).

La LPDP define al tratamiento de datos personales como

> cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales (Ley 29733, 2011, art. 2 inciso 19).

D. ¿Cuáles son las principales obligaciones establecidas por la normativa de protección de datos?

Las principales obligaciones para cumplir con la normativa de protección de datos son las siguientes:

a) **Obtener consentimiento:** la protección de datos supone, en primer lugar, que todo 'tratamiento' se realice con el consentimiento previo, informado y expreso del titular, salvo excepciones establecidas por la ley. Así, el consentimiento relativo a datos sensibles debe ser obtenido por escrito. Se considera consentimiento escrito a aquel que otorga el titular mediante un documento con su firma autógrafa, huella dactilar o cualquier otro mecanismo autorizado por el ordenamiento jurídico que queda o pueda ser impreso en

una superficie de papel o similar. Tratándose del entorno digital, el consentimiento escrito podrá otorgarse mediante firma electrónica, mediante escritura que quede grabada, de forma tal que pueda ser leída e impresa, o que por cualquier otro mecanismo o procedimiento establecido permita identificar al titular y recabar su consentimiento, a través de texto escrito.

b) **Cumplir con el deber de información:** el titular del banco de datos debe dar a conocer al titular de los datos personales toda la información relevante sobre los usos y el 'tratamiento' que se le dará a estos. Se debe informar de manera completa y veraz antes de la recopilación de los datos[3].

c) **Asegurar la confidencialidad y la seguridad:** la responsabilidad por el manejo de los datos personales recae no solo sobre el titular del banco de datos, sino sobre todos los que intervengan en su tratamiento. Todos ellos están obligados a garantizar la confidencialidad y la seguridad de los datos personales. La responsabilidad se extiende más allá de la finalización de las relaciones con el titular del banco de datos personales. Esto supone la obligación de adoptar las medidas que sean necesarias, tanto técnicas como legales y organizacionales, para impedir la filtración, alteración o el uso inadecuado de esos datos.

d) **Conservar la información por tiempo limitado:** la protección implica también que los datos personales no se conserven más tiempo del necesario que se requiera para cumplir con la finalidad del tratamiento. El tiempo permitido de conservación depende del tipo de relación y de las correspondientes obligaciones legales y contractuales. Podemos decir que se pueden conservar mientras persistan las responsabilidades legales derivadas de dicha relación.

e) **Garantizar los derechos ARCO:** esta sigla se refiere a los derechos al acceso, rectificación, cancelación y oposición, que sintetizan los atributos del control que se le debe garantizar a las personas sobre sus datos personales. Cada uno de estos derechos está sujeto a sus propias formalidades.

f) **Inscripción de bases de datos:** los titulares de las bases de datos deben inscribirlos en el Registro Nacional de Protección de Datos Personales.

g) **Requisitos para el flujo de datos transfronterizo:** en caso de que los datos se transfieran fuera del territorio nacional, el titular de la base de datos debe informarlo a la autoridad nacional de protección de datos. Solo se puede realizar dicha transferencia a países que cuenten con una normativa apropiada de protección de datos. En caso contrario, se debe obtener el consentimiento informado del titular para realizar la transferencia y tomar medidas que garanticen que el tratamiento de los datos cumpla con los requisitos de la ley.

E. ¿Qué casos están exceptuados del consentimiento informado para el tratamiento de datos personales?

Enumeramos a continuación los casos previstos en la LPDP, en los cuales no se requiere el consentimiento del titular de datos personales[4]:

[3] El artículo 18 de la LPDP establece que

> el titular de datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados; quiénes son o pueden ser sus destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del o de los encargados del tratamiento de sus datos personales; el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserven sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello (Ley 29733, 2011).

Asimismo, el Reglamento establece que se le deberá comunicar al titular de los datos personales clara, expresa e indubitablemente, con lenguaje sencillo, cuando menos lo siguiente:

a) La identidad y domicilio o dirección del titular del banco de datos personales o del responsable del tratamiento al que puede dirigirse para revocar el consentimiento o ejercer sus derechos.
b) La finalidad o finalidades del tratamiento a las que sus datos serán sometidos.
c) La identidad de los que son o pueden ser sus destinatarios, de ser el caso.
d) La existencia del banco de datos personales en que se almacenarán, cuando corresponda.
e) El carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, cuando sea el caso.
f) Las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo.
g) En su caso, la transferencia nacional e internacional de datos que se efectúen (Decreto Supremo 003-2013-JUS, 2013, artículo 12 inciso 4).

[4] Resumen tomado de Blume Moore (2021, pp. 275-276).

1) Cuando los datos personales se recopilen o transfieran para el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias.
2) Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles para el público.
3) Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley.
4) Cuando medie norma para la promoción de la competencia en los mercados regulados emitida en ejercicio de la función normativa por los organismos reguladores a que se refiere la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, o la que haga sus veces, siempre que la información brindada no sea utilizada en perjuicio de la privacidad del usuario.
5) Cuando los datos personales sean necesarios para la preparación, celebración y ejecución de una relación contractual en la que el titular de datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento.
6) Cuando se trate de datos personales relativos a la salud y sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico del titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud, observando el secreto profesional; o cuando medien razones de interés público previstas por ley o cuando deban tratarse por razones de salud pública, ambas razones deben ser calificadas como tales por el Ministerio de Salud; o para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.
7) Cuando el tratamiento sea efectuado por organismos sin fines de lucro cuya finalidad sea política, religiosa o sindical y se refiera a los datos personales recopilados de sus respectivos miembros, los que deben guardar relación con el propósito a que se circunscriben sus actividades, no pudiendo ser transferidos sin consentimiento de aquellos.
8) Cuando se hubiera aplicado un procedimiento de anonimización o disociación.
9) Cuando el tratamiento de los datos personales sea necesario para salvaguardar intereses legítimos del titular de datos personales por parte del titular de datos personales o por el encargado de tratamiento de datos personales.
10) Cuando el tratamiento sea para fines vinculados al sistema de prevención de lavado de activos y financiamiento del terrorismo u otros que respondan a un mandato legal.
11) En el caso de grupos económicos conformados por empresas que son consideradas sujetos obligados a informar, conforme a las normas que regulan a la Unidad de Inteligencia Financiera, que éstas puedan compartir información entre sí de sus respectivos clientes para fines de prevención de lavado de activos y financiamiento del terrorismo, así como otros de cumplimiento regulatorio, estableciendo las salvaguardas adecuadas sobre la confidencialidad y uso de la información intercambiada.
12) Cuando el tratamiento se realiza en ejercicio constitucionalmente válido del derecho fundamental a la libertad de información.
13) Otros que deriven del ejercicio de competencias expresamente establecidas por Ley (Ley 29733, 2011, art. 14).

F. ¿Qué principios rigen el tratamiento de los datos personales según el marco legal?

Los principios que rigen el tratamiento de los datos personales, en concordancia con la normativa actual, son los siguientes:

> **Artículo 4. Principio de legalidad**: el tratamiento de los datos personales se hace conforme a lo establecido en la LPDP. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos.
>
> **Artículo 5. Principio de consentimiento:** para el tratamiento de los datos personales debe mediar el consentimiento de su titular.
>
> **Artículo 6. Principios de finalidad:** los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.
>
> **Artículo 7. Principio de proporcionalidad:** todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.
>
> **Artículo 8. Principio de calidad:** los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fue-

ron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento.

Artículo 9. Principio de seguridad: el titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

Artículo 10. Principio de disposición de recurso: todo titular de datos personales debe contar con las vías administrativas o jurisdiccionales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales.

Artículo 11. Principio de nivel de protección adecuado: para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por la LPDP o por los estándares internacionales en la materia (Ley 29733, 2011, arts. 4-11) [el énfasis es nuestro].

IV. OBLIGACIONES DE LOS EMPLEADORES FRENTE A LOS DATOS PERSONALES DE SUS TRABAJADORES

Los principios que enunciamos en el punto anterior aplican en términos generales al ámbito laboral. Sin embargo, en el caso de las relaciones laborales, el empleador no requiere un consentimiento expreso cuando la finalidad del tratamiento se pueda enmarcar en las obligaciones previstas en el contrato de trabajo. Aunque no requiere consentimiento, sí está obligado a informarle al trabajador sobre el tratamiento que se les dará a los datos.

Sin embargo, en nuestro país la mayoría de empleadores no son conscientes de que en la relación con sus trabajadores actúan como titulares legales de bases de datos personales y que como tales son responsables de las obligaciones previstas en la LPDP. Cumplir con esas obligaciones implica tomar medidas para garantizar la seguridad y confidencialidad de los datos, así como para evitar su alteración, pérdida, tratamiento o acceso no autorizado. No tomarlas pone en riesgo la protección de derechos fundamentales de los trabajadores y expone a los empleadores a las correspondientes sanciones.

Por otro lado, son escasos los desarrollos normativos y la jurisprudencia sobre la aplicación del derecho a la protección de datos en el ámbito, y los requerimientos específicos de las relaciones laborales. Teniendo en cuenta lo anterior, es útil revisar algunos referentes internacionales. Por ejemplo, la publicación titulada Protection of Worker's Personal Data (International Labour Office Geneva, 1997) contiene una especie de código adoptado a principios de octubre de 1996 en una Reunión de Expertos de la OIT en materia de privacidad de los trabajadores, siguiendo las decisiones del Órgano de Gobierno de la OIT en su sesión de noviembre de 1995. En este documento se señala lo siguiente:

a) El tratamiento de datos personales de los trabajadores debería efectuarse de manera ecuánime y lícita, y limitarse exclusivamente a asuntos directamente pertinentes a la relación de empleo del trabajador.

b) En principio, los datos personales deberían utilizarse únicamente para el fin con el cual hayan sido acopiados.

c) Los empleadores deberían evaluar periódicamente sus métodos de tratamiento de datos, con el objeto de: (i) reducir lo más posible el tipo y el volumen de datos personales acopiados, y (ii) mejorar el modo de proteger la vida privada de los trabajadores.

d) Las personas encargadas del tratamiento de datos personales deberían recibir periódicamente una formación que les permita comprender el proceso de acopio de datos y el papel que les corresponde en la aplicación de los principios.

e) El tratamiento de datos personales no debería conducir a una discriminación ilícita en materia de empleo u ocupación.

f) Todas las personas, tales como los empleadores, los representantes de los trabajadores, las agencias de colocación y los trabajadores, que tengan acceso a los datos personales de los trabajadores deberían tener una obligación de confidencialidad, de acuerdo con la realización de sus tareas y el ejercicio de los principios de tratamiento de datos.

g) Los empleadores deberían garantizar, mediante las salvaguardias de seguridad que permitan las circunstancias, la protección de los datos personales contra su pérdida y todo acceso, utilización, modificación o comunicación no autorizados.

h) Los empleadores deberían verificar periódicamente que los datos personales conservados son exactos, actualizados y completos (International Labour Office Geneva, 1997).

Los rápidos desarrollos tecnológicos y la evolución de las relaciones sociales que permea también el ámbito laboral plantea una serie de retos no solo jurídicos, sino prácticos para el cumplimiento por parte del empleador de las normativas y principios generales en casos específicos. En este sentido, un referente que puede llegar a ser muy ilustrativo es la guía sobre la protección de datos personales en las relaciones laborales publicada recientemente por la AEPD. Dicha publicación no solo resume el nuevo marco normativo español y europeo sobre protección de datos, sino que proporciona orientaciones de carácter práctico, no vinculante, para facilitar el cumplimiento de la legislación.

Con ese fin, el documento fue elaborado con la participación tanto del Ministerio del Trabajo como de organizaciones empresariales y sindicales. Recoge además "la experiencia atesorada por la AEPD a lo largo de los años" (Agencia Española de Protección de Datos [AEPD], 2021, p. 6). Esto le permite ofrecer un panorama comprehensivo de las múltiples facetas de la gestión de personal y la relación laboral en las que surge la necesidad de la protección de datos personales.

Nos referiremos a algunas recomendaciones específicas que trae la guía en el siguiente apartado, cuando revisemos ejemplos de problemáticas concretas que surgen a partir de algunas aplicaciones informáticas. Vale la pena, sin embargo, mencionar de manera general los temas que introduce o desarrolla la guía y que pueden ser relevantes para nuestro medio (AEPD, 2021):

a) La necesidad de contar con estándares para el tratamiento de datos personales en los procesos de selección de personal. Se aclara que, dentro del marco legal español, el proceso de selección no exige el consentimiento de la persona candidata, pero que se debe cumplir con el deber de informar y las demás obligaciones propias del tratamiento de los datos personales. La empresa es responsable de la custodia de la documentación entregada por la persona candidata (como el *currículum vitae*) y será responsable por su pérdida, sustracción o el uso indebido de la información allí contenida.

b) El uso de la información de las redes sociales de los trabajadores. La guía aclara que, aunque el perfil en las redes sociales de un candidato a un empleo sea de acceso público, el empleador necesita una base jurídica válida para "efectuar un tratamiento de los datos obtenidos por esa vía" (AEPD, 2021, p. 22). Las personas no están obligadas a permitir que el empleador indague en sus perfiles de redes sociales, ni durante el proceso de selección ni durante la ejecución del contrato.

c) La protección de la privacidad de las víctimas de acoso laboral o de violencia de género, así como de quienes presentan cualquier tipo de denuncia interna. Estos son casos especialmente sensibles de protección de datos personales que obligan al empleador a implementar medidas y mecanismos que protejan la identidad de las personas involucradas.

d) El uso de los mecanismos lo menos invasivos posibles y la restricción de la publicación de la información obtenida a través de herramientas de control, como el registro de jornada obligatorio, los controles de ingreso, la georreferenciación o la videovigilancia (sobre esto último punto, profundizaremos más adelante).

e) Los riesgos y obligaciones frente a los datos personales derivados de la responsabilidad del empleador de velar por la salud de los trabajadores. En España, al igual que en Perú, esta responsabilidad faculta al empleador a realizar vigilancia periódica del estado de salud de sus trabajadores. Aspecto que ha adquirido una especial relevancia en el contexto de la pandemia y al que nos referiremos más adelante.

f) En términos de aplicaciones tecnológicas, lo más novedoso que incluye la guía es lo relativo al uso de algoritmos o sistemas de inteligencia artificial para tomar decisiones en cuanto al acceso (procesos de selección), condiciones y mantenimiento del empleo. La normatividad española obliga al empleador a informar sobre los parámetros en los que se basa el algoritmo y a tomar medidas que eviten que estos produzcan algún tipo de discriminación (AEPD, 2021).

V. DECISIONES RECIENTES SOBRE PROTECCIÓN DE DATOS EN SITUACIONES Y DESARROLLOS TECNOLÓGICOS ESPECÍFICOS

Aunque en nuestro país no es mucho lo que se ha avanzado en el establecimiento de reglas específicas para la protección de datos personales en situaciones o usos de tecnologías particulares, existen algunos desarrollos normativos y jurisprudenciales recientes que han empezado a abordar la problemática concreta que surge a partir de algunas aplicaciones informáticas, como los correos electrónicos, las redes sociales institucionales o la videovigilancia.

Por otro lado, la emergencia del COVID-19 puso al descubierto las tensiones que pueden surgir entre la necesidad de proteger la salud, evitando la propagación del virus, y el derecho a la protección de los datos personales. Esto obligó al gobierno a pronunciarse a través de una opinión consultiva sobre el tratamiento de datos de salud durante la pandemia en el ámbito laboral. Si bien en esta no se aborda directamente el uso de tecnologías, por su urgencia y actualidad consideramos pertinente examinar las principales consideraciones que el reto de controlar la epidemia plantea en cuanto a protección de datos personales y las obligaciones de los empleadores de velar por la salud de sus trabajadores.

Al respecto, revisaremos a continuación algunas decisiones jurisprudenciales o actos regulatorios recientes.

A. La inviolabilidad de las comunicaciones en tiempos del *e-mail* y las redes sociales

Si bien desde hace ya más de veinte años se generalizó el uso del correo electrónico como herramienta de trabajo de las empresas, persisten aún dudas sobre cómo se deben aplicar en el contexto actual los principios que protegían las comunicaciones antes de la era digital. Además del ya mencionado derecho a la intimidad, el principal referente para el tratamiento de las comunicaciones antes de que se considerara la protección de los datos personales como un derecho autónomo era el principio de la inviolabilidad de las comunicaciones. Desarrollado originalmente para evitar que alguien distinto al destinatario abriera la correspondencia, el principio se extendió más tarde a las comunicaciones telegráficas y telefónicas (Vegas Torres, 2011, p. 34). Atendiendo a dicho principio, las comunicaciones solo pueden ser interceptadas por terceros por orden de un juez y siguiendo un procedimiento regular.

Estos principios se extienden por analogía al correo electrónico. Sin embargo, su uso generalizado como herramienta laboral plantea algunas dudas sobre el alcance de este principio en dicho ámbito. En particular, ¿qué pasa con las comunicaciones que se realizan por medio de las cuentas institucionales o de los equipos de computación que la empresa entrega a los trabajadores? ¿son comunicaciones privadas protegidas por los principios de inviolabilidad de la correspondencia o del derecho a la intimidad? ¿O, al ser una herramienta de trabajo por medio de las cuales las empresas suelen llevar buena parte de sus procesos e interacciones, tiene derecho el empleador a acceder a esas comunicaciones como parte de sus funciones de control y supervisión del trabajo?

Tanto en nuestro país como en el ámbito internacional, esta disyuntiva ha conducido a un debate jurídico que aún no se ha resuelto del todo. La posición de varias sentencias del TC ha sido consistente en considerar que los trabajadores están protegidos por el principio de inviolabilidad de las comunicaciones, aun si se comunican a través de los equipos y las cuentas de correo suministrados por el empleador. El TC incluso ha declarado ilegal el despido o la sanción disciplinaria de un empleado por conductas que iban en contra del reglamento interno de trabajo (como enviar correos con material pornográfico en horarios laborales desde cuentas oficiales) porque la prueba de ese comportamiento se obtuvo accediendo al correo institucional sin acudir a un proceso judicial[5]. En años recientes, esta tendencia jurisprudencial ha sido ratificada por una controvertida decisión de la Corte Suprema (en adelante, CS). En respuesta a una demanda iniciada por el sindicato de una empresa, consideró como un 'exceso' que en el reglamento interno laboral el empleador señalara que era propietario de las cuentas de correo institucionales y que eso le permitía revisar su contenido para fines de control, pues ello desconocía el derecho a la intimidad e inviolabilidad de las comunicaciones de los trabajadores[6].

Sin embargo, algunas decisiones recientes parecen estar señalando un cambio, o al menos una matización, de esta línea jurisprudencial garantista. En efecto, en la sentencia recaída en el Expediente 00943-2016-PA/TC, discutido en el Pleno de Sentencia 412/2020 de 14 de julio de 2020, el TC consideró por primera vez la posibilidad del empleador de poder revisar los correos electrónicos que le ha proporcionado al trabajador para el desarrollo efectivo de sus actividades, sin vulnerar con ello derechos constitucionales. Aunque no hubo la mayoría necesaria para formar sentencia al respecto, los conceptos expresados por los magistrados parecen apuntar a una flexibilización en la interpretación del principio de inviolabilidad de la correspondencia aplicado a los correos y redes institucionales de las empresas[7].

[5] Para mayor información, véase la sentencia recaída en el Expediente 1058-2004-AA/TC (2020).

[6] Para mayor información, véase la Casación 14614-2016 (2017).

[7] En un proceso de amparo ante el TC, una sentencia se forma a partir del voto conforme de cuatro magistrados. En este caso, la sentencia fue declarada improcedente debido a que dos magistrados (Ledesma y Miranda) consideraron que el caso debió resolverse en la vía ordinaria laboral, y otros dos (Sardón y Ferrero) siempre han estimado que la protección

El caso corresponde a un proceso de reposición seguido en la vía de amparo. En este se invocaba la vulneración de los derechos constitucionales al trabajo, al secreto y la inviolabilidad de las comunicaciones, a la intimidad personal, entre otros. El trabajador denunció que, para imputarle las faltas, la empresa accedió a una conversación en Facebook entre su persona y una asistente de la empresa, interviniendo una conversación de carácter privado.

El TC reiteró la línea jurisprudencial en el sentido de que, aun cuando las cuentas y los equipos sean provistos por la compañía, el trabajador mantiene una esfera de privacidad y de autodeterminación personal en el uso que hace de ellos, por lo que la empresa no tiene la prerrogativa de atribuirse la titularidad de las comunicaciones y los documentos pertenecientes a las redes de sus trabajadores. Sin embargo, consideró algunas circunstancias en las que el empleador podría acceder a las comunicaciones de sus trabajadores en el marco de procesos de monitoreo laboral o de procesos disciplinarios, sin el requisito de una orden judicial. Para ello, tuvo en cuenta en la discusión algunos referentes internacionales.

Menciona, por ejemplo, que el Tribunal Europeo de Derechos Humanos ha establecido los siguientes criterios para determinar si el empleador puede monitorear la comunicación de sus trabajadores: (i) el trabajador debe ser informado previamente y con claridad de las medidas de control que la empresa puede utilizar (y el alcance de estas); (ii) el empleador debe optar por la acción menos intrusiva en la vida personal y familiar del trabajador; (iii) se debe acreditar la existencia de motivos objetivos y concretos que justifiquen la necesidad de fiscalizar las comunicaciones del trabajador; y (iv) la medida de fiscalización se debe llevar de forma previa al inicio del procedimiento disciplinario (*Bărbulescu c. Romania*, 2017).

Por su parte, el Tribunal Constitucional español ha establecido que: (i) el control o fiscalización se debe realizar con garantías (como, por ejemplo, a través de un petitorio informático y notario); (ii) el contenido fiscalizado no puede ser sobre aspectos personales y familiares del trabajador, sino únicamente de la actividad empresarial realizada; y (iii) debe existir proporcionalidad entre la posible infracción del trabajador y la afectación a su privacidad por parte de la actividad fiscalizadora de la empresas (STC 170/2013, 2013).

Teniendo en cuenta lo anterior, el TC peruano consideró que sí es posible intervenir o fiscalizar el correo institucional del trabajador si previamente se le ha comunicado de dicha posibilidad y de sus alcances, y si dicha intervención contempla criterios de proporcionalidad con relación al grado de afectación a la privacidad y al fin último de la intervención (en este caso, determinar una infracción del trabajador).

No obstante, para el TC, el empleador no puede ejercer esta prerrogativa si se trata del acceso a una red social del trabajador, puesto que es un medio de comunicación externo a los instrumentos que brinda el empleador. Aunque no profundiza mucho en este aspecto, la discusión dentro del órgano también pone en evidencia los retos que plantean las redes sociales y otras formas de interacción social por medio de tecnologías digitales para la aplicación de los principios de inviolabilidad de las comunicaciones y protección de la intimidad en el ámbito laboral.

Por ejemplo, será necesario revisar qué ocurre cuando no se trata de redes sociales personales del trabajador, sino de actividades de *community manager* en las redes sociales institucionales. Esta preocupación fue señalada por uno de los magistrados en el mencionado expediente[8], quien se apartó de la opinión mayoritaria sobre las redes sociales considerando que el empleador podría fiscalizar el uso de las redes institucionales de quien le esté prestando los servicios de *community manager*, con la finalidad de asegurar un grado de idoneidad en el servicio brindado al cliente y en la imagen de la empresa.

Una decisión anterior correspondiente a la CS apunta en un sentido similar en cuanto a una mayor flexibilización de la protección a la inviolabilidad de las comunicaciones cuando se trata de correos institucionales, así como resalta la necesidad de monitoreo y control por parte de los empleadores, el cual no se refiere a un control disciplinario, sino a una investigación interna por la posible comisión de un delito. En el Recurso de Nulidad 817-2016, la CS anuló una sentencia previa que excluía de un proceso penal por colusión las pruebas obtenidas mediante el acceso del empleador sin

constitucional contra un despido ilegítimo sería el pago de una indemnización y no la reposición. Es por ello que estos jueces no se pronuncian sobre el fondo de la controversia. Sin embargo, los tres magistrados restantes (Espinosa-Saldaña, Blume y Ramos) han suscrito una posición en minoría por la que consideran que la demanda debería declararse fundada.

8 Véase los fundamentos del Magistrado Ramos Núñez en la citada sentencia recaída en el Expediente 00943-2016-PA/TC (2020).

mediar orden judicial a la información contenida en los correos electrónicos y los equipos de un trabajador (2017).

La CS considera que la protección a la inviolabilidad de las comunicaciones del trabajador debe tener en cuenta la existencia de una expectativa razonable de privacidad en relación a las circunstancias; es decir, que la persona entienda que su información privada puede ser objeto de fiscalización o registro en el marco de las funciones de control y monitoreo que ejerce el empleador. Ante ello, la CS consideró que la empresa sí tenía un fundamento razonable para fiscalizar; puesto que (i) la empresa misma habilitó la herramienta informática (correo) para la prestación laboral y (ii) en las circunstancias, el correo electrónico se utilizó para las comunicaciones respectivas de carácter delictivo (posible colusión). Este último aspecto es relevante en el caso, puesto que no nos encontramos ante una medida disciplinaria por parte de la empresa, sino ante la posible comisión de un delito. Así, la CS determinó que el caso en cuestión es de interés público, en la medida en que comprende la posible colusión en una licitación pública para patrullas policiales.

Tal situación genera que sea factible y previsible que la empresa pueda ejercer su facultad de fiscalización al contenido de los correos archivados del trabajador, en tanto (i) supervisa el correcto cumplimiento del monitoreo de sus obligaciones laborales, y (ii) constata que la utilización del instrumento informático respete el ordenamiento jurídico y las propias directivas internas de buen funcionamiento y licitud. Así, la CS concluye que: (i) no existe otra medida menos lesiva para conseguir la información correspondiente a la posible comisión de un delito; (ii) la fiscalización fue ponderada, puesto que se evaluó el interés general en comparación a los perjuicios generados a bienes jurídicos en particular; (iii) la medida fue justificada, puesto que existían sospechas de la posible comisión de un delito; (iv) la medida era necesaria, puesto que la información buscada solo se encontraba en los correos; y (v) la información obtenida versa sobre información relevante al caso y no sobre aspectos personales o familiares del trabajador (Recurso de Nulidad 817-2016, 2017).

Finalmente, en una sentencia aún más reciente recaída en el Expediente 04386-2017-PA/TC (2020), el TC reiteró una vez más que para acceder al correo electrónico de los trabajadores es necesario iniciar una investigación judicial, en la medida que se requiere de un mandato motivado del juez y con las garantías previstas en la ley, para que las comunicaciones y documentos privados sean abiertos, incautados, interceptados o intervenidos.

En atención a ello, consideramos que resulta altamente recomendable obtener la autorización expresa del trabajador para que el empleador pueda acceder con total seguridad al correo electrónico asignado a aquél.

B. La videovigilancia

La voz y la imagen de una persona registrada por medios tecnológicos como las cámaras de videovigilancia hacen parte de los datos personales protegidos por las disposiciones de la LDPD. Este es una de las pocas aplicaciones del derecho a la protección de datos para las que se ha desarrollado una directiva específica en el Perú. La Directiva de Tratamiento de Datos Personales mediante Sistemas de Videovigilancia entró en vigor el 16 de marzo de 2020.

En cuanto a las obligaciones y recomendaciones de la directiva que aplican al ámbito laboral, destacamos las siguientes (Directiva 01-2020-JUS/DGTAI-PD, 2020):

a) **Consentimiento:** la empresa no requiere consentimiento de sus trabajadores, salvo situaciones que no se enmarquen en su poder de dirección, que a su vez engloba el control, supervisión de las labores, protección de bienes, seguridad y salud en el trabajo, entre otros.

b) **Proporcionalidad:** debe cumplirse con el principio de proporcionalidad (ej. las cámaras de videovigilancia no deben ubicarse en lugares destinados para el descanso, esparcimiento, vestuarios, servicios higiénicos, comedores, etc.). La grabación con sonido solo se admite cuando es relevante para los riesgos involucrados. La videovigilancia debe ser adecuada, pertinente y no excesiva en relación con el ámbito y finalidad para la instalación de las cámaras.

c) **Conservación:** las imágenes o voces grabadas deben ser almacenadas por 30 días como mínimo y por 60 días como máximo. Sin embargo, las imágenes y voces sin editar que den cuenta de presuntas infracciones laborales y/o accidentes de trabajo, deben conservarse por 120 días, salvo que existan razones que justifiquen su conservación por más tiempo. En caso de indicios de delito o falta debe comunicársele a la autoridad de inmediato. Los archivos deben eliminarse hasta dos días hábiles de cumplido el plazo máximo.

d) **Derecho de acceso:** los trabajadores podrán solicitar el acceso a las grabaciones o una

copia digital de sus inconductas o incumplimientos que se les haya imputado.

e) **Registrar bases de datos:** al igual que con cualquier dato, los sistemas de videovigilancia implican la titularidad de una o más bases de datos que deben ser registradas ante la Autoridad de Protección de Datos Personales.

f) **Implementar medidas de seguridad:** la empresa debe garantizar la seguridad, confidencialidad y evitar la alteración, pérdida, tratamiento o acceso no autorizado a las imágenes captadas por los sistemas de videovigilancia. Se recomienda, por eso, adoptar medidas técnicas, organizativas y legales pertinentes.

g) **Informar:** cada acceso a la zona de videovigilancia debe tener un cartel o anuncio visible. Se recomienda que contraste con el color de pared y que sea suficientemente visible. Como mínimo el cartel debe indicar la identidad y domicilio de la empresa; ante quién y cómo ejercer los derechos en materia de protección de datos (ej. derechos ARCO), y el lugar en el que se puede obtener más información (la empresa debe contar con un informativo adicional sobre el sistema de videovigilancia). Debe tener una dimensión mínima de 297 x 210 mm, salvo que el espacio no lo permita.

h) **No afectar derechos de terceros**: prevenir la captación de imágenes de terceros ajenos a los fines de la captación. La empresa es responsable por la implementación de mecanismos o medidas adecuadas para no afectar los derechos de terceros (anonimizar, difuminar, etc.).

i) **Tratamiento por encargo:** existen reglas para el uso de servicios o gestión de la videovigilancia realizados por terceros.

j) **Confidencialidad:** deben suscribirse acuerdos de confidencialidad con las personas que, en razón de sus funciones, operan o tiene acceso al sistema de videovigilancia.

k) **Derechos ARCO:** se establecen reglas específicas para el ejercicio de los derechos al acceso, rectificación, cancelación y oposición de los titulares de las imágenes y sonidos captados por los sistemas de videovigilancia.

Más allá de estas disposiciones, al igual que con el correo electrónico, el uso de la videovigilancia plantea preguntas sobre el alcance de la esfera privada y la intimidad de los trabajadores en el ámbito laboral y sobre cómo armonizar la protección de datos personales con las necesidades de monitoreo y control del empleador.

El documento ya citado de la OIT sobre protección de datos personales (International Labour Office Geneva, 1997) establece que el empleador puede hacer uso de los sistemas de videovigilancia para fines de monitoreo de sus trabajadores, pero debe cumplir ciertos requisitos, que coinciden con lo señalado en la directiva de la autoridad del Perú. En primer lugar, solo puede ser llevado a cabo si los trabajadores involucrados son informados previamente de las intenciones del empleador. Los trabajadores deben conocer el propósito del monitoreo y tener una idea clara del funcionamiento de los aparatos que se utilicen (ubicación y horarios en que funcionan, por ejemplo). No puede haber 'cámaras escondidas'.

En segundo lugar, los empleadores no están en libertad total de elegir el método y medios del monitoreo que ellos consideren más apropiados para sus intereses; antes bien, deben tener en consideración las consecuencias para la privacidad de los trabajadores y preferir los medios de vigilancia menos invasivos. En el caso del monitoreo secreto o continuo, la aproximación es mucho más restrictiva. Debe ser limitado a los casos en los que el monitoreo es indispensable para lidiar con específicos problemas vinculados a la seguridad y salud, o a la protección de la propiedad.

El cumplimiento de estas recomendaciones incorpora la valoración de aspectos subjetivos como la intención que se persigue con la utilización de las cámaras y las expectativas razonables de privacidad de los trabajadores.

Al respecto, existe un referente jurisprudencial reciente en el Perú que se ocupa específicamente del uso de cámaras en entornos laborales. El 25 de setiembre de 2020, el TC desestimó una demanda de un sindicato de trabajadores que buscaba que se retirara un sistema de redes de cámaras de video que la empresa había instalado en las áreas de producción, almacenes y fábrica[9]. El sindicato sostenía que las cámaras de vigilancia vulneraban los derechos a la dignidad, la intimidad y la salud de los trabajadores.

[9] El 25 de setiembre de 2020, el Pleno del Tribunal Constitucional emitió, por unanimidad, la sentencia, que declara infundada la demanda de amparo que dio origen al Expediente 02208-2017-PA/TC (2020). Dicha demanda fue presentada contra Nestlé Perú por el Sindicato de Obreros P y A D'Onofrio SA.

La sentencia señala que se pudo constatar que los trabajadores habían sido informados por la empresa de la instalación de las cámaras y del objetivo que se buscaba con ellas. Dicho objetivo correspondía, además, a funciones legítimas de monitoreo y control por parte del empleador y no se encontró evidencia de que se le estuviera dando un uso que extralimitara dichas funciones o que no fuera proporcional a los fines establecidos. Se observó, por ejemplo, que las cámaras habían sido instaladas "en zonas que no constituyen espacios íntimos o reservados para los trabajadores" (Expediente 02208-2017-PA/TC, 2020, fundamento 13). La sentencia describe en detalle lo que considera objetivos legítimos de la utilización de la videovigilancia en este caso específico:

> […] Se puede distinguir que la instalación de cámaras tiene como objetivo el monitorear los procesos de producción y, de ser el caso, poder analizar cualquier incidente de producción o de seguridad; por ejemplo, verificar que las rutas de evacuación se encuentran despejadas, mantener las zonas seguras libres de camiones, asegurar un buen estado y evitar sabotajes en la fuente de energía alterna de la fábrica, poder visualizar el video ante potenciales reclamos vinculados con la presentación de cuerpos extraños en los productos, etc. También se puede advertir que las videocámaras no están instaladas en un ambiente que pudiera ser calificado como "privado", pues son áreas en las que el personal autorizado transita libremente (Expediente 02208-2017-PA/TC, 2020, fundamento 15).

Los fundamentos del TC en el examen de la demanda están en línea con los principios de la legislación sobre protección de datos personales. Lo realmente importante es la ratificación por parte del máximo intérprete de la Constitución sobre la validez del uso de esta tecnología en ámbito laboral.

Además de este referente jurisprudencial, para la aplicación de la directiva al ámbito laboral vale la pena revisar las orientaciones que incluye al respecto la guía que ya hemos citado del gobierno español (AEPD, 2021). Esta aclara, en primer lugar, que la base jurídica para el control de las personas trabajadoras mediante videovigilancia es el contrato de trabajo y las facultades legales de control concedidas al empleador, por lo que no se requiere el consentimiento, pero sí se debe cumplir a cabalidad con el deber de informar. Va, además, en la misma dirección que el TC y la normativa peruana en lo que se refiere a los alcances y limitaciones del uso de este tipo de tecnología para cumplir con funciones de control dentro de las relaciones laborales. Se enfatiza en la importancia de respetar siempre el principio de proporcionalidad.

Por otro lado, aborda el tema específico del uso de las imágenes de videovigilancia como prueba de "la comisión flagrante de un acto ilícito" (AEPD, 2021, p. 52) por un trabajador. Explica que "se entenderá cumplido el deber de informar cuando se haya colocado un dispositivo informativo en lugar suficientemente visible concretando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos" (AEPD, 2021, p. 52). Advierte que la sentencia del Tribunal Europeo de los Derechos Humanos (*López Ribalda et. al. c. España*, 2019) admite que una prueba de incumplimientos graves de las obligaciones laborales (como robos a la empresa) no necesariamente será nula en caso se haya incumplido con el deber de información, siempre que existe una sospecha razonable sobre el ilícito[10].

C. Salud pública y protección de datos de los trabajadores

La emergencia sanitaria generada por la pandemia puso en primer plano una nueva fuente de tensión entre el derecho a la protección de los datos personales y otros derechos individuales y sociales. Una tensión que toca el ámbito laboral en aspectos como la necesidad de controles epidemiológicos y de la vacunación masiva para la protección colectiva de la salud de los trabajadores. Si bien este aspecto no se refiere directamente a una nueva tecnología, sí afecta dinámicas sociales, laborales y legales que pueden, a su vez, incidir en la manera en que en el futuro cercano se desarrollen y adopten nuevas soluciones tecnológicas.

En el marco de la emergencia nacional generada por la pandemia, el 5 de mayo de 2020 la ANPDP emitió la Opinión Consultiva 32-2020-JUS/DGTAI-PD en la que fijó los criterios para armonizar la protección de datos personales de los trabajadores con la obligación de los empleadores en materia de la salud de sus empleados y de la prevención de riesgos laborales.

Recordemos que la información sobre la salud se considera un dato sensible sujeto de especial protección. Es decir, solo puede ser tratada con previo consentimiento de sus titulares por escrito, salvo que exista una excepción que lo justifique. En este contexto, constituye una excepción a la regla del consentimiento la celebración, ejecución y desarrollo de la relación laboral en dónde se

[10] Para mayor información, véase Consejo de Trabajo (2019).

circunscribe el deber del empleador de preservar la salud de sus trabajadores en el entorno laboral. Además, la Opinión Consultiva sostiene que, si bien el principio de consentimiento es un principio rector de la LPDP, en el marco de una relación laboral debe tomarse en cuenta las excepciones contempladas en el artículo 14 de dicha norma (Ley 29733, 2011). Es decir, dada la existencia de una relación contractual de trabajo entre empleador y trabajador, y las obligaciones de garantizar la seguridad y la salud de todos los trabajadores, así como la existencia de una emergencia sanitaria declarada, se configuran las citadas excepciones previstas en la LPDP.

La ANPDP considera que

> es posible que el empleador realice el tratamiento de datos personales sensibles referidos al COVID-19 de los trabajadores sin su consentimiento, siempre que este tratamiento […] tenga como fin garantizar la seguridad y salud en el trabajo con el objeto evitar los contagios de esta enfermedad en los centros laborales (Opinión Consultiva 32-2020-JUS/DGTAIPD, 2020, acápite 9).

Lo anterior se justifica jurídicamente en la obligación del empleador de prevenir los riesgos laborales a los que los trabajadores puedan estar sujetos. Además, los trabajadores deben cooperar con el empleador para dicho fin.

La opinión originalmente estaba dirigida a permitir que se llevaran a cabo controles como la toma de temperatura y el registro de la información sobre los trabajadores contagiados. Señalaba al respecto que

> un dato que arroje una situación anormal de salud puede constituir un peligro para los mismos trabajadores, para el resto del personal o para otras personas relacionadas con el centro laboral; por ende, esta medida constituye un medio relacionado con la vigilancia de la salud de los trabajadores que, conforme a la Ley de Seguridad y Salud en el Trabajo, resulta obligatoria para el empleador (Opinión Consultiva 32-2020-JUS/DGTAIPD, 2020, acápite 22).

Esta Opinión no se ha extendido ni actualizado para abordar el tratamiento a la información sobre la vacunación de los trabajadores. Sin embargo, los criterios anteriormente citados pueden ser relevantes a la hora de examinar esta cuestión. Reconociendo que lo ideal sería obtener el consentimiento de los trabajadores para estos efectos, ¿podría el empleador requerirles la información sobre la vacunación en la medida que sea necesaria para salvaguardar la salud de los trabajadores en el centro de trabajo?

Es importante recordar que la normativa vigente establece que la vacunación es libre y voluntaria. Por lo que, salvo que en un futuro se apruebe una norma específica que establezcan la obligatoriedad de la vacunación, no es posible obligar a los trabajadores a vacunarse. Sin embargo, el empleador podría adoptar medidas proporcionales para preservar la salud de sus trabajadores según sea el caso, tal como solicitar medidas de seguridad más estrictas para aquellos trabajadores no vacunados, y promover y exhortar a sus trabajadores a que se vacunen, continuar con el trabajo remoto, entre otros.

En cualquier caso, es importante tener siempre presente las siguientes recomendaciones en el tratamiento de la información sobre la salud de los trabajadores:

- Cumplir con el deber información. Es decir, cumplir con todos los elementos del artículo 18 de la LPDP (Ley 29733, 2011), aportando información clara y veraz sobre el uso y finalidad del tratamiento de los datos personales;

- Limitar el número de personas con acceso a esta información a quienes por razones de su cargo y función deban necesariamente conocerla, a fin de cumplir con las obligaciones legales relacionadas con la prevención del COVID-19.

- Preservar la confidencialidad y seguridad de la información. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido establecida de manera inequívoca al momento de su recopilación. La finalidad del tratamiento de los datos personales debe expresarse con claridad, sin lugar a confusión y reflejando el objeto del tratamiento de los datos.

VI. COMENTARIOS FINALES

Desde los desarrollos normativos y jurisprudenciales, existe hoy más preguntas que respuestas sobre los alcances y límites del derecho a la protección de los datos personales en el ámbito laboral. Los casos analizados tocan apenas una fracción de las aplicaciones tecnológicas que se están usando en dichos ámbitos laborales y que involucran el tratamiento de los datos personales de los trabajadores. Es importante, sin embargo, que los empleadores tengan claras sus responsabilidades frente a la protección de la información personal de sus trabajadores y que apliquen los principios generales en esta materia que hemos intentado resumir en este artículo.

Se trata, sin lugar a dudas, de un tema de gran relevancia y actualidad, no solo por la multiplicación de aplicaciones tecnológicas, sino por los desafíos que la pandemia del COVID-19 nos ha planteado frente a las necesidades de armonizar derechos individuales como la protección de los datos personales, protección de la salud y la seguridad ocupacional. Frente a ello, es necesario revisar no solo la normatividad y las decisiones jurisprudenciales locales, sino los referentes internacionales que pueden coadyuvar a resolver dudas y controversias en casos concretos.

REFERENCIAS

Agencia Española de Protección de Datos [AEPD] (2021). *La protección de datos personales en las relaciones laborales*. Agencia Española de Protección de Datos.

Blume Moore, I. (2021). El derecho fundamental a la protección de datos en el entorno laboral. *Revista Laborem,* (24), 277-299.

Castro Cruzatt, K. (2008). El derecho fundamental a la protección de datos personales: aportes para su desarrollo en el Perú. *Ius et Veritas*, *18*(37), 260-276.

Consejo de Trabajo (15 de noviembre de 2019). Cámaras ocultas en el trabajo, ¿medida legítima o violación a la privacidad? *Enfoque Derecho*. https://www.enfoquederecho.com/2019/11/15/camaras-ocultas-en-el-trabajo-medida-legitima-o-violacion-a-la-privacidad/

International Labour Office Geneva (1997). *Protection of Worker's Personal Data*. International Labour Organization. https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normative-instrument/wcms_107797.pdf

Vegas Torres, J. (2011). *Obtención de pruebas en ordenadores personales y derechos fundamentales en el ámbito de la empresa*. Universidad Rey Juan Carlos- KPMG.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Bărbulescu c. Romania, 2017 Eur. Ct. H.R. 210.

Constitución Política del Perú [Const.] (1993) (Perú).

Decreto Supremo 003-2013-JUS, Decreto Supremo que aprueba el Reglamento de Ley 29733, Ley de Protección de Datos Personales, Diario Oficial *El Peruano*, 22 de marzo de 2013 (Perú).

Directiva 01-2020-JUS/DGTAIPD, Tratamiento de Datos Personales mediante Sistemas de Videovigilancia, Diario Oficial *El Peruano*, 16 de enero de 2020 (Perú).

Ley 29733, Ley de Protección de Datos Personales, Diario Oficial *El Peruano*, 3 de julio de 2011 (Perú).

López Ribalda et. al. c. España, 2013 Eur. Ct. H.R. 233.

Opinión Consultiva 32-2020-JUS/DGTAIPD, Tratamiento de datos de salud durante la pandemia en el ámbito laboral, 5 de mayo de 2020 (Perú).

Resolución Directoral 019-2013-JUS/DGPDP, Aprueba la Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales, Diario Oficial *El Peruano*, 11 de octubre de 2013 (Perú).

Resolución Directoral 008-2017-JUS/DGPDP, Tratamiento de datos mediante geolocalización, Diario Oficial *El Peruano*, 25 de enero de 2017 (Perú).

Resolución Directoral 02-2020-JUS/DGTAIPD, Aprueba la Directiva para el Tratamiento de Datos Personales mediante Sistemas de Videovigilancia, Diario Oficial *El Peruano*, 16 de enero de 2020 (Perú).

Sala Penal Permanente de la Corte Suprema de Justicia de la República, 20 de noviembre de 2017, Recurso de Nulidad 817-2016/LIMA (Perú).

Segunda Sala de Derecho Constitucional y Social Transitoria de la Corte Suprema de Justicia de la República, 19 de marzo de 2017, Casación 14614-2016-Lima (Perú).

S.T.C. 170/2013, 7 de octubre de 2013 (B.J.C. 170/2013) (Esp.).

Tribunal Constitucional [T.C.], 29 de enero de 2003, sentencia recaída en el Expediente 1797-2002-HD/TC (Perú).

Tribunal Constitucional [T.C.], 18 de agosto de 2004, sentencia recaída en el Expediente 1058-2004-AA/TC (Perú).

Tribunal Constitucional [T.C.], 14 de julio de 2020, sentencia recaída en el Expediente 00943-2016-PA/TC (Perú).

Tribunal Constitucional [T.C.], 25 de septiembre de 2020, sentencia recaída en el Expediente 02208-2017-PA/TC (Perú).

Tribunal Constitucional [T.C.], 27 de octubre de 2020, sentencia recaída en el Expediente 04386-2017-PA/TC (Perú).

MARTINOT

ABOGADOS

Av. Canaval y Moreyra 480, Piso 10-B, San Isidro, Lima, Perú
Teléfono: (511) 748 2288
Email: contactenos@martinotabogados.pe

10.18800/themis.202101.026

DEBATES EMERGENTES EN MATERIA LABORAL Y DE PRIVACIDAD: SISTEMAS DE VIDEOVIGILANCIA, ALGORITMOS DIGITALES E IDENTIFICACIÓN BIOMÉTRICA DE LA PERSONA TRABAJADORA

EMERGING DEBATES ON LABOR AND PRIVACY MATTERS: VIDEO SURVEILLANCE SYSTEMS, DIGITAL ALGORITHMS AND BIOMETRIC IDENTIFICATION OF THE WORKER

Lucía Aragüez Valenzuela*
Universidad de Málaga

Information and communication technologies have revolutionized the world of labor by strengthening, among other things, the power of corporate surveillance. This has affected workers' most basic rights, including their privacy, in a way that is certainly invasive. This corporate control through technological tools is sometimes not entirely transparent or honest, and can even invade the worker's private sphere in an inadvertent way.

In this article, the author reflects on these topics that, in turn, are the subject of certain controversies at the doctrinal and jurisprudential level, trying to provide a critical perspective in favor of greater protection for the working person and a strengthening of the regulations existing labor.

Keywords: Work; technologies; digitalization; privacy; video surveillance.

Las tecnologías de la información y de la comunicación han revolucionado el mundo del trabajo reforzando, entre otros aspectos, el poder de vigilancia empresarial. Esto ha afectado a los derechos más básicos de los trabajadores, entre ellos, a su privacidad, de una forma ciertamente invasiva. Más aún, este control empresarial a través de las herramientas tecnológicas a veces no resulta ser del todo transparente u honesto, sino que puede llegar a invadir en la esfera privada de la persona trabajadora de forma inadvertida, creando incluso situaciones de discriminación.

En este artículo, la autora reflexiona acerca de estos extremos que, a su vez, son objeto de ciertas controversias a nivel doctrinal y jurisprudencial, tratando de aportar una perspectiva crítica en favor de una mayor protección hacia la persona trabajadora y un fortalecimiento de la normativa laboral existente.

Palabras clave: Trabajo; tecnologías; digitalización; privacidad; videovigilancia.

* Abogada. Magíster en Derecho, y Doctora en Ciencias Jurídicas y Sociales por la Universidad de Málaga. Doctorado con mención internacional por efectuar dos estancias de investigación en la Universidad de Berkeley y la Universidad Nacional de Irlanda. Docente en el Departamento de Derecho del Trabajo y de la Seguridad Social de la Universidad de Málaga (Málaga, España). Investigadora Post Doctoral. Contacto: luciaaraguez@uma.es

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 8 de enero de 2021, y aceptado por el mismo el 22 de junio de 2021.

I. EL CONTROL EMPRESARIAL A TRAVÉS DEL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN: ALGUNOS RASGOS DE LABORALIDAD A DEBATE

En los últimos años ha habido una creciente incorporación de las tecnologías de la información y de la comunicación en el mundo laboral. Su utilización se ha efectuado para agilizar los procesos de producción, facilitar el trabajo a las personas trabajadoras, optimizar los recursos empresariales, obtener un mayor lucro a un menor coste, entre otros aspectos. Sin embargo, las tecnologías también van a afectar a la propia relación de trabajo, así como a los derechos más básicos de los trabajadores, por lo que merece una especial reflexión.

En un primer término, podemos decir que el uso de las herramientas tecnológicas va a repercutir en el carácter personal de la relación laboral al verse modificadas las formas de supervisión y control del trabajo de una forma más estricta –e invasiva–. En este caso, no estamos hablando solamente de un poder de vigilancia del empleador, sino que este control se extiende también a la propia persona trabajadora y a su relación jurídica con el empresario. Así, debemos decir que realmente uno de los rasgos esenciales de laboralidad es el carácter personal de la relación laboral, el cual implica que el trabajador es considerado insustituible para el ejercicio de su puesto de trabajo. Por lo tanto, en principio, para el empresario no va a ser indiferente que la realización del trabajo contratado sea llevada a cabo por cualquier persona, sino que debe ser realizado por la propia persona trabajadora contratante siendo, de la misma manera, contratada la persona trabajadora por sus capacidades y aptitudes propias. De esta manera, se elige a una determinada persona en la que se confía por razón de sus características propias para realizar el trabajo. En este sentido, los servicios deben ser prestados de forma personal y directa, y solo ejecutados por el trabajador como persona física insustituible por otra. Esto implica que la relación de trabajo se caracteriza, entre otros factores, por la confianza entre las partes (empresario-trabajador). Este carácter personalísimo de la relación de trabajo es trascendente (López Álvarez *et al.*, 2017) y es que se elige a la persona trabajadora teniendo en cuenta los conocimientos, aptitudes, experiencia e incluso su propia identidad.

Sin embargo, parece que con la introducción de las tecnologías de la información y de la comunicación ha tenido lugar una cierta perdida de la relación basada en la confianza entre ambas partes. Y es que lo que anteriormente –esto es, con anterioridad a la utilización de los sistemas tecnológicos como medio de control– se entendía como un control empresarial personal, directo e inmediato –en el que era necesaria la presencia física del empresario–, ahora se ha visto transformado –y también reforzado– el poder de vigilancia empresarial al encontrarnos con un sistema de control en remoto o a distancia, donde las conductas de los trabajadores podrán ser valoradas sin necesitar esa presencia personal e inmediata. Esto implica a su vez una cierta transformación en la subordinación de la persona trabajadora a las directrices empresariales.

En este contexto, la subordinación o dependencia (López Álvarez *et al.,* 2017) del trabajador respecto del empresario, el cual se plantea de forma más invasiva en la esfera privada de la persona trabajadora, implica una cierta pérdida del carácter personal de la relación laboral, puesto que la relación humana deja de ser tan importante, gozando de un mayor protagonismo el elemento tecnológico y, por consiguiente, un reforzamiento de la capacidad de control empresarial. Realmente nos referimos a una transformación de este rasgo, ya que estamos haciendo referencia a un tipo de control que no solamente se limita a vigilar el trabajo desarrollado por la persona trabajadora, sino que también se extiende a la forma de actuar o comportarse de quien lo ejecuta, viéndose notablemente subordinado al empresario. Tanto es así que, en ocasiones, la voluntariedad puede encontrarse igualmente mermada, principalmente en aquellos casos en los que el trabajador va a desconocer que en su puesto de trabajo está siendo vigilado –mediante cámaras de videovigilancia, algoritmos digitales, sistemas biométricos o de geolocalización, así como la posible monitorización de los ordenadores–, al no haber sido informado de estos extremos.

La voluntariedad realmente se corresponde con el consentimiento de las partes para mantener una relación laboral con un modelo de trabajo caracterizado por la libertad, es decir, por el hecho de que no exista una imposición externa para ejecutar un trabajo. En principio, la voluntariedad no es incompatible, lógicamente, con las propias obligaciones laborales, pero sí es necesario que las mismas sean aceptadas previamente por el trabajador, siendo compromisos libremente asumidos (García Murcia *et al.*, 2013). Esta voluntariedad puede quedar desvirtuada cuando no se permite a la persona trabajadora participar en aquellos compromisos u obligaciones que debería estar dispuesto a asumir. Esto puede ocurrir, como veremos más adelante, por ejemplo, cuando el trabajador no es informado previamente de la vigilancia incisiva en su persona mientras está desarrollando su actividad laboral, cuando su comportamiento está siendo controlado a través de algoritmos digitales pasando de

forma inadvertida para la persona trabajadora, o incluso cuando no se le informa del tratamiento de sus datos personales recabados a través de sistemas biométricos.

Por otro lado, en cuanto a la retribución, debemos decir que los servicios del trabajador deben ser retribuidos "dentro del ámbito de organización y dirección de otra persona", conforme lo señala el artículo 1 inciso 1 del Estatuto de los Trabajadores (en adelante, ET) (Real Decreto Legislativo 2/2015, 2015); por consiguiente, parece que la finalidad de la norma es que efectivamente el salario sea un elemento importante dentro del contrato de trabajo (López Álvarez *et al.*, 2017). Con independencia de ello, lo cierto es que generalmente la retribución suele venir establecida por el propio empresario o incluso puede depender de ciertos algoritmos el hecho de que finalmente el trabajador obtenga una mayor o menor retribución (esto será abordado en la sección cuatro), lo cual deja a la persona trabajadora en una posición de absoluta vulnerabilidad.

En cualquier caso, como se puede observar, resulta complicado aquí encontrar un equilibrio digno entre las exigencias organizativas de la empresa y la consideración que merece la persona que trabaja. De hecho, al utilizar de una forma tan incisiva las tecnologías difícilmente podemos resaltar en la relación laboral su factor humano subyacente, es decir, su carácter personal, sino que, por el contrario, nos situamos ante una 'mera' relación con tendencia preocupantemente instrumentalizadora (Márquez Prieto, 2016). En esta relación parece no importar tanto el lugar donde se ejecute la prestación de servicios o el trabajo, ya que el control se extiende a poder ser a distancia (Borrajo Dacruz, 1990). De esta manera, podemos decir que las tecnologías ocasionan que las empresas se encuentren muy ausentes –o al menos de manera muy lejana– de la propia relación interactiva y humana en el ámbito del trabajo.

II. LOS SISTEMAS DE VIDEOVIGILANCIA EMPRESARIAL CON RELACIÓN A LA ACTUAL NORMATIVA SOBRE PROTECCIÓN DE DATOS Y GARANTÍA DE DERECHOS DIGITALES

En la actualidad existen diversos medios de control empresarial. En este trabajo vamos a centrarnos en el uso de cámaras de videovigilancia puesto que se consideran una de las modalidades más usuales de control de la actividad laboral, sin obviar la existencia de otras[1]. Mediante este sistema, el empresario capta datos del comportamiento de los trabajadores a través del tratamiento de las imágenes de la cámara de videovigilancia en un circuito cerrado de televisión. Estas imágenes aportan información personal sobre la persona trabajadora[2] a través de una gráfica o fotográfica acerca de su persona.

La imagen permite efectuar una identificación o ser susceptible de identificación. Es más, al ser imágenes que se engloban dentro del centro o lugar de trabajo, se hace más perfectamente identificable a las personas que son objeto de vigilancia empresarial, siendo incluso más fácil establecer por parte del empresario un perfil sobre su comportamiento en el entorno laboral. Sin embargo, como no podría ser de otra manera, este control empresarial resulta ser más invasivo en la intimidad de los trabajadores afectando, entre otros aspectos, a su privacidad. Y es que no debemos olvidar que, aunque el trabajador se encuentre realizando su actividad laboral, ello no debe ser interpretado como un abandono de sus derechos más básicos, sino que igualmente su persona merece ser protegida y no solo por parte del empresario, sino también a través de un fortalecimiento de la propia normativa laboral al respecto.

En este contexto, han sido muchas las sentencias relativas a las medidas disciplinarias empresariales derivadas de la captación de imágenes por parte de cámaras de videovigilancia que abogaban por, entre otros aspectos, la importancia del principio de proporcionalidad y, en su caso, por la existencia de una información previa a la persona trabajadora donde se indicase que su comportamiento estaba siendo videovigilado en vistas al cumplimiento –o no– de sus obligaciones laborales[3]. Sin embargo, también nos hemos encontrado con sentencias contradictorias, donde no parecía ser tan relevante la puesta en conocimiento a la persona trabajadora de la existencia de una cámara de videovigilancia, sino el hecho ilícito que había cometido. En este contexto de ciertas controversias a nivel jurisprudencial, fruto de la no existencia de una normativa consolidada al respecto, algunas sentencias protegían la efectividad de los

1 Por ejemplo, los sistemas de geolocalización, el correo electrónico, el acceso a los datos de búsqueda de Internet, vigilancia de redes sociales, etc.

2 En este mismo sentido, se pronuncia el artículo 89 de la LOPDGDD (Ley Orgánica 3/2018, 2018).

3 A título ilustrativo, cabe mencionar la STC 186/2000, del 10 de julio de 2000; STC 29/2013, del 11 de febrero de 2013; STSJ 25/2018, de 12 de enero de 2018; STEDH de 9 de enero de 2018 (caso *López Ribalda y otros c. España*); entre otras.

derechos fundamentales; mientras que otros la facultad empresarial de control, siendo necesario en ambos supuestos la superación del principio de proporcionalidad, donde tiene una gran importancia el análisis de la reciprocidad de las partes en la relación jurídica.

Por ende, se promulgó finalmente la actual Ley Orgánica 3/2018, de 5 de diciembre de 2018, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), la cual tuvo por objeto regular, entre otros extremos, el derecho a la intimidad frente al uso de dispositivos de videovigilancia y grabación de sonidos en el lugar de trabajo. Haciendo un análisis de la actual norma, debemos decir, en primer lugar, que este derecho digital se encuentra regulado en el artículo 89 de la LOPDGDD, donde se indica que: "[l]os empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida" (haciendo referencia a la instalación de las cámaras de videovigilancia y al tratamiento de las imágenes que se hayan obtenido) (Ley Orgánica 3/2018, 2018). Como consecuencia, esta información previa va a ser un requisito esencial en el cumplimiento de la norma para valorar si realmente se está vulnerando la protección jurídica de la persona trabajadora. Sin embargo, no debemos pensar que el hecho de que exista esta información previa ocasione *per se* la no vulneración de los derechos de los trabajadores. Y es que parece que lo que pretende la normativa es que, además de esta información, sea necesario valorar otros factores relativos a los posibles límites inherentes a la instalación por parte del empresario.

En cualquier caso, la normativa también menciona una excepción al deber empresarial de información en los casos en los que se haya captado la comisión flagrante de un acto ilícito por los trabajadores, siempre y cuando se cumpla con los parámetros legales previstos para el tratamiento de datos con fines de videovigilancia (Ley Orgánica 3/2018, 2018, art. 22). El citado artículo se refiere a la instalación de cámaras para preservar la seguridad de las personas o bienes, así como de las instalaciones que tenga la empresa. Por lo que, en principio, parece que cuando el empresario tenga sospechas de que se están cometiendo hechos ilícitos, podrá colocar cámaras sin necesitar informar previamente a los trabajadores. A ello se suma –aparentemente– que el deber de información a los trabajadores se entiende cumplido con la colocación de un dispositivo en un lugar suficientemente visible, identificando la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar derechos (Ley Orgánica 3/2018, 2018, art. 22.4), es decir, lo que comúnmente se conoce por un dispositivo que señala que es una 'zona videovigilada'.

La normativa señala que "en ningún caso se admitirá la instalación de sistemas de grabación de sonidos[4] ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos" (Ley Orgánica 3/2018, 2018, art. 89). Por consiguiente, limita la discrecionalidad empresarial para instalar las cámaras de videovigilancia, debiendo focalizarse solamente en que el trabajador este eficazmente cumpliendo con sus obligaciones laborales, limitando de esta manera una mayor invasión en la privacidad e intimidad de las personas trabajadoras.

Por lo expuesto, lo primero que debemos mencionar es, en cualquier caso, el desarrollo tecnológico derivado de la utilización de cámaras de videovigilancia genera un nuevo conocimiento progresivo que puede invadir la protección jurídica de los trabajadores. En este contexto, en el contrato de trabajo no se debe imponer, como derecho absoluto, la libertad de empresa, ni tampoco venir a limitar el "ejercicio de los derechos fundamentales que incumben al trabajador como ciudadano, que no pierde su condición de tal por insertarse en el ámbito de una organización privada" (S.T.C. 99/1994, 1994, fundamento 2). De esta manera, se produce una ponderación de derechos entre las partes intervinientes en la relación laboral –o al menos esa parece ser la finalidad de la actual LOPDGDD–, pudiendo ser los derechos fundamentales de los trabajadores objetos de cierta modulación, "en la medida estrictamente imprescindible para el correcto y ordenado desenvolvimiento de la actividad productiva reflejo, a su vez, de derechos que han recibido consagración en el texto de nuestra norma fundamental (arts. 38 y 33 C.E.)" (S.T.C. 99/1994,

[4] En este sentido, la normativa refuerza la protección jurídica de los trabajadores cuando, además de la captación de imágenes, también se produzca de sonido, estableciéndose expresamente que:

> La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley (Ley Orgánica 3/2018, 2018, art. 89).

1994, fundamento 4). De este modo, la LOPDGDD parece indicar la necesidad, salvo en determinados casos relacionados con los posibles hechos ilícitos efectuados por los trabajadores, de obtener una información previa por parte de la persona trabajadora para esta postulación de derechos. Una vez que tiene lugar esta puesta en conocimiento, parece que el trabajador deja de mantener cierta expectativa de privacidad puesto que es conocedor de que su comportamiento se encuentra vigilado. Por ende, lo que pretende la norma es el reconocimiento de estos derechos digitales, a diferencia de la anterior Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, de manera que expresamente se reconozcan una serie de derechos de los trabajadores frente a la utilización de medios digitales puestos a su disposición por el empresario.

A ello se suma que, a nivel jurisprudencial, se ha establecido doctrina que aplica dos criterios diferenciales, además por supuesto de lo establecido en norma: uno basado en la necesaria adaptación de los derechos fundamentales "por razones de necesidad" (S.T.C. 99/1994, fundamento 4) y, el segundo de los criterios, respecto a establecer un juicio de ponderación adecuado (S.T.C. 20/1990, 1990; S.T.C. 171/1990, 1990; S.T.C. 240/1992, 1992) porque, en definitiva, el conflicto entre lo contemplado en el contrato de trabajo y las exigencias de la producción y el reconocimiento de efectos a los derechos fundamentales, es una cuestión de límites (Sierra Benítez, 2011). Así, parece que tanto a nivel jurisprudencial como legislativo se aboga por esa necesidad de informar previamente al trabajador, garantizándose la protección jurídico-constitucional de los mismos. Se tiende a considerar que es necesaria una información clara, inequívoca y transparente de que está siendo vigilado, la finalidad de dicho control y el tratamiento de las imágenes que se capten sobre el cómo desarrolla su actividad laboral.

Tras analizar esta normativa y cómo ha afectado la incorporación de las tecnologías al mundo laboral, podemos decir que los distintos contextos en el trabajo, sin lugar a dudas, han ocasionado –y siguen haciéndolo en la actualidad– un nuevo desafío en el derecho del trabajo, ya que se origina un mayor número de entornos cambiantes promovido por la introducción –poco gradual– del factor tecnológico. Esta situación hace que sea difícil adaptar la legislación laboral en materia tecnológica, incluso a pesar de reconocerse una serie de derechos digitales mediante la actual LOPDGDD, aún quedan algunos desafíos por resolverse. Es cierto que la normativa parece remitirse a la negociación colectiva para abordar determinados aspectos relacionados, entre otras herramientas, a las cámaras de videovigilancia, debiendo las empresas establecer los límites oportunos para garantizar la protección jurídica a las personas trabajadoras. A ello se suma el papel tan relevante que tiene la jurisprudencia en la materia –y, sobre todo, el que ha tenido cuando la ausencia normativa era más que evidente–, profundizando en cada caso concreto y avanzando hacia un cambio de cultura tendente a la digitalización jurídica y del trabajo.

Así, a nivel jurisprudencial, aunque no haya sido objeto de análisis en este apartado, se ha priorizado el principio de proporcionalidad donde, en la mayoría de los casos, se ha dotado de una mayor relevancia al carácter recíproco de las partes, es decir, ante el insuficiente marco normativo, los tribunales parecen dotar de una mayor importancia a los comportamientos y actitudes de las partes en la propia relación laboral. De esta manera, aunque nos encontramos ante una era digital, parece ser muy importante para los tribunales que ello no suponga un quiebre del vínculo o de la proximidad relacional entre las partes (empresario y trabajadores), de la confianza o del diálogo, mostrando una especial preocupación en mantener el equilibrio entre el mundo digitalizado –que refuerza el poder de vigilancia y control empresarial– y el carácter humano de la relación laboral (Romero Frías, 2014).

Tras este análisis, lo cierto es que el uso de las cámaras de videovigilancia invade en la esfera privada de los trabajadores y, por tanto, es necesario establecer límites en el ejercicio de ambos derechos (poder de control y privacidad). La normativa parece reforzar la institucionalidad, aportando una mayor seguridad jurídica, pero, realmente, deberíamos analizar también cada caso concreto e ir avanzando hacia un cambio de cultura ('socialidad') tendente a la digitalización jurídica; pero sin que ello suponga un quiebre en la confianza. Para conseguirlo, sería necesario reforzar la norma en este sentido, asentando las bases garantistas en materia de protección de datos e intimidad de los trabajadores.

III. EL REGISTRO BIOMÉTRICO DE JORNADA: LUCES Y SOMBRAS

El control empresarial a través del registro de jornada se viene efectuando desde mucho tiempo atrás; sin embargo, no existía ningún impositivo legal entonces para vigilar el comportamiento de los trabajadores en la entrada y salida al trabajo hasta la publicación del Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, donde se establece la obligación del registro horario de jornada (2019), modificando de

esta manera también el artículo 34 inciso 9 del ET (Real Decreto Legislativo 2/2015, 2015)[5].

Antes de abordar la problemática que supone en materia de privacidad la utilización de sistemas biométricos para realizar el registro de jornada laboral, es necesario que, de manera sucinta, contextualicemos esta necesidad de registrar la jornada por parte del legislador. Como sabemos, el artículo 34 inciso 9 del ET ofrece una obligación formal a las empresas de realizar el registro de jornada de los trabajadores y, en este sentido, debemos previamente reflexionar sobre este deber (Real Decreto Legislativo 2/2015, 2015). En primer lugar, el artículo menciona que "[l]a empresa garantizará el registro diario de jornada" (Real Decreto Legislativo 2/2015, 2015, art. 34.9), lo que indica no solo un deber de hacer, sino también de garantizar que el registro efectivamente se lleve a cabo. Además, deberá ser diario el registro y, por ende, no se prevé que el mismo resulte ser esporádico o arbitrario. La normativa indica que deberá registrarse "el horario concreto de inicio y de finalización de la jornada de trabajo de cada persona trabajadora" (Real Decreto Legislativo 2/2015, 2015, art. 34.9)[6]. En este sentido, prevé la necesidad de adaptar la jornada del trabajador a determinadas circunstancias, siendo posible una cierta flexibilidad horaria en lo que respecta al registro, es decir, en lo relativo a la distribución irregular de la jornada, los periodos de descanso, la duración máxima de jornada, posibles adaptaciones en la jornada relativas a la ordenación del tiempo de trabajo –siempre que sean razonables y proporcionadas–, ausencias, etc.

En cualquier caso, es cierto que el control de la jornada al final implica una vigilancia más incisiva por parte del empresario, ya que, de esta manera, la empresa podrá comprobar si efectivamente el trabajador asiste puntualmente a su puesto de trabajo, cumple con su jornada laboral y si se encuentran justificadas –o no– las posibles irregularidades o faltas que pudieran surgir durante el desarrollo de su actividad laboral. Con esta obligación legal se permite también que pueda existir cierta flexibilidad horaria en el trabajo, pero sin que ello implique una prolongación indebida de la jornada laboral y, con mayor motivo, cuando esta situación no se encuentra debidamente compensada la persona trabajadora con dinero o tiempo de descanso retribuido. Y es que no debemos olvidar que la finalidad de la norma no es otra que evitar los posibles abusos empresariales en materia de jornada laboral.

En este sentido, lo cierto es que los abusos relacionados con la jornada laboral son muy habituales[7], viéndose, en cierta medida, desprotegida la persona del trabajador al tener que realizar una labor bastante difícil durante un procedimiento judicial para demostrar que efectivamente se encontraba sometido a un exceso de jornada, el cual no era compensado ni en tiempo de descanso ni tampoco en dinero. En este sentido, parece que el precepto pretende, además de reforzar la vigilancia empresarial en el comportamiento de los trabajadores, protegerlos jurídicamente al obtener así un medio de defensa ante un posible procedimiento judicial o como herramienta para paliar la precarización del mercado de trabajo.

En este sentido, debemos señalar que el origen de esta modificación normativa y nueva obligación empresarial de registrar la jornada de los trabajadores, encuentra su primera base en la Sentencia de la Audiencia Nacional 207/2015 (2015) (la cual fue anulada por el Tribunal Supremo[8]) que indicó la necesidad de efectuar una reforma legislativa que clarificase la obligación de llevar un registro horario para garantizar los derechos laborales básicos de los trabajadores y reforzar su protección jurídica. La Audiencia Nacional, el 4 de diciembre de 2015, dictó sentencia en la que consta el siguiente fallo:

> […] Estimamos la demanda y condenamos a BANKIA, SA a establecer un sistema de registro de la jornada diaria efectiva que realiza la plantilla, que permita comprobar el adecuado cumplimiento de los horarios pactados, tanto

[5] Concretamente, el artículo indica que

> La empresa garantizará el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora, sin perjuicio de la flexibilidad horaria que se establece en este artículo. Mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empresario previa consulta con los representantes legales de los trabajadores en la empresa, se organizará y documentará este registro de jornada. La empresa conservará los registros a que se refiere este precepto durante cuatro años y permanecerán a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social (Real Decreto Legislativo 2/2015, 2015, artículo 34).

[6] Como se puede observar, la norma está realizando una terminología inclusiva por razón de género al sustituir el término 'trabajadores' por 'personas trabajadoras'.

[7] Así lo indica el Criterio Técnico 101/2019 sobre actuación de la Inspección de Trabajo y Seguridad Social en materia de registro de jornada, publicado por el Ministerio de Trabajo, Migraciones y Seguridad Social de junio de 2019.

[8] Véase S.T.S. 246/2017 (2017).

> en el convenio sectorial como en los pactos de empresa que sean de aplicación, así como que proceda a dar traslado a la representación legal de los trabajadores de la información sobre las horas extraordinarias realizadas, en cómputo mensual, de acuerdo con lo previsto en el artículo 35.5 del Estatuto de los Trabajadores y en la Disposición Adicional Tercera del Real Decreto 1561/1995 y en el artículo 32.5 del Convenio Sectorial de Ahorro (S.A.N. 207/2015, 2015).

La Audiencia Nacional considera que, si la razón de ser de este precepto es procurar al trabajador un medio de prueba documental para acreditar la realización de horas "extraordinarias, parece evidente que el registro de la jornada diaria es la herramienta, promovida por el legislador, para asegurar efectivamente el control de las horas extraordinarias" (S.A.N. 207/2015, 2015, fundamento 3). Y, ello además evidencia que los representantes de los trabajadores tengan la acción para reclamar el cumplimiento de dichos derechos informativos.

Contra dicha resolución, la parte demandada interpuso recurso de casación, siendo admitida con fecha 17 de junio de 2016. La Sentencia 246/2017 del Pleno del Tribunal Supremo (2017) desestimó la demanda sobre la base de una serie de consideraciones[9]:

> La primera de ellas indica que, a pesar de que la norma tenga como principal objetivo establecer un sistema de control de horas extraordinarias –para evitar los posibles abusos existentes en la persona del trabajador–, esto no quiere decir que sea necesario implementar un control de la jornada ordinaria. En segundo lugar, lleva a cabo un análisis detallado a nivel jurisprudencial acerca de la interpretación del artículo 35.5 del ET respecto a la obligación –o no– de proceder a un registro de jornada. De estas sentencias se desprende que el artículo 35.5 parece sólo obligar, salvo pacto que amplíe ese deber, a llevar el registro de las horas extras realizadas y a comunicar a final de mes su número al trabajador y a la representación legal de los trabajadores el número de horas extras realizadas, caso de haberse efectuado. Por consiguiente, parece no existir una obligación legal de llevar un registro para el control de las horas durante la jornada ordinaria. En este mismo sentido entiende el Tribunal que se refiere la Directiva 2003/88/CE, del Parlamento Europeo y del Consejo, de 4 de noviembre de 2003, relativa a determinados aspectos de la ordenación del tiempo de trabajo (Aragüez Valenzuela, 2019, p. 6).

Tras esta sentencia, que parecía finalizar el conflicto existente, el Tribunal de Justicia de la Unión Europea (en adelante, TJUE), en su reciente sentencia de 14 de mayo de 2019, establece que, efectivamente, sin un sistema de registro de jornada no es posible determinar de manera objetiva y, sobre todo, fiable, el número de horas extraordinarias realizadas por el trabajador, así como la distribución de su tiempo, viéndose mermada la protección jurídica de su persona (Caso C-55/18, 2019). De esta manera –y en la misma línea interpretativa de la anteriormente conocida Dirección General de Empleo[10]–, se establece textualmente que "para comprobar si se han realizado horas extraordinarias, es preciso conocer con exactitud el número de horas ordinarias de trabajo realizadas" (Caso C-55/18, 2019, párr. 2016) y, precisamente, para que de manera efectiva se tenga en consideración dicha exactitud, es necesario realizarlo de manera documental. Por este motivo, la Sentencia del TJUE indica en su párrafo 62 lo siguiente:

> la implantación de un sistema oportuno, fiable y accesible que permita computar la jornada laboral diaria realizada por cada trabajador forma parte de la obligación general que incumbe a los Estados miembros y a los empresarios […]. Además, tal sistema es necesario para permitir que los representantes de los trabajadores que tengan una función específica en materia de protección de la seguridad y salud de los trabajadores ejerzan su derecho (Caso C-55/18, 2019).

En este contexto, el Real Decreto-Ley de 8/2019, de 8 de marzo de 2019, establece finalmente la obligación legal de registro de jornada de trabajo. Sin embargo, uno de los vacíos existentes en la actual normativa es que no establece una moda-

9 Resulta interesante igualmente indicar aquí que la presente Sentencia tuvo un voto particular por parte de la Magistrada Mª Lourdes Arastey Sahún en la que resalta, entre otros aspectos, lo que a continuación se indica:

> Sostuve en la deliberación que la obligación de registrar las horas extraordinarias se vacía de contenido si no se efectúa un seguimiento o control de la jornada realizada por el trabajador, pues el concepto de hora extraordinaria solo surge cuando se produce la superación de la jornada ordinaria y, por ello, no cabe argumentar que el cumplimiento de la obligación legal para la empresa se satisface cuando ésta registra las horas extraordinarias, ya que la calificación como tales solo será posible "ex post", esto es, tras haberse efectuado un determinado número de horas, al día, a la semana, al mes o al año. Decae así la posibilidad de interpretar de manera tan estricta y literalmente el precepto –interpretación a la que se acoge el texto de la sentencia que no comparto– (S.T.S. 246/2017, 2017).

10 Hoy conocida como la Dirección General de Trabajo, en Informes de fechas 31/7/2014 y 1/3/2016.

lidad específica para realizar el registro diario de jornada, ya que se limita a indicar que se deberá realizar diariamente. Por consiguiente, parece que será válido cualquier sistema que cumpla con estas premisas, esto es, que proporcione "información fiable, inmodificable y no manipulable a posteriori, ya sea por el empresario o por el propio trabajador" (Ministerio de Trabajo, Migraciones y Seguridad Social, 2019, p. 6). En este sentido, debemos reflexionar sobre la opción de llevar a cabo el registro diario de jornada mediante sistemas de datos biométricos[11].

El efectuar un registro biométrico de la jornada es una forma de incidir de una forma más incisiva en la esfera privada de los trabajadores, puesto que los datos proporcionados pueden presentar una cierta sensibilidad (huella dactilar, reconocimiento facial u ocular, entre otros). Es cierto que en el ámbito laboral el uso de datos biométricos ha sido generalmente admitido por la jurisprudencia[12] a efectos de identificación del trabajador. Así se indica en la sentencia del Tribunal Supremo de 2 de julio de 2007, recaída en el Recurso 5017/2003, o en la Sentencia del TJUE, de 19 de junio de 2014, *Pharmacontinente-Saúde e Higiene SA y otros c. Autoridade Para As Condições do Trabalho (ACT)* (Caso C-683/13)[13]. Sin embargo, un aspecto relevante a destacar es que ambas sentencias se dictaron con anterioridad a la promulgación de la LOPD-GDD, de 5 de diciembre, que entre otros aspectos, refuerza la protección jurídica de la persona trabajadora en el ejercicio de sus derechos digitales.

En cualquier caso, los medios más habituales para realizar un posible control de la jornada laboral son en la actualidad: (i) la huella dactilar; (ii) el reconocimiento facial u ocular; (iii) la geometría del mano; y (iv) la voz.

En primer lugar, debemos mencionar que los datos obtenidos a través de la huella dactilar –así como cualquier otro sistema biométrico– son personales. En este sentido al menos se pronuncia el artículo 4 inciso 14 del Reglamento General de Protección de Datos (en adelante, RGPD) (Reglamento 2016/679, 2016)[14], ya que permite la identificación de una persona física uniendo el dato con una identidad concreta, con un nombre y unos apellidos, llevándose a cabo un proceso en el que se distingue a dicho trabajador del resto. Ahora bien, el RGPD califica estos datos como especialmente sensibles y, por tanto, protegidos, por lo que para que se pueda realizar su tratamiento es necesario mantener un riguroso juicio de proporcionalidad (Reglamento 2016/679, 2016).

El registro mediante huella dactilar ha sido implantado en numerosas empresas. Incluso podemos decir que es uno de los sistemas más habituales en la actualidad establecidos para registrar la jornada de los trabajadores. Con la utilización de los mismos, se permite a la empresa acceder a cierta información (Aguilar *et al.*, 2008) como pudiera ser, en un primer término, la identificación (Abundiz-Pérez *et al.*, 2014)[15] de la persona –al ser cada vez más difíciles de falsear

[11] Según el artículo 4 inciso 14 del Reglamento General de Protección de Datos, son datos biométricos los "datos personales obtenidos a partir de un tratamiento técnico especifico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" (Reglamento 2016/679, 2016).

[12] De igual modo, la Agencia Española de Protección de Datos (en adelante, AEPD) dictó tres Informes (Informe 0368/2006, 0324/2009, y 1999/9904) en relación con los datos biométricos. En el primero de ellos, se pretendía el acceso de los alumnos/as a un centro escolar mediante la utilización de la huella dactilar para, de este modo, poder gestionar las posibles ausencias o retrasos de los estudiantes. La AEPD entendió que era posible efectuar dicho control de una manera menos intrusiva a la privacidad y datos sensibles de los alumnos/as, por lo que no era un sistema proporcional a la finalidad propuesta (Agencia Española de Protección de Datos [AEPD], 2006). Por otro lado, en el Informe 0324/2009 se planteaba la posibilidad de implantar un sistema de control horario de los trabajadores basado en la lectura de la huella digital (AEPD, 2009). En este sentido, la AEPD reflexiona no tanto sobre la posibilidad –o no– de realizar dicho registro, sino más bien acerca del nivel de protección a los datos de los trabajadores recabados. De este modo, la Agencia indica que el nivel de seguridad relativo a los datos biométricos para el acceso al centro de trabajo debe ser el correspondiente al de los datos especialmente sensibles o protegidos (AEPD, 2009). Finalmente, en el Informe 1999-0000 se plantea algo ciertamente sorprendente al entender la Agencia que es posible que el empresario acceda a las huellas dactilares de los trabajadores sin ser necesario su consentimiento por estar avalado en el artículo 6 inciso 2 de la LOPD (AEPD, 1999).

[13] La presente sentencia considera que un registro del tiempo de trabajo, el cual incluya una indicación para cada trabajador del inicio y el final del trabajo y las posibles interrupciones de la jornada correspondientes, coincide con la definición de "datos personales" en el sentido del artículo 2 literal a) de la Directiva (Caso C-683/13, 2014).

[14] Según el artículo 4 inciso 14 del RGPD

> [los] «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos (Reglamento 2016/679, 2016).

[15] El proceso de autentificación biométrica tradicional se basa en la lectura del biométrico mediante un sensor, procesamiento, extracción de características y comparación plantilla previamente almacenada en la base de datos. Inicialmente, en el proceso de enrolamiento se determina un biométrico físico o de comportamiento, como iris, rostro, huella

por las técnicas de encriptación existentes–; y, en segundo lugar, conocer otros datos relativos a la persona trabajadora en la faceta más íntima y privada, como es el acceso a su huella dactilar. De esta manera, la identificación de su persona resulta ser más invasiva que otros medios tradicionales, como, por ejemplo, el registro de jornada mediante firma manuscrita o acceso a plataformas digitales, tarjetas de identificación, accesos al centro de trabajo con un código personal de acceso, entre otros.

Por otro lado, respecto al reconocimiento facial u ocular, debemos decir que hace referencia a un *software* automatizado de identificación biométrica capaz de identificar o verificar una persona mediante la comparación y el análisis de modelos basados en sus rasgos y contornos faciales (Alvez *et al.*, 2011). De esta manera, realmente el reconocimiento facial tiene en cuenta distintos factores, como el envejecimiento, la cirugía plástica, la utilización de cosméticos, la calidad de la imagen, posibles efectos del consumo excesivo de drogas o tabaco o incluso la pose del sujeto. Así, la maquina accede a las características propias del rostro de una persona o de los rasgos específicos relativos a su ojo en el caso del reconocimiento ocular. Algunos estudios confirman que incluso el reconocimiento facial permite observar el estado de ánimo de la persona, lo cual puede resultar una información bastante útil para las empresas que buscan que los trabajadores no únicamente rindan adecuadamente en el trabajo, sino que también estén motivados y se encuentren en un buen estado anímico.

Otros medios empleados, aunque quizá menos habituales, son el acceso al centro de trabajo mediante la geometría de la mano en el que, al igual que ocurría con las huellas dactilares, se permite el acceso al centro de trabajo a través de la palma de la mano, ya que la misma contiene ciertas peculiaridades que la hacen única. En este mismo sentido, también se permite acceder a centros de trabajo a través de la voz, evaluándose las señales que generan las diferentes voces de las personas trabajadoras atendiendo a la combinación de ciertos factores que influyen en el momento de producir el sonido (la estructura de la laringe, la elasticidad de las cuerdas vocales o el tamaño de la boca y la nariz).

En cualquier caso, una vez que hemos realizado esta contextualización relativa al registro de jornada mediante sistemas biométricos, debemos ahora reflexionar sobre si su uso pudiera invadir en exceso la esfera privada de los trabajadores y es que, en realidad, aunque la normativa no limita el instrumento que el empresario debiera utilizar para efectuar el registro de jornada, dejando plena libertad a las partes para establecer el medio más oportuno para ejercitar este derecho, el acceso por parte del empresario a datos biométricos del trabajador debiera requerir, a nuestro entender, de un riguroso juicio de proporcionalidad en su tratamiento, principalmente al tener la condición de un dato especialmente protegido. Así, este control no debiera ampararse en una necesidad general para controlar la jornada de los trabajadores, sino que, por el contrario, tendría que ser entendida como una necesidad específica. Por consiguiente, no nos referimos a que no se recurran a los datos biométricos en ningún caso, sino solamente cuando se cumpla con el juicio de proporcionalidad[16].

A pesar de estas consideraciones, la normativa deja en manos de una posible eventual negociación colectiva –siendo en la actualidad prácticamente inexistentes los convenios colectivos que regulan esta cuestión– el utilizar un registro u otro para controlar la jornada laboral de los trabajadores. En este sentido, se evidencia el papel tan importante que debiera asumir la representación de los trabajadores, ya que resulta ser fundamental para proteger la posible invasión en la esfera privada de los mismos, derivada de la utilización de estos sistemas tecnológicos de control, accediendo a datos íntimos relacionados con su persona.

Sin embargo, esto nos hace preguntarnos qué pudiera ocurrir en el caso de que en la empresa no exista representación de los trabajadores. En estos casos parece que la protección jurídica de la persona del trabajador se encuentra mermada al existir una plena libertad empresarial para efectuar el registro de jornada que considere oportuno, pudiendo acudir al principio de proporcionalidad o no. Esto indica que, en realidad, corresponderá solamente al empresario el establecimiento de un sistema propio de control. Esta misma solución ocurriría en el caso de que tampoco exista una posible previsión en convenio o acuerdo colectivo, debiendo el empresario establecer el sistema concreto de registro, la organización y la documentación requerida.

dactilar, palma de la mano, voz, firma, etc., para utilizase como identificador; después, un sensor realiza la adquisición de datos; posteriormente, un algoritmo procesa los datos y extrae características biométricas (plantillas); finalmente, la plantilla es almacenada en una memoria local o remota para futuras comparaciones. Una vez que el enrolamiento se ha concluido con éxito, se puede realizar el proceso de verificación para autentificar al usuario (Abundiz-Pérez *et al*., 2014).

[16] En este sentido se pronuncia Agencia Catalana de protección de datos, en lo referente a su ámbito de competencia en Recursos Humanos en las Administraciones públicas catalanas.

Por lo expuesto, entendemos que, aunque la normativa concede plena libertad empresarial –aunque limitada cuando exista representación de los trabajadores– para establecer un sistema de registro de jornada, debiéramos reflexionar acerca del carácter personal de la relación laboral, esto es, de la necesidad de establecer un sistema de control empresarial que no resulte ser tan invasivo en la esfera privada y personal de la persona trabajadora, como es el acceso a un dato biométrico, o si, en la mayoría de los casos, se pudiera alcanzar el mismo resultado con un medio de control menos intrusivo. Esto es, mostrar una especial referencia al principio de proporcionalidad atendiendo al trabajo desarrollado por la persona trabajadora y el entorno empresarial existente (Caro Gándara, 2014).

Así, es importante dotar de una mayor relevancia a la percepción recíproca de un trato más personal y honesto (Chandola *et al.*, 2007), reduciéndose la invasión en los datos biométricos de las personas trabajadoras únicamente para casos justificados y muy específicos relacionados con el trabajo (Márquez Prieto, 2015). Así, a nuestro parecer, la obligación empresarial de registro debiera tener en cuenta las circunstancias concretas existentes en la empresa, el nivel de confianza depositada en los trabajadores y la posible flexibilidad o rigidez en el cumplimiento de la jornada de trabajo, velando por el principio de proporcionalidad. Como consecuencia, lo que se pretende en esta reflexión es la necesidad de ir más allá de lo regulado en la propia norma –la cual deja plena libertad para establecer el sistema más adecuado de registro–, teniendo en cuenta otros factores tales como las necesidades empresariales, el tipo de trabajo que se desempeñe y la posible invasión innecesaria en los datos personales –y sensibles– de los trabajadores.

IV. EL USO DE ALGORITMOS DIGITALES COMO MÉTODO INADVERTIDO DE CONTROL EMPRESARIAL

Un fenómeno revolucionario para el mundo del trabajo, de entre otros muchos escenarios, es el *big data* y el empleo de la inteligencia artificial para diversos fines. Con ello, se pretende por parte del empresario el poder cotejar una serie de datos, ya sean personales o no, respecto a la persona trabajadora para realizar un perfil concreto. De esta manera, el empresario tendrá la facultad de tomar decisiones –incluso automatizadas– de la información extraída mediante el empleo de las tecnologías. Una de las formas más usuales para el intercambio de datos y su automatización es a través del empleo de algoritmos digitales[17].

Debe entenderse el algoritmo como

> [aquel] procedimiento sistemático y efectivo [empleado] para resolver un problema [que] se compone de un número concreto de instrucciones que deben estar bien definidas para operar sobre un tipo concreto de datos, a través de un número finito de pasos, que aporta una solución —generalmente matemática— a todos los casos analizados. La solidez de la formulación de un algoritmo dependerá de que sea sistemático y consistente, pero también de que sea no ambiguo, es decir que no deje abierta la solución a interpretaciones. La misión de un algoritmo no es el cálculo de una solución exacta o precisa, sobre todo porque como objetivo se convierte en inalcanzable en muchos casos; su misión está más próxima a facilitar una respuesta (Benítez Eyzaguirre, 2019, p. 1308).

Por consiguiente, realmente la finalidad del algoritmo es aportar una información objetiva al empresario sobre un hecho concreto, esto es, ajeno a cualquier tipo de sentimientos o de sensibilización respecto a las personas trabajadoras.

Es cierto que actualmente nos encontramos con diversos algoritmos que facilitan un procesamiento de datos para localizar la solución más adecuada, incluso empleando diversas vías para ello. Todo depende de su formulación, un aspecto que queda bastante alejado del conocimiento de los juristas y, por supuesto, de la propia persona trabajadora debido a la complejidad técnica en su creación[18] y desarrollo.

---

[17] Como dato curioso, podemos indicar que la matemática británica Ada Lovelace fue la primera persona en desarrollar un algoritmo destinado a ser procesado por una máquina.

[18] A título ilustrativo podemos mencionar que

> Desde 2013, Google utiliza un algoritmo semántico, Hummingbird, diseñado para el análisis del lenguaje natural o búsqueda conversacional. Con este nuevo algoritmo, la compañía actualizó los criterios incorporando la relevancia social, los factores personales, la calidad del contenido y los enlaces, así como la elección personal del usuario a la hora de dirigirse a uno de los resultados. En este sentido, Sweeney (2013) cuestiona cómo este modelo expone a las audiencias a prejuicios raciales y de género, a la vista de cómo se publica la publicidad contextual.
>
> Dos años después Google implementó el componente RankBrain, para analizar un quince por ciento de las búsquedas, cuando incluyen términos coloquiales, frases complejas o neologismos, y así anticiparse a la intención

Los datos están, por tanto, cargados de poder para las empresas, permitiéndose tomar importantes decisiones –automatizas, sin apenas esfuerzos y de manera objetiva– relacionadas con el trabajo de una manera eficiente y rápida. El factor clave de todo este desarrollo tecnológico digital radica en la inteligencia artificial (en adelante, IA) (Goñi Sein, 2019).

En este sentido, cabría preguntarse si esta automatización en la toma de decisiones, sin intervención humana o siendo la misma francamente mínima, se ajusta –o no– a los parámetros relacionados con la justicia, siendo este un aspecto que abordaremos en las siguientes líneas pero que, en cualquier caso, merece la pena adelantar aquí el fin último de este capítulo. Y es que no debemos olvidar que, aunque el uso de los algoritmos se efectúe para analizar datos y tomar decisiones de diverso calibre, también se pueden emplear como medio de control por parte de las empresas. Por ejemplo, los algoritmos pueden establecer el ritmo de trabajo o medir automáticamente la velocidad y la eficiencia de cada trabajador de manera individual (Goñi Sein, 2019).

A ello se suma la capacidad de los algoritmos en realizar predicciones relacionadas con el talento y la capacidad de los trabajadores; supervisar, evaluar y estimular el rendimiento; fijar objetivos y valorar los resultados del trabajo; poner en contacto a los trabajadores con los clientes; juzgar estados de ánimo y emociones; proporcionar formación modular en el lugar de producción; encontrar patrones de comportamiento dentro de la plantilla, entre otros aspectos.

Por consiguiente, el uso de la inteligencia artificial para la toma automatizada de decisiones empresariales puede ser considerado un acierto, pero siempre va a depender de otros factores. Y es que hoy en día parece que muchas empresas recurren a la utilización de algoritmos digitales para establecer situaciones de discriminación, ya que la complejidad técnica de este sistema de control empresarial resulta ser poco transparente y casi imposible de detectar o, al menos, en un primer término. De hecho, podemos incluso decir que los algoritmos son considerados prácticamente un secreto industrial (Azuaje Pirela & Finol González, 2020) por parte de las empresas, ocultando de esta manera cierta información relativa a su procedencia y al tratamiento de los datos recabados. Estos sesgos se pueden producir una vez que los algoritmos establecen un perfil determinado de las personas que, o bien ya se encuentran trabajando en la empresa, o pretenden hacerlo tras un proceso de selección; no siendo algo éticamente aceptado al esconder el mismo una lógica discriminatoria. Por lo tanto, estamos hablando de una discriminación creada por el ser humano, aunque aplicando la IA, que resulta igual de reprochable que si se hubiese realizado dicha actuación de manera personal.

A ello se suma que estas situaciones discriminatorias controladas por la empresa pueden pasar de forma inadvertida para las propias personas trabajadoras, por lo que se dificulta de una mayor manera su detección. A título ilustrativo, se mencionan a continuación algunos ejemplos relacionados con el ámbito laboral que han ocasionado sesgos entre las personas trabajadoras de diversa índole.

A. Acceso al empleo

Para acceder a los puestos de trabajo se tiende a efectuar un determinado proceso de selección, el cual, dependiendo de la empresa, suele presentar una serie de pruebas más o menos complejas hasta alcanzar a los candidatos finalmente elegidos –que serán los futuros trabajadores de la empresa–. Este proceso presenta cierta complejidad cuando el número de candidatos resulta ser muy elevado o los perfiles presentan características muy similares entre sí (fundamentalmente por los requisitos previos necesarios –que sirven como primer filtro– establecidos por la empresa).

En este contexto, se han utilizado los algoritmos digitales para este primer proceso de acceso al empleo, sirviendo como verdaderos agentes de recursos humanos. Sin embargo, algunos algoritmos han presentado sesgos y tratos discriminatorios entre unos candidatos u otros. Esto, por ejemplo, ocurrió en una empresa que, al ofrecer un determinado puesto de trabajo, el algoritmo se encargaba de eliminar a la mayoría de los perfiles que tenían nombres típicos de raza negra o que en la foto del currículum se pudiera detectar que eran personas de color. Un hecho significativo que aventuró a que un grupo de investigadores del Instituto Tecnológico de Massachusetts se alarmasen de dicha situación al recibir las personas blancas más del

del usuario. Entonces también incluyó la herramienta de código abierto TensorFlow, que aplica el modelo matemático Word2Vec, con el que se inicia el aprendizaje de conceptos a partir de las lecturas de artículos y sin supervisión humana. Usa representaciones distribuidas del texto para detectar similitudes entre conceptos, de forma que se hace útil para representar y extraer conocimiento, la traducción automática, la formulación de preguntas y respuestas (Benítez Eyzaguirre, 2019, p. 1310).

50% de las llamadas –y, por ende, la reclamasen–. Ante esta situación, se confirmó finalmente que la empresa estaba utilizando un determinado algoritmo digital que discriminaba el acceso al empleo a las personas de raza negra, estableciéndose claramente un sesgo de origen racial propiciado por el propio algoritmo que, recordemos, ha sido creado por una mente pensante.

B. Reducción de costes

En este caso, nos referimos a un algoritmo digital creado para evitar posibles costes futuros a las empresas a raíz de una serie de predicciones tras cotejar la masividad de datos de las personas trabajadoras. Concretamente, nos referimos a la aplicación que fue conocida como Predective Hire (en español, contratación anticipada), analizada por el profesor adjunto Nathan Newman del John Jay College of Criminal Justice (2017). Esta aplicación se basaba en descartar a los empleados que tenían una mayor probabilidad de pedir un aumento del salario o de apoyar la sindicalización a través de la transferencia y el análisis de una serie de datos recabados de los trabajadores por las plataformas virtuales (intercambio de correos electrónicos, mensajes, acceso a páginas de internet, entre otros).

El algoritmo realmente analizaba la personalidad y la intención de los trabajadores a través de la IA mediante un sistema de aprendizaje automático. De esta forma, las empresas podían anticiparse a estos comportamientos considerados como 'negativos' o 'rebeldes', modificando algunos aspectos relativos a los contratos de trabajo o, incluso, efectuando un posible despido.

De esta manera, podemos observar como a través de este tipo de algoritmos el poder de análisis de los datos ha desempeñado un papel fundamental en la reducción del poder colectivo de los trabajadores, ya que con el acceso a esta información se permite a las grandes empresas tener un perfil mucho más preciso de sus trabajadores, anticipándose incluso a las pretensiones que se les pudieran plantear en un futuro, teniendo acceso a una información mucho más completa acerca de su persona e incidiendo en un mayor control sobre sus comportamientos. En otras palabras, esta aplicación permite conocer a quienes realmente se han contratado, saber lo que piensan, creen y quieren, lo que otorga a las empresas una ventaja en cada negociación sobre la remuneración y las prestaciones. De esta manera, la aplicación genera, a través de la tecnología, un aumento del conocimiento de las empresas en los procedimientos de negociación a fin de ganar cada momento de la negociación sobre el precio, las condiciones de empleo, entre otros aspectos.

Así, los empresarios utilizan esta información para ejercer un mayor control respecto a la persona trabajadora, al tener acceso a sus deseos y preferencias, en el lugar de trabajo en todo momento, dejando a la representación de los trabajadores –que pretenden reivindicar los derechos del colectivo– en un papel francamente residual o secundario.

C. Eficacia en el trabajo

Una persona eficiente en el trabajo es uno de los aspectos más valorados por parte de las empresas, ya que ello suele indicar la obtención de un mayor lucro económico. Por consiguiente, la medición de los resultados del comportamiento de los trabajadores es un aspecto relevante desde una perspectiva empresarial. Antes esto era objeto de valoración de manera más personal, donde el empresario tendía a vigilar la actitud de los trabajadores. Sin embargo, hoy en día podemos decir que este control personal ha sido sustituido por la valoración del comportamiento de los trabajadores a través de una máquina –aunque siempre con intervención humana–, es decir, a través del uso de algoritmos digitales que miden los resultados obtenidos de forma individual. Concretamente nos referimos a la eventual programación de un algoritmo que permita al empresario acceder a determinada información sobre si la persona trabajadora está rindiendo conforme a lo esperado en el puesto laboral que ocupe. Sin embargo, el problema estriba cuando los resultados presentados por parte del algoritmo no son conformes a lo esperado y es que, ante estas circunstancias, la empresa podrá tener la capacidad de adoptar las medidas disciplinarias que considere oportunas al respecto.

En este sentido, también se ha analizado la posible existencia de sesgos atendiendo al nivel de eficacia de los trabajadores. Un ejemplo característico lo encontramos en las nuevas formas de trabajo derivadas del uso de plataformas virtuales donde el trabajador 'a llamada' recibe la orden de efectuar un determinado pedido –como en el caso de Uber Eats, Deliveroo o Glovo– o realizar algún traslado –como en el caso de Uber o Wizz–. En las presentes plataformas se ha demostrado que, si los prestadores de servicios no operan para las mismas durante un determinado periodo de tiempo o reciben comentarios desfavorables por sus actuaciones con los consumidores y usuarios, las empresas tienden a enviarles cada vez menos 'llamadas', llegando incluso al punto de tener la capacidad de darles de baja de la propia plataforma.

Sin embargo, no debemos olvidar que esto no es más que una valoración presentada por el propio algoritmo sobre la base de si los comportamientos de estos prestadores se ajustan –o no– a lo

esperado, reservándose la propia plataforma la capacidad de 'amonestar' al trabajador de la forma anteriormente referenciada. Esto crea ciertas diferenciaciones entre unos trabajadores y otros, ya que, en muchas ocasiones, no se valoran las circunstancias personales de las personas trabajadoras, sino una serie de datos obtenidos por el algoritmo que reflejan únicamente un descenso en su rendimiento en el trabajo, perdiéndose de esta manera el carácter personal de la relación laboral y el trato humano.

D. Por razón de género o raza

Existen también otros algoritmos que pueden efectuar diferencias por razón de género o de raza, y es que el uso de las herramientas tecnológicas puede desencadenar también brechas digitales en este sentido.

Respecto al género, podemos indicar el ejemplo de la empresa Amazon, la cual desarrolló un determinado algoritmo en materia de contratación del personal a un determinado puesto de trabajo a través de una serie de puntuaciones que iban desde alcanzar una estrella, hasta cinco, siendo esta ultima la máxima puntuación posible. El algoritmo que empleaba Amazon para valorar a los candidatos demostró que los trabajadores hombres eran preferibles puesto que obtenían una valoración mayor con respecto a las mujeres de forma arbitraria y desproporcionada. Tanto es así que incluso el algoritmo 'penalizaba' aquellos currículums que incluían alguna palabra femenina.

Por otro lado, en cuanto a la raza, podemos señalar a título ilustrativo la empresa Uber. Esta empresa estructuró un correspondiente algoritmo que discriminaba a las personas de raza negra con respecto a los de raza blanca para operar en la plataforma. Lo que ocurría es que la plataforma encargaba menos trabajo a unos trabajadores (los de raza negra) con respecto a los otros. Esto, indiscutiblemente, afectaba a la precarización de sus puestos de trabajo, ya que el hecho de que la plataforma no necesitase sus servicios implicaba la obtención de un salario menor, a pesar de estar conectados –y con intención de operar para Uber– el mismo periodo de tiempo que los trabajadores de raza blanca. De esta manera, la actuación de la empresa resultaba ser discrecional, arbitraria, injusta y, sobre todo, desigualitaria.

Ahora bien, los anteriores ejemplos no dejan de ser tan solo algunos de los muchos existentes en el ámbito laboral, aunque es cierto que los algoritmos tecnológicos se utilizan en muchos otros sectores. En cualquier caso, se ha podido observar que los algoritmos son cuestiones matemáticas muy técnicas y complejas, donde difícilmente las personas pueden comprender su actuación dentro del entorno empresarial por no tener los suficientes conocimientos o incluso la correspondiente información acerca de su existencia. En este sentido, merece la pena reflexionar sobre si el uso de los mismos se ajusta o no a parámetros basados en la justicia.

En primer lugar, debemos decir que la utilización de los algoritmos por parte de las empresas es perfectamente posible, ya que el RGPD no impide la posibilidad de una decisión automatizada a través del procesamiento datos. Por tanto, el trabajador no tendría derecho a oponerse a este procesamiento enteramente automatizado. Ahora bien, el responsable del tratamiento debe cumplir con una serie de obligaciones como es la necesaria información previa del uso de estos algoritmos para vigilar su comportamiento en el entorno empresarial o para la toma de determinadas decisiones que directamente le afecten. Con esta información previa, la persona trabajadora tendrá derecho a efectuar las alegaciones oportunas, a recibir una explicación de la decisión adoptada después de la evaluación por parte de la empresa, o incluso ejercer su derecho a impugnar la decisión si se considera lesiva de sus derechos (Reglamento 2016/679, 2016, art. 22.3).

Esta necesaria información también ha sido objeto de análisis por el conocido Grupo de Trabajo del artículo 29 (Dictamen 2/2017, 2017), el cual considera que, antes de la utilización de cualquier herramienta de monitoreo, debería tenerse en cuenta, como ocurrían en los casos anteriormente analizados, el principio de proporcionalidad. Para ello, se debiera dejar constancia de los datos y los procesos que determinan la decisión, así como de la necesidad de una explicación adecuada del proceso de toma de decisiones del sistema y, por supuesto, informar a las personas trabajadoras sobre todos los posibles extremos que resulten relevantes. Con ello, se pretende evitar que la decisión quede exclusivamente en las manos del algoritmo o de la inteligencia artificial, ya que en este caso la persona trabajadora puede llegar a perder completamente el control de las decisiones que la conciernen.

En este sentido, además de esta necesaria información previa, para que un algoritmo se ajuste a los parámetros de la justicia, será necesario que el mismo garantice la transparencia y la calidad de los datos mediante un código fuente en abierto (lo que se conoce como *open data*). De esta forma, nos encontraremos con un algoritmo digital que no solo será fácilmente auditable –para detectar si establece algún tipo de discriminación en el entorno de trabajo–, sino también alterable. Así, el algoritmo digital presentará una estructura 'flexi-

ble' que permite su posible modificación ante una posible respuesta a las reclamaciones futuras de los trabajadores fruto de su funcionamiento. Esta sería una manera adecuada de garantizar un sistema de control empresarial transparente, leal, justo y, ante todo, que pretenda evitar la discriminación entre unas personas trabajadoras y otras.

En cualquier caso, lo cierto es que la utilización de los algoritmos digitales por parte de las empresas es algo bastante actual, por lo que presenta un importante desafío para el derecho del trabajo su posible eventual regulación, y es que hoy en día no existe una verdadera normativa consolidada en la materia que aporte al sistema cierta seguridad jurídica. Es cierto que encontramos algunas normativas a nivel comunitario, como la Recomendación CM/Rec(2020)1 del Comité de Ministros a los Estados miembros de la Unión Europea sobre los impactos de los sistemas algorítmicos en los derechos humanos, pero, desde luego, aún queda un largo camino por recorrer.

V. REFLEXIONES FINALES

Como se ha podido apreciar, nos encontramos en la actualidad ante un entorno laboral con tendencia preocupantemente instrumentalizadora a través del uso –y abuso– de las tecnologías de la información y de la comunicación. Esta situación implica una cierta pérdida del carácter humano, no solo por encontrarse sustituida por las tecnologías, sino porque no parece ser una verdadera preocupación para las empresas ni tampoco para la normativa.

De hecho, nos encontramos ante un fortalecimiento del poder de control empresarial, donde parece perderse la confianza depositada en la persona trabajadora al requerirse de una vigilancia mucho más incisiva sobre su persona. Ha quedado suficientemente demostrado que en estos modelos digitalizados de las relaciones laborales no priorizan el elemento humano frente al factor tecnológico, y que, además, su uso se suele efectuar de una forma poco transparente, pasando incluso de manera inadvertida.

La principal reflexión del presente trabajo versa en enfocar el uso de las tecnológicas en el ámbito laboral priorizando el trato humano, utilizando las mismas de manera honesta y evitando una invasión desproporcionada o innecesaria en la esfera privada de las personas trabajadoras atendiendo al principio de proporcionalidad, el cual ha resultado adquirir un papel protagonista a lo largo del presente estudio. Para conseguir esto, es importante recurrir a una base normativa consolidada; sin embargo, actualmente resulta ser prácticamente inexistente la regulación de la digitalización de las relaciones de trabajo, puesto que aún quedan muchos aspectos por perfilar debido, fundamentalmente, a su reciente incorporación en el mercado de trabajo.

Finalmente, también merece una especial consideración el papel de los representantes de los trabajadores en este sentido, ya que son muy pocos los convenios y/o acuerdos colectivos que abordan estos aspectos (videovigilancia, registro de jornada y algoritmos digitales). En este sentido, es necesario resaltar la labor tan necesaria que debieran tener los mismos, junto con las empresas, en analizar y regular estas cuestiones para aportar una mayor seguridad jurídica a los trabajadores, garantizando así sus derechos más básicos y es que, como ha quedado suficientemente demostrado, a veces dejar en manos de una máquina la toma de decisiones no siempre aporta una solución justa.

REFERENCIAS

Åborg, C., Johansson, G., Stoetzer, U., & Svartengren, M. (2014). Organization, relational justice and absenteeism. *Work*, *47*(4), 521–529. https://doi.org/10.3233/WOR-131624

Abundiz-Pérez, F., Cruz-Hernández, C., Murillo-Escobar, M. A., & López-Gutiérrez, R. M. (octubre de 2014). *Cifrado caótico de plantilla de huella dactilar en sistemas biométricos*. Memorias del XVI Congreso Latinoamericano de Control Automático, Cancún, México.

Agencia Española de Protección de Datos (1999). *Solicitudes de datos efectuadas por la Policía Judicial sin mandamiento judicial o requerimiento previo del Ministerio Fiscal* (Informe 1999/9904). https://www.aepd.es/es/documento/1999-9904.pdf

(2006). *Proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio* (Informe 368/2006).

(2009). *Informe sobre posibilidad de implantar un sistema para el control horario de los trabajadores basado en la lectura de la huella digital* (Informe 0324/2009).

Aguilar, G., Nakano, M., Pérez, H., Sánchez, G., & Toscano, K. (2008). Reconocimiento de Huellas Dactilares Usando Características Locales. *Revista de la Facultad de Ingeniería de la Universidad de Antioquia*, (46), 101-109.

Alvez, C., Benedetto, M., Etchart, G., Leal, C., & Luna, L. (mayo de 2011). *Sistemas de reconocimiento*

biométrico, importancia del uso de estándares en entes estatales. Trabajo presentado en el XIII Workshop de Investigadores en Ciencias de la Computación, Santa Fe, Argentina.

Aragüez Valenzuela, L. (diciembre de 2019). *Los sistemas biométricos de registro de jornada y la (des)protección jurídica de la persona del trabajador*. Ponencia presentada en las XXXVIII Jornadas Universitarias Andaluzas de Derecho del Trabajo y Relaciones Laborales, Sevilla, España.

Azuaje Pirela, M., & Finol González, D. (2020). Transparencia algorítmica y la propiedad intelectual e industrial: tensiones y soluciones. *Revista de propiedad inmaterial*, (30), 111-146. https://doi.org/10.18601/16571959.n30.05

Benítez Eyzaguirre, L. (2019). Ética y transparencia para la detección de sesgos algorítmicos de género. *Estudios sobre el Mensaje Periodístico*, *25*(3). https://doi.org/10.5209/esmp.66989

Borrajo Dacruz, E. (1990). *El Estatuto de los Trabajadores. Conceptos fundamentales: empresa y trabajador* (tomo I). Revista de Derecho Privado.

Caro Gándara, R. (2014). Reconstrucción de la justicia contractual desde la justicia relacional. *Recerca. Revista De Pensament I Anàlisi,* (14), 93-116.

Chandola, T, Marmot, M., & Siegrist J. (2007). Failed reciprocity in close social relationships and health: Findings from the Whitehall II study. *Journal of Psychosomatic Research*, *63*(4), 403-411. https://doi.org/10.1016/j.jpsychores.2007.07.012

García Murcia, J., Martín Valverde, A., & Rodríguez-Sañudo Gutiérrez, F. (2013). *Derecho del Trabajo*. Tecnos.

Goñi Sein J. L. (septiembre de 2019). *Defendiendo los derechos fundamentales frente a la inteligencia artificial*. Lección inaugural del curso académico 2019-2020 en la Universidad Pública de Navarra, Pamplona, España.

López Álvarez, M. J., Matorras Díaz-Caneja, A., Molero Manglano, C., & Sánchez Cervera Valdés, J. M. (2017). *Manual de Derecho del Trabajo*. Tirant lo Blanch.

Márquez Prieto, A. (2015). La relación laboral como relación social (justicia relacional y socialidad común). *Estudios Financieros. Revista de Trabajo y Seguridad Social: Comentarios, casos prácticos: recursos humanos*, (382), 13-42.

(2016). Naturaleza jurídica y social del trabajo asalariado. En A. Márquez Prieto & J. L. Monereo Pérez (dirs.), *La política y el derecho del empleo en la nueva sociedad del trabajo: Liber amicorum en honor de la profesora Rosa Quesada Segura* (pp. 176-186). Consejo Andaluz de Relaciones Laborales.

Ministerio de Trabajo, Migraciones y Seguridad Social (2019). *Guía sobre el Registro de Jornada.* https://www.mites.gob.es/ficheros/ministerio/GuiaRegistroJornada.pdf

(2019). *Criterio Técnico 101/2019 sobre actuación de la inspección de trabajo y Seguridad Social en materia de registro de jornada*. https://www.mites.gob.es/itss/ITSS/ITSS_Descargas/Atencion_ciudadano/Criterios_tecnicos/CT_101_2019.pdf

Newman, N. (2017). Reengineering Workplace Bargaining: How Big Data Drives Lower Wages and How Reframing Labor Law Can Restore Information Equality in the Workplace. *University of Cincinnati Law Review*, (85), 693-760.

Rodríguez-Sañudo, F. (1999). La integración del teletrabajo en el ámbito de la relación laboral. En J. Cruz Villalón (ed.), *Trabajo subordinado y trabajo autónomo en la delimitación de fronteras del Derecho del Trabajo*. Tecnos.

Romero Frías, E. (2014). Ciencias sociales y humanidades digitales: Una visión introductoria. En E. Romero Frías & M. Sánchez González (eds.), *Ciencias sociales y humanidades digitales. Técnicas, herramientas y experiencias de e-Research e investigación en colaboración*. Sociedad Latina de Comunicación Social.

Sierra Benítez, E. M. (2011). *El contenido de la relación laboral en el teletrabajo*. Consejo Económico y Social de Andalucía.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Caso C-55/18, Federación de Servicios de Comisiones Obreras (CCOO) c. Deutsche Bank SAE, ECLI:EU:C:2019:402 (may. 14, 2019) (Procedimiento prejudicial).

Caso C-683/13, Pharmacontinente-Saúde e Higiene S.A. y otros c. Autoridade Para As Condições do Trabalho (ACT), O.J. (C 261) 11 (ago. 11, 2014).

Dictamen 2/2017 sobre el tratamiento de datos en el trabajo del Grupo de Trabajo de Protección de Datos del Artículo 29 (GT29) (WP 249), U.N. Doc. 17/ES (WP 194) (8 de junio de 2017) (UE).

Ley Orgánica 3/2018, Protección de Datos Personales y garantía de los derechos digitales (B.O.E. 2018, 3) (Esp.).

Real Decreto Legislativo 2/2015, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores (B.O.E. 2015, 2) (Esp.).

Real Decreto-Ley 8/2019, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo (B.O.E. 2019, 8) (Esp.).

Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), 2016 O.J. (L 119) 1 (UE).

S.A.N., 4 de diciembre de 2015 (No. 207/2015) (Esp.).

S.T.C., 15 de febrero de 1990 (B.J.C., No. 20/1990) (Esp.).

S.T.C., 12 de noviembre de 1990 (B.J.C., No. 171/1990) (Esp.).

S.T.C., 21 de diciembre de 1992 (B.J.C., No. 240/1992) (Esp.).

S.T.C., 11 de abril de 1994 (B.J.C., No. 99/1994) (Esp.).

S.T.S., 2 de marzo de 2007 (Recurso 5017/2003) (Esp.).

S.T.S., 23 de marzo de 2017 (No. 246/2017) (Esp.).

10.18800/themis.202101.027

HACIA UNA ADECUADA PROTECCIÓN DEL DERECHO FUNDAMENTAL AL SECRETO E INVIOLABILIDAD DE LAS COMUNICACIONES EN LA RELACIÓN LABORAL: ANÁLISIS CONSTITUCIONAL A LA LUZ DE LAS NUEVAS TECNOLOGÍAS

TOWARDS ADEQUATE PROTECTION OF THE FUNDAMENTAL RIGHT TO SECRET AND INVIOLABLE COMMUNICATIONS IN THE LABOR RELATIONSHIP: CONSTITUTIONAL ANALYSIS IN THE LIGHT OF NEW TECHNOLOGIES

Raúl Humberto Feijóo Cambiaso*
Pontificia Universidad Católica del Perú
Payet, Rey, Cauvi, Pérez

We are currently immersed in accelerated technological progress, which brings with it both advantages for the world of communications and challenges for fundamental rights. These challenges are exemplified when talking about communications within the workplace. The phenomenon is such that both the Peruvian Supreme Court and Constitutional Court have emphasized the protection of the worker against a possible inspection by the employer of the content of his work email, unless there is a prior judicial investigation.

This article analyzes the right to secrecy and inviolability of communications in labor relations from a current perspective. The axis of the research deals with the treatment of technological support provided by employers, especially the regulation of institutional emails. The author performs a comparative analysis of Peruvian, Spanish and European Court of Human Rights jurisprudence and concludes by delving into the topic of control of conversations in the worker's social media carried out by means of an electronic support provided by the employer.

Keywords: Secrecy and inviolability of communications; email, social networks; employment relationship; new technologies.

Actualmente nos encontramos inmersos en un acelerado progreso tecnológico, el cual trae consigo ventajas para el mundo de las comunicaciones, pero retos para los derechos fundamentales. Estos desafíos se evidencian en el ejemplo de las comunicaciones dentro del contexto laboral. Es tal el fenómeno que tanto la Corte Suprema como el Tribunal Constitucional peruano han puesto de manifiesto la protección del trabajador ante una eventual inspección por parte del empleador del contenido de su correo electrónico institucional, salvo que exista una investigación de carácter judicial previa.

El presente artículo analiza el derecho al secreto e inviolabilidad de las comunicaciones en las relaciones laborales desde una perspectiva actual. El eje de la investigación versa sobre el tratamiento del soporte tecnológico brindado por los empleadores, en especial la regulación sobre los correos electrónicos institucionales. Para ello, el autor realiza un análisis comparado de la jurisprudencia peruana, española y del Tribunal Europeo de Derechos Humanos, y concluye explorando la problemática del control de las conversaciones en las redes sociales del trabajador realizadas mediante un soporte electrónico brindado por el empleador.

Palabras clave: Secreto e inviolabilidad de las comunicaciones; correo electrónico; redes sociales; relación laboral; nuevas tecnologías.

* Abogado. Adjunto de docencia del curso de Sistema de Justicia y Fundamentos Constitucionales del Proceso en la Pontificia Universidad Católica del Perú. Asociado en el Área de Solución de Controversias del Estudio Payet, Rey, Cauvi, Pérez Abogados (Lima, Perú). Contacto: rfeijooc@pucp.pe

Nota del Editor: El presente artículo fue recibido por el Consejo Ejecutivo de THĒMIS-Revista de Derecho el 24 de enero de 2021, y aceptado por el mismo el 27 de junio de 2021.

I. INTRODUCCIÓN

El 30 de mayo de 2017 se publicó en el Diario Oficial El Peruano la Casación 14614-2016, donde la Corte Suprema fijó como criterio que el establecer de forma expresa en el reglamento interno de trabajo una facultad de control por parte del empleador no permite que este pueda revisar el contenido del correo electrónico institucional de sus trabajadores. A partir del recurso de casación interpuesto por Nestlé Perú S.A., esta sentencia consideró que los medios informáticos (*chat*, correo electrónico, entre otros) que son propiedad del empleador, pero que se encuentran a disposición del trabajador, pueden ser usados por este último para fines personales. Asimismo, estableció en su décimo sexto fundamento jurídico que una intromisión en tales correos electrónicos supone una violación de los derechos fundamentales del trabajador (Casación 14614-2016, 2017).

En la misma línea, se publicó el 14 de diciembre de 2018 en el Diario Oficial El Peruano la sentencia recaída en el Expediente 5532-2014-AA/TC del Tribunal Constitucional del Perú. Dicha sentencia coincide con los criterios señalados por la Corte Suprema en el párrafo anterior, estableciendo que existe una prohibición para el empleador de intervenir en el contenido de los mensajes de los medios informáticos brindados a sus trabajadores, salvo que exista una investigación de carácter judicial previa, pues ello vulneraría su derecho al secreto e inviolabilidad de las comunicaciones (Expediente 5532-2014-AA/TC, 2018).

En la actualidad, las nuevas tecnologías poseen un rol central en el ámbito de las relaciones laborales, su importancia para permitir una mejor comunicación, tanto a nivel interno como con los consumidores, ha llevado a que el empleador provea a sus trabajadores de diversos medios tecnológicos para un uso estrictamente laboral. Ello abre la puerta a un conflicto que requiere de un análisis por parte del derecho constitucional: nos referimos al conflicto entre, por un lado, la facultad de fiscalización del empleador sobre el uso de dichos medios tecnológicos y, por el otro, el derecho fundamental al secreto e inviolabilidad de las comunicaciones de los trabajadores como un límite a dicha facultad.

Siendo el trabajador consciente de que la razón para la cual le ha sido entregado dicho medio tecnológico es el facilitar la realización de sus labores, debemos cuestionarnos si resulta lógico pensar que un trabajador pueda contar con la denominada 'expectativa de secreto o confidencialidad' en el correo electrónico institucional proporcionado por su empleador. Y si vamos aún más allá, ¿puede controlar el empleador las conversaciones en redes sociales de sus trabajadores en caso se hayan efectuado desde un soporte tecnológico brindado por este?

Plantear una respuesta a estas interrogantes en nuestro país encuentra grandes dificultades al no existir una norma que regule estos supuestos. El único reciente intento que hemos podido identificar para lograr una adecuada regulación se encuentra en los Proyectos de Ley 2604/2013-CR (2013) y 3329/2013-CR (2014). Ambos fueron respaldados por un dictamen de la Comisión de Trabajo y Seguridad Social del Congreso de la República, de fecha 24 de setiembre de 2014. Es posible verificar a partir de una lectura de ambos proyectos y del acta de la segunda sesión ordinaria de dicha comisión que proponían lo siguiente:

a) Los trabajadores no cuentan con una expectativa razonable de privacidad al utilizar los medios informáticos en el centro de trabajo, en tanto el empleador es el titular de dichos medios

b) Si el empleador previamente ha comunicado a sus trabajadores las políticas de uso de los medios informáticos, este se encuentra facultado para establecer medidas de fiscalización; siempre y cuando sean idóneas, y con base en causas objetivas y razonables (Comisión de Trabajo y Seguridad Social del Congreso de la República, 2014, p. 9)

Al respecto, encontramos una clara contradicción con lo establecido por la Corte Suprema y el Tribunal Constitucional, en tanto el dictamen del Congreso se encontraría a favor de permitir que el empleador controle el contenido de las comunicaciones de sus trabajadores en caso estas se realicen mediante medios tecnológicos brindados para uso exclusivamente laboral.

Como analizaremos más adelante, una posición similar a la adoptada por los proyectos de ley a los que hemos hecho referencia ha sido desarrollada recientemente por un voto en minoría de la actual composición del Tribunal Constitucional en la ponencia de la sentencia recaída en el Expediente 0943-2016-PA/TC, publicada el 23 de setiembre de 2020. En efecto, puede verificarse que dicho voto en minoría respalda la facultad de fiscalización del empleador de los correos electrónicos institucionales con la condición de un previo aviso sobre las políticas de uso y control y que, incluso, realiza un importante análisis sobre los alcances de dicha fiscalización sobre las conversaciones en redes sociales de los trabajadores desde un soporte electrónico brindado por el empleador con fines estrictamente laborales (Expediente 0943-2016-PA/TC, 2020).

Es por ese motivo que consideramos que nos encontramos ante un tema actual de gran relevancia, el cual exige analizar las diversas consideraciones desarrolladas a nivel doctrinal y jurisprudencial para poder determinar una posición respecto a una correcta regulación para nuestro país.

En ese sentido, en primer lugar, delimitaremos el contenido constitucionalmente protegido del derecho al secreto e inviolabilidad de las comunicaciones. Posteriormente, analizaremos lo señalado por el Tribunal Constitucional de nuestro país respecto a la facultad de fiscalización del empleador de los correos electrónicos institucionales. Asimismo, realizaremos una comparación con lo señalado tanto por la jurisprudencia española como por el Tribunal Europeo de Derechos Humanos (en adelante, TEDH), de modo que podamos determinar si aquello considerado por nuestro Tribunal Constitucional se encuentra acorde a los últimos pronunciamientos a nivel internacional. Finalmente, haremos un breve análisis sobre el control de las conversaciones en las redes sociales del trabajador realizadas mediante un soporte electrónico brindado por el empleador a la luz del reciente voto en minoría en la ponencia de la sentencia del Tribunal Constitucional recaída en el Expediente 00943-2016-PA/TC, el caso Paucarcaja.

II. EL CONTENIDO CONSTITUCIONALMENTE PROTEGIDO DEL DERECHO AL SECRETO E INVIOLABILIDAD DE LAS COMUNICACIONES

El derecho fundamental al secreto e inviolabilidad de las comunicaciones se encuentra recogido en el artículo 2, inciso 10, de la Constitución Política del Perú de 1993, el cual, tal y como señala el profesor Díaz Revorio, representa un derecho fundamental autónomo que busca proteger la vida privada de la persona (2006, p. 125). Respecto al carácter autónomo de este, coincide con esta posición el profesor Samuel Abad Yupanqui, quien considera que no es posible sostener que este y el derecho fundamental a la intimidad sean equivalentes, pues una vulneración del primero no conlleva necesariamente la violación de este último (2012, p. 15).

En esa línea, debe tomarse en cuenta que nos encontramos frente a una 'garantía objetiva', la cual protege "cualquier comunicación con independencia de su contenido, sean aspectos íntimos o cuestiones intrascendentes" (Díaz Revorio, 2006, p. 129). Este es el denominado 'carácter formal' que el profesor Abad Yupanqui considera que posee este derecho fundamental, el cual permite afirmar que este "comprende toda la comunicación con independencia de cuál sea su contenido" (2012, p. 17).

Por lo tanto, una primera aproximación a este derecho fundamental nos permite concluir que se trata de un derecho autónomo que no puede ser confundido con el derecho a la intimidad. Asimismo, es posible afirmar que este derecho fundamental representa una garantía formal y objetiva que protege toda comunicación, sin importar su contenido.

Ahora bien, en relación con el bien constitucionalmente protegido por este derecho fundamental, el profesor Gimeno Sendra considera que este se encuentra en el derecho a mantener el carácter reservado de una información privada, es decir, el derecho a que ningún tercero pueda intervenir en el proceso de comunicación y conocer su contenido (2011, p. 334). Por otro lado, el Tribunal Constitucional español ha considerado que el bien constitucionalmente protegido por este derecho fundamental es la libertad de las comunicaciones, como un contenido implícito que puede identificarse a partir de este derecho fundamental (S.T.C. 114/1984, 1984).

Asimismo, el Tribunal Constitucional español ha establecido que esta libertad de comunicaciones puede ser vulnerada tanto "por la interceptación en sentido estricto (aprehensión del soporte o captación del proceso de comunicativo) como por el conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena)" (S.T.C. 114/1984, 1984). Ello confirma lo sostenido por el profesor Díaz Revorio, quien señala que aquello que es objeto de protección por parte de este derecho fundamental no debe limitarse "solo al contenido de la comunicación, sino que alcanza al soporte de la misma, así como las circunstancias que la rodean" (2006, p. 129).

De este modo, puede afirmarse que el derecho al secreto e inviolabilidad de las comunicaciones conlleva a una protección amplia de todo el proceso comunicativo, el cual va desde la comunicación hasta el soporte de la misma. Como veremos más adelante, esto puede tener una gran importancia respecto a los medios tecnológicos que el empleador brinda a sus trabajadores, como es el caso del celular o la computadora de la empresa, los cuales sirven como soporte de las comunicaciones y que también se encontrarían protegidos por este derecho fundamental, a pesar de no intervenir el empleador necesariamente en una conversación específica.

Corresponde ahora analizar quién posee la titularidad de este derecho fundamental. Según señala Díaz Revorio, es titular de este derecho cualquier persona natural o jurídica, siendo necesario anotar que evidentemente la persona jurídica solo podrá

mantener comunicaciones a través de la mediación de personas físicas (2006, p. 128). Asimismo, este autor añade que no es posible sostener que en una misma comunicación se dé una concurrencia de titularidades, siendo necesario utilizar criterios en el caso concreto, como el determinar quién es el propietario del medio utilizado o si la comunicación se hace a nombre de la persona jurídica (Díaz Revorio, 2006, p. 129).

Coincide con dicha posición Samuel Abad Yupanqui, quien agrega que "los titulares de este derecho son las personas que se comunican, por lo que este derecho se opone a los terceros, mas no a quienes intervienen en el proceso mismo de la comunicación" (2012, p. 16). En ese sentido, considera que la grabación de la conversación con otra persona sin su autorización no conlleva por ningún motivo a una vulneración del derecho al secreto de las comunicaciones (Abad Yupanqui, 2012, p. 16).

Ante ello, queda claro que lo que se busca proteger es el proceso comunicativo de los terceros que no participan directamente en este, siendo posible afirmar, de acuerdo con la doctrina, que la titularidad de este derecho fundamental alcanza incluso a las personas jurídicas dependiendo de si la comunicación se hace a su nombre o si se utiliza un medio de su propiedad. Debemos prestar especial atención a esto, pues podría llevarnos a concluir la necesidad de limitar la protección del derecho al secreto e inviolabilidad de las comunicaciones de los trabajadores al realizarse una comunicación a nombre del centro de trabajo o a través de un medio tecnológico brindado por el empleador.

Debemos analizar, a continuación, si la delimitación del contenido constitucionalmente protegido de este derecho fundamental por el Tribunal Constitucional peruano se encuentra en la misma línea de lo señalado anteriormente por la doctrina.

De este modo, a partir de una revisión de los últimos pronunciamientos del Tribunal Constitucional peruano respecto al contenido de este derecho fundamental, puede identificarse que en el segundo fundamento jurídico de la sentencia recaída en el Expediente 00867-2011-PA/TC (2014) se establece que el derecho al secreto e inviolabilidad de las comunicaciones prohíbe que las comunicaciones y documentos privados puedan ser interceptados o conocidos por terceros ajenos al proceso comunicativo, salvo que exista una autorización judicial de por medio. En esa misma línea, nuestro Tribunal Constitucional señaló en el tercer fundamento jurídico de la misma sentencia que la protección de este derecho no alcanza a quien registra, capta o graba su propia conversación ni tampoco a aquel que, siendo parte de dicha comunicación, autoriza a un tercero para que acceda a la comunicación (Expediente 00867-2011-PA/TC, 2014).

Esta definición coincide con lo señalado por la doctrina, siendo aquello que busca protegerse el proceso comunicativo de los terceros ajenos a la comunicación misma. Por lo tanto, la definición de nuestro tribunal se encuentra en armonía con nuestras aproximaciones respecto al bien constitucionalmente protegido y a la titularidad de este derecho fundamental que hemos desarrollado en los párrafos anteriores.

Ahora bien, es necesario anotar que la jurisprudencia del Tribunal Constitucional peruano establece como límite al ejercicio de este derecho la existencia de una autorización judicial debidamente motivada, lo cual se encuentra recogido expresamente en nuestra Constitución. En relación a este límite, el profesor Samuel Abad Yupanqui considera que es posible afirmar que nuestro país acoge la tesis del "monopolio judicial" de las intervenciones sobre las comunicaciones privadas (2012, p. 14) o, en palabras de nuestro Tribunal Constitucional, la "garantía de judicialidad" (Expediente 1058-2004-AA/TC, 2004, fundamento 22). Ello encuentra su base en lo recogido por el artículo 15 de la Constitución italiana de 1948 y el artículo 18, inciso 3, de la Constitución española (1978), razón por la cual analizaremos la jurisprudencia de España más adelante, pues ambos países poseen un modelo de regulación de este derecho fundamental similar al nuestro.

Por otro lado, el Tribunal Constitucional peruano también ha establecido que este derecho fundamental "comprende a la comunicación misma, sea cual fuere su contenido y pertenezca o no el objeto de la comunicación al ámbito de lo personal, lo íntimo o lo reservado" (Expediente 2863-2002-AA/TC, 2003, fundamento 3). Ello coincide con el carácter formal de este derecho fundamental que hemos reconocido anteriormente y permite confirmar su carácter autónomo frente al derecho fundamental a la intimidad por parte de nuestra jurisprudencia constitucional.

Finalmente, debemos destacar que nuestro tribunal ha considerado en reiterada jurisprudencia que este derecho "se dirige a garantizar de manera inequívoca la impenetrabilidad de la comunicación en cualquiera de sus formas o medios" (Expediente 00867-2011-PA/TC, 2014, fundamento 3). Por lo tanto, el Tribunal Constitucional coincide con la propuesta de una protección amplia a todo el proceso comunicativo, el cual va desde la comunicación hasta el soporte de esta.

Consideramos que la delimitación del contenido constitucionalmente protegido de este derecho fundamental por parte de la jurisprudencia de nuestro Tribunal Constitucional es correcta, pues ha logrado recoger las principales características establecidas por un importante sector de la doctrina, lo cual creemos permite una adecuada protección de las comunicaciones y documentos privados en nuestro país. Corresponde ahora analizar el ejercicio de este derecho fundamental en un ámbito específico como son las relaciones laborales, siendo necesario partir por analizar lo señalado por el Tribunal Constitucional peruano, con el objetivo de determinar si su jurisprudencia se encuentra acorde a los recientes pronunciamientos a nivel comparado.

III. EL DERECHO AL SECRETO E INVIOLABILIDAD DE LAS COMUNICACIONES EN LA RELACIÓN LABORAL: EL CASO DEL CORREO ELECTRÓNICO INSTITUCIONAL

Antes de pasar a analizar cuál ha sido el tratamiento de este derecho fundamental en el ámbito de las relaciones laborales por nuestro Tribunal Constitucional, debemos contextualizar nuestro análisis en el conflicto que se presenta para su ejercicio por parte de los trabajadores frente a la facultad de fiscalización por parte del empleador de los medios tecnológicos brindados para un uso estrictamente laboral.

Al respecto, se ha señalado que la intervención de las comunicaciones de los trabajadores por parte del empresario conlleva un necesario análisis sobre el contenido y los límites del poder de fiscalización empresarial, lo cual permite identificar algunos derechos fundamentales enfrentados: por un lado, "el derecho de organización del empresario y la libertad de empresa"; y, por otro lado, "los derechos a la intimidad y al secreto de las comunicaciones de los trabajadores de la empresa" (García Bel & García Sánchez, 2015, p. 122).

Ahora bien, tal y como ha señalado parte de la doctrina española, podría pensarse que los contenidos de un ordenador de propiedad de la empresa son precisamente de la empresa, por lo que la invocación de derechos del trabajador como su intimidad personal quedan fuera de lugar, en tanto nos encontramos frente a datos o informaciones empresariales a las que debe tener acceso el propietario (Aba-Catoira, 2011, p. 269).

Sin embargo, "esta argumentación no se sostiene desde la concepción de los derechos fundamentales como normas iusfundamentales que vinculan a todos, particulares y Estado, y que nunca desaparecen" (Aba-Catoira, 2011, p. 269). En ese sentido, "los derechos que puede invocar el trabajador para evitar la intervención empresarial representan límites que se han de respetar para que ese acceso sobre los equipos informáticos no devenga en una restricción injustificada de derechos" (Aba-Catoira, 2014, p. 92).

Por lo tanto, no es posible dar solución a este conflicto vaciando de contenido los derechos fundamentales de los trabajadores, los cuales no pueden ser limitados de forma irrazonable, siendo necesario encontrar una solución razonable y proporcional que no termine por vaciar de contenido ningún derecho fundamental.

Es importante tomar en cuenta que María Belén Cardona Rubert señala que la incorporación de las nuevas tecnologías a las relaciones laborales plantea dos grandes cuestiones: (i) los límites al uso para fines no laborales de los medios informáticos que pertenecen al empleador; y (ii) "la legitimidad de los controles empresariales y de vigilancia" por parte del empleador (2015, p. 34).

En la presente investigación, nos centraremos en el segundo de estos nuevos retos que plantea el uso de nuevas tecnologías en la relación laboral, pues su implementación conlleva un gran aumento de las facultades de control del empleador (Cardona Rubert, 2015, p. 35). Al respecto, debe tomarse en cuenta que ello puede generar una grave vulneración de los derechos fundamentales de los trabajadores.

Asimismo, nos centraremos en el análisis de un medio tecnológico específico que ha tenido una gran importancia en la jurisprudencia de nuestro Tribunal Constitucional, lo cual nos ayudará a encontrar criterios que podrán ser del mismo modo aplicados a otros medios tecnológicos: nos referimos específicamente al correo electrónico que brinda el empleador para fines laborales o, también llamado, 'correo electrónico institucional'.

El análisis de los límites del uso de este medio tecnológico por parte de los trabajadores para fines personales presenta una gran importancia, pues, como señala Cardona Rubert

> un uso abusivo del correo electrónico institucional puede generar diversos perjuicios al empleador, los cuales van desde el tiempo que el trabajador no emplea para cumplir con sus labores o la distracción que genera en sus compañeros mediante la remisión de comunicaciones con contenido que escapa completamente a lo laboral, hasta situaciones más graves, como la envío de información confidencial relacionada a otros trabajadores, clientes o proveedores a

personas fuera de la organización de la empresa, entre otras (2015, p. 36).

Incluso, surgen supuestos en los que el empleador posee "interés directo en fiscalizar el tráfico de mensajes electrónicos personales, como son los casos de «acoso sexual» o de «espionaje industrial»" (Martínez Fons, 2005, p. 225).

Ello nos muestra claramente la importancia de este tema en la actualidad, donde la ausencia de una adecuada comprensión del tema puede generar desde fuertes perjuicios para el centro laboral hasta un uso abusivo de las medidas de control y vigilancia por parte del empleador. Es por este motivo que, a continuación, analizaremos lo señalado por la jurisprudencia del Tribunal Constitucional del Perú sobre este conflicto y el uso del correo electrónico institucional.

A. Alcances de la jurisprudencia el Tribunal Constitucional del Perú

1. La exigencia absoluta de una investigación judicial para autorizar la intervención sobre el correo electrónico por parte del empleador

La primera sentencia que se pronuncia sobre estos temas es aquella recaída en el Expediente 1058-2004-AA/TC, publicada el 16 de setiembre de 2004, en la cual un trabajador de SERPOST S.A. demanda haber sido despedido por haber enviado material pornográfico a través del sistema de comunicación electrónico de la empresa, es decir, desde el correo institucional, durante el horario de trabajo y a través de una computadora del centro laboral.

Al respecto, el Tribunal Constitucional consideró que, en relación con las facilidades técnicas o informáticas brindadas por la empresa a los trabajadores, el hecho de que la fuente o soporte pertenezca a la empresa por ningún motivo significa que esta última sea la titular de forma exclusiva y excluyente de tales comunicaciones y documentos (Expediente 1058-2004-AA/TC, 2004, fundamento 18).

Ahora bien, debe tomarse en cuenta que en dicha sentencia el Tribunal Constitucional aclara que ello no significa que el empleador no pueda hacer uso de su poder fiscalizador en caso se incumplan las obligaciones de trabajo. Sin embargo, añade que deben implementarse mecanismos que no distorsionen el contenido de los derechos fundamentales del trabajador.

Asimismo, señaló que era necesario el inicio de una investigación judicial para determinar si el trabajador utilizó el correo electrónico para fines distintos a sus obligaciones laborales. En ese sentido, consideró que, al sustentarse la empresa demandada simplemente en su facultad fiscalizadora para acceder a los correos institucionales de sus trabajadores, se vulneró el derecho fundamental al secreto e inviolabilidad del demandante al no existir un mandato judicial de por medio (Expediente 1058-2004-AA/TC, 2004).

Posteriormente, se publicó la sentencia recaída en el Expediente 04224-2009-PA/TC, publicada el 1 de agosto de 2011, en la cual la demandante fue despedida al haberse comunicado, a través de su correo electrónico Hotmail, con un extrabajador sobre información confidencial de la institución y sobre su opinión del presidente del directorio y de la gerencia, lo cual dañaba su honor. Dicha comunicación se realizó durante el horario de trabajo y a través de una computadora brindada por el empleador.

En esta sentencia, el Tribunal Constitucional peruano reiteró en su décimo sexto fundamento jurídico los criterios establecidos en la sentencia antes mencionada, reafirmando la importancia del respeto de los derechos fundamentales en la fiscalización del empleador en estos casos, así como la obligación de iniciar una investigación de tipo judicial para determinar el correcto uso del correo electrónico por parte del trabajador (Expediente 04224-2009-PA/TC, 2011).

Luego de haber revisado ambas sentencias, consideramos necesario señalar nuestras apreciaciones.

En primer lugar, coincidimos con la posición del tribunal respecto al límite de la facultad de fiscalización del empleador, el cual debe respetar en todo momento el contenido de los derechos fundamentales de los trabajadores. De esta manera, se confirma su supremacía y su obligatorio cumplimiento por parte de las entidades estatales y los privados.

Sin embargo, consideramos que el tribunal ha pasado por alto un detalle de gran importancia en su análisis, el cual se refiere a la necesaria distinción entre el control sobre un correo electrónico personal utilizado en la computadora del centro laboral y el control sobre el correo electrónico institucional. Y es que una interrogante que no fue planteada en ambas sentencias es la siguiente: ¿es necesario contar con un mandato judicial para controlar las conversaciones en el correo institucional si es que previamente el trabajador era consciente de la posibilidad de su revisión por parte del empleador si es que este era utilizado para fines personales?

Ello no fue analizado por el tribunal en dichas sentencias, en las cuales, más bien, se ha planteado

una posición similar a aquella de la Suprema Corte de Justicia de México. En una sentencia del 2011, esta consideró que no importa quién es el propietario del medio informático para justificar que este pueda acceder al correo.

Al respecto, dicha corte señaló que, siendo una de las características del correo "su virtualidad y ubicuidad, [aquello que se protege] es la comunicación en sí, siendo el tipo de computador y su propietario simples cuestiones accidentales" (Cobos Campos, 2017, p. 58). Al igual que el caso de México, nuestro Tribunal Constitucional se limitó hasta ese momento a cerrar las puertas a un control del correo electrónico, ello sin evaluar la necesaria distinción que debe hacerse entre los tipos de correo electrónico, los cuales fueron parcialmente tomados en cuenta en sentencias posteriores del mismo tribunal, las cuales analizaremos a continuación.

2. La distinción entre el correo electrónico personal y el institucional: surgimiento de la 'expectativa de confidencialidad'

Debemos, a continuación, hacer referencia a las sentencias recaídas en los Expedientes 03599-2010-AA/TC y 00114-2011-PA/TC, publicadas el 23 de abril de 2012 y el 24 de mayo de 2012 respectivamente. Ambas demandas de amparo fueron declaradas fundadas por el tribunal peruano, al considerar que se había producido la vulneración del derecho al secreto e inviolabilidad de las comunicaciones de los trabajadores que habían sido despedidos.

Al respecto, debe tomarse en cuenta que la empresa demandada había intervenido en la conversación de sus trabajadores, las cuales se habían producido a través de un *chat* virtual llamado Net Send, un servicio de mensajería instantánea donde era posible sostener conversaciones en tiempo real, herramienta que fue otorgada por el empleador exclusivamente para coordinaciones laborales.

Puede observarse que la sentencia en su mayoría, en ambos casos, no logra llegar a un consenso sobre los límites de la facultad de fiscalización del empleador en el correo electrónico institucional o en un *chat* proporcionado para fines laborales, siendo necesario detenernos a analizar cada uno de los votos de los magistrados del Tribunal Constitucional.

En primer lugar, podemos identificar los votos de los magistrados Mesía Ramírez y Calle Hayen, los cuales siguen el criterio establecido anteriormente, considerando que en el presente caso solo era posible intervenir en las conversaciones del servicio de mensajería brindado por el empleador si se contaba previamente con un mandato judicial que justifique la intromisión en dichas comunicaciones (Expediente 03599-2010-AA/TC, 2012; Expediente 00114-2011-PA/TC, 2012).

Sin embargo, es importante tomar en cuenta que el magistrado Mesía Ramírez realiza en su voto una distinción entre el correo electrónico personal, por un lado, y el correo electrónico o el servicio de mensajería proporcionado por el empleador, por el otro. En esa línea, señala en el quinto fundamento jurídico de su voto que existen dos posturas respecto a estos últimos, las cuales se diferencian por si se exige o no una resolución judicial debidamente motivada (Expediente 03599-2010-AA/TC, 2012; Expediente 00114-2011-PA/TC, 2012). Finalmente, a pesar de realzar esta importante distinción, opta por considerar que los correos electrónicos y servicios de mensajería proporcionados por el empleador requieren de un mandato judicial para proceder a su intervención. Ello representa un primer avance hacia la distinción entre los tipos de correos electrónicos que hemos indicado anteriormente.

Por otro lado, debemos destacar lo señalado en el voto del magistrado Eto Cruz en ambas sentencias, quien resalta en su noveno fundamento jurídico que aquello que debe ser considerado como privado cuando hablamos de este derecho fundamental no se encuentra referido "al tipo de contenido o mensaje comunicado, sino a la cualidad del medio empleado", a partir de la cual surge una expectativa de confidencialidad (Expediente 03599-2010-AA/TC, 2012, fundamento 9; Expediente 00114-2011-PA/TC, 2012, fundamento 9). De este modo, considera que "el elemento central en la definición del derecho es el tipo de medio empleado para la comunicación", donde este será considerado como privado "por las características intrínsecas de dicho medio y por las condiciones bajo las cuales se utiliza" (Expediente 03599-2010-AA/TC, 2012, fundamento 9; Expediente 00114-2011-PA/TC, 2012, fundamento 9).

A partir de esta cita, puede verificarse cómo en este voto se introduce el concepto de expectativa de confidencialidad que ha sido analizado por la jurisprudencia y doctrina española, como veremos más adelante. Ahora bien, el magistrado Eto Cruz considera que son dos los elementos necesarios para configurar dicha expectativa, la cual además permite considerar que una comunicación se encuentra protegida por este derecho: (i) el medio haya sido utilizado para realizar una comunicación con una persona en particular o un grupo cerrado de participantes; y (ii) que hayan sido empleados medios que objetivamente generen que una per-

sona asuma que la comunicación se mantendrá en secreto (Expediente 03599-2010-AA/TC, 2012; Expediente 00114-2011-PA/TC, 2012).

Este voto es de gran importancia, pues los votos de los magistrados Álvarez Miranda y Urviola Hani en ambas sentencias parten del concepto de expectativa de confidencialidad desarrollada por el magistrado Eto Cruz.

Al respecto, el magistrado Álvarez Miranda considera que las cuentas de correo electrónico que son propiedad del empleador deben ser utilizadas para fines estrictamente laborales (Expediente 03599-2010-AA/TC, 2012; Expediente 00114-2011-PA/TC, 2012). Ello se encuentra justificado en el hecho de que la marca o nombre comercial del empleador podría verse perjudicada a través de dichas comunicaciones, así como también podría tener como consecuencia que el empleador deba enfrentar futuros litigios judiciales. En ese sentido, considera que un medio informático propiedad del empleador, proporcionado como herramienta de trabajo, no permite que el trabajador pueda asumir la existencia de una expectativa razonable de confidencialidad.

Asimismo, el magistrado Urviola Hani considera en el sexto fundamento jurídico de su voto que en el caso concreto "no es posible afirmar la existencia de una expectativa de secreto o confidencialidad de las comunicaciones" (Expediente 03599-2010-AA/TC, 2012; Expediente 00114-2011-PA/TC, 2012), pues el reglamento interno de trabajo había previsto la prohibición de dar un uso distinto al laboral a los medios informáticos brindados para dicho fin.

Luego de haber podido revisar lo señalado en los diversos votos de los magistrados en ambas sentencias, puede verificarse una evolución en la jurisprudencia del Tribunal Constitucional peruano. Es evidente como de una concepción que no distinguía entre el correo electrónico personal y el institucional, y que, además, establecía la prohibición de su intervención al empleador de forma absoluta, se ha pasado a tener un arduo debate en la jurisprudencia constitucional a partir de la introducción de la noción de 'expectativa de confidencialidad'.

Sin embargo, como ha podido verificarse, no existía hasta ese momento un verdadero consenso por parte de la jurisprudencia constitucional. Debe tomarse en cuenta que transcurrieron ocho años entre lo establecido por la sentencia recaída en el Expediente 1058-2004-AA/TC y las sentencias analizadas en este apartado, sin que sea posible encontrar una solución para las consecuencias negativas que trae para el empleador el no poder establecer mecanismos adecuados para el control de las comunicaciones realizadas a través del correo electrónico por él proporcionado.

A continuación, analizaremos dos recientes pronunciamientos del Tribunal Constitucional, de modo que podamos verificar si luego de casi diez años desde los pronunciamientos del Tribunal Constitucional apenas analizados sobre este tema, se ha logrado identificar nuevos criterios que se encuentren en armonía con lo establecido por la jurisprudencia internacional en torno a cuáles deberían ser los límites al poder de control del empleador en estos casos.

3. Los avances hacia el reconocimiento de la facultad de fiscalización del empleador sobre el correo electrónico institucional

La sentencia recaída en el Expediente 5532-2014-PA/TC, publicada el 14 de diciembre de 2018, se encuentra referida a una demanda de amparo interpuesta por una trabajadora de la empresa Cencosud Perú SA, la cual fue despedida por supuestamente haber difundido de forma irresponsable información que generaba un grave perjuicio a la imagen de la empresa desde su cuenta de correo electrónico institucional.

En los fundamentos 4 y 5 de la sentencia fueron confirmados los criterios establecidos en las sentencias recaídas en los Expedientes 1058-2004-AA/TC (2004) y 3599-2010-PA/TC (2012), considerando que una intervención del empleador en los medios informáticos brindados a los trabajadores, sin que se haya iniciado previamente una investigación judicial, representa una vulneración del derecho fundamental al secreto e inviolabilidad de las comunicaciones (Expediente 5532-2014-PA/TC, 2018).

En el caso concreto, el Tribunal Constitucional consideró que, al ser la propia empresa demandada la que adjuntó en la carta de preaviso de despido las impresiones de pantalla sin poder acreditar que fueron obtenidas a través de su trabajadora, el despido del que había sido objeto la demandante correspondía ser declarado nulo.

A pesar de ello, merece una especial mención el fundamento de voto del magistrado Ramos Núñez, en el cual sostiene que no es posible que los trabajadores presenten una expectativa razonable de privacidad cuando se trata de mensajes enviados a través del correo institucional o de los ordenadores que han sido proporcionados por el empleador (Expediente 5532-2014-PA/TC, 2018). En esa línea, considera que el solo hecho de que el empleador

brinde medios informáticos a sus trabajadores genera una presunción de falta de expectativa razonable de privacidad.

Esta última posición ha sido desarrollada por el voto en minoría en la sentencia recaída en el Expediente 0943-2016-PA/TC, publicada el 23 de setiembre de 2020. La ponencia del magistrado Eloy Espinosa-Saldaña, suscrita por los magistrados Ramos Núñez y Blume Fortini, realiza un importante análisis en torno a la facultad del empleador de fiscalizar el correo electrónico institucional de sus trabajadores.

En ese sentido, puede verificarse que, luego de evaluar los recientes pronunciamientos jurisprudenciales a nivel comparado, el voto en minoría presente en la ponencia establece lo siguiente:

> Por lo tanto, este Tribunal debe reconocer la facultad del empleador de fiscalizar e intervenir en el correo electrónico institucional si es que previamente ha comunicado al trabajador tanto de la posibilidad de la monitorización de sus comunicaciones a través de este medio, así como de las condiciones de uso permitido por la empresa.
>
> Asimismo, este Tribunal debe precisar que dicha intervención debe respetar ciertos criterios, los cuales se encuentran relacionados con el respeto del principio de proporcionalidad entre el fin que se persigue lograr con dicha intervención y la intensidad de la eventual vulneración o amenaza de violación del derecho fundamental al secreto e inviolabilidad de las comunicaciones (Expediente 0943-2016-PA/TC, 2020, fundamentos 29 & 30).

Como puede verificarse, el voto en minoría realiza un importante avance en torno al reconocimiento de la facultad de fiscalización del empleador sobre el correo electrónico institucional, estableciendo requisitos y criterios relacionados a: (i) la necesidad de comunicar previamente al trabajador sobre las políticas de uso del correo institucional y de control por parte de la empresa, y (ii) el respeto del principio de proporcionalidad en la intervención, evitando que esta sea desmedida sobre el derecho al secreto e inviolabilidad de las comunicaciones de los trabajadores (Expediente 0943-2016-PA/TC, 2020).

Lamentablemente, este último pronunciamiento del Tribunal Constitucional no logró los votos necesarios para emitir una sentencia en mayoría, por lo que queda evidenciado que la jurisprudencia constitucional no ha logrado aún establecer de forma uniforme nuevos criterios que permitan lograr soluciones a los perjuicios que puede sufrir el empleador por uso indebido del correo electrónico institucional.

Como puede verificarse, la posición que mantiene el Tribunal Constitucional de nuestro país coincide con lo establecido por la Casación 14614-2016, en la cual la Corte Suprema ha cerrado las puertas a la intervención de las comunicaciones al empleador de forma absoluta (2017). La adopción de una postura como esta, nos obliga a analizar los pronunciamientos a nivel internacional y que han sido tomados en cuenta por el voto en minoría en la sentencia recaída en el Expediente 0943-2016-PA/TC, de modo que podamos plantear nuevos criterios en el panorama que plantea la evolución de las relaciones laborales a causa de las nuevas tecnologías.

B. Desarrollo por parte de la jurisprudencia de España

Como hemos señalado anteriormente, España presenta un modelo de regulación constitucional similar al de nuestra Constitución de 1993. En ese sentido, consideramos que el desarrollo de la jurisprudencia constitucional de este país debe servir como una importante referencia a tomar en cuenta para futuros pronunciamientos de nuestro Tribunal Constitucional.

Un importante antecedente en ese país fue la sentencia de la Sala Cuarta del Tribunal Supremo, del 26 de setiembre de 2007 (S.T.S. 6128/2007). Allí, se estableció que "el ordenador era una herramienta de trabajo, propiedad del empresario, y que, en consecuencia, la potestad de control y supervisión derivaba de forma directa del poder de dirección del empresario" (García Bel & García Sánchez, 2015, p. 118). Asimismo, se consideró que dicha potestad del empleador no podía ser utilizada sin respetar los derechos fundamentales del trabajador, por lo que "las pruebas obtenidas mediante ese control empresarial que pudiesen vulnerar el derecho a la intimidad o al secreto de las comunicaciones de los trabajadores serían consideradas ilícitas" (García Bel & García Sánchez, 2015, p. 118).

Sin embargo, y esto es lo que debe ser destacado de esta sentencia, estableció que, si el empresario

> ha destruido esa presunción de privacidad o confidencialidad en el uso personal del ordenador o el correo electrónico proporcionado por este, ese control de los medios informáticos no vulneraría los derechos a la intimidad y de secreto de las comunicaciones (García Sánchez & García Bel, 2015, p. 118).

Al respecto, consideró que la forma en la cual debía eliminarse esa presunción de confidencialidad se encontraría en establecer de forma previa: (i) "las reglas del uso del ordenador", e (ii) "informando a los trabajadores de la existencia de control y de las medidas aplicables en cada caso" (García Sánchez & García Bel, 2015, p. 118).

Ello fue confirmado en una posterior sentencia de la Cuarta Sala del mismo órgano, del 6 de octubre de 2011 (S.T.S. 8876/2011), donde "aceptó las pruebas aportadas mediante el control del empleador de los medios informáticos proporcionados al trabajador, debido a que la trabajadora era conocedora de la prohibición absoluta por parte del empresario de un uso personal de las herramientas informáticas" (García Sánchez & García Bel, 2015, p. 118).

Ello llevó a la necesidad de que la jurisprudencia constitucional se pronuncie sobre el tema, al encontrarse involucrados derechos fundamentales de los trabajadores. En esa línea, el Tribunal Constitucional español reconoció en el quinto fundamento jurídico de la sentencia 241/2012 (2012) lo señalado previamente por la Cuarta Sala, respecto a que los medios informáticos de propiedad del empleador se encuentran sujetos a las facultades de control de este último. En ese sentido, consideró que el empresario debe establecer pautas relacionadas al uso de dichos medios e indicar a los trabajadores sobre la presencia de controles, así como de las medidas concretas que son empleadas (S.T.C. 241/2012, 2012). Ello, sin que deba descartarse la aplicación de otras medidas preventivas como el bloqueo de algunas páginas web (S.T.C. 241/2012, 2012).

Posteriormente, el Tribunal Constitucional español emitió una segunda sentencia respecto a este tema, la sentencia 170/2013, donde reconoció en su cuarto fundamento jurídico la facultad del empleador de fiscalizar los correos electrónicos de sus trabajadores si es que la evaluación sobre la medida aplicada permite concluir que se ha respetado el principio de proporcionalidad (2013). De este modo, estableció que debe tratarse de una medida ponderada y equilibrada que cumpla con los siguientes criterios: (i) el control del empleador ha de realizarse respetando determinadas garantías, como es el caso de la presencia de un perito informático o un notario; (ii) el contenido de las comunicaciones no deben mostrar aspectos de la vida personal y familiar del trabajador, debiendo limitarse a la información relacionada con las actividades laborales; y (iii) el control del empleador no debe tratarse de una fiscalización desproporcionada respecto a la privacidad del trabajador (S.T.C. 170/2013, 2013).

Como puede comprobarse, la jurisprudencia española apuesta por permitir el control de las comunicaciones a través de los medios informáticos proporcionados para un uso estrictamente laboral, si y solo si, el empleador ha cumplido con informar previamente las pautas de uso de dichos medios, así como las medidas de control a adoptarse. De este modo, puede verificarse una posición contraria a lo señalado por la Casación 14614-2016 (2017) y a la posición que actualmente mantiene vigente la jurisprudencia del Tribunal Constitucional del Perú, y que más bien rechaza el negar de forma absoluta el control del empleador sobre dichas comunicaciones.

C. Desarrollo por parte del TEDH

A continuación, consideramos de gran importancia destacar la publicación de una reciente sentencia de la Gran Sala del TEDH que desarrolla importantes criterios relacionados con la facultad del empleador de controlar el contenido de los correos electrónicos de sus trabajadores. Nos referimos a la sentencia 61496/08, de fecha 5 de setiembre de 2017, asunto *Barbulescu c. Rumania*, caso sobre la intervención del empleador en una cuenta de Yahoo Messenger creada a petición del empleador, con el fin de interactuar directamente con los clientes; es decir, un correo institucional.

En dicha sentencia se estableció que el vigilar y el acceder al contenido de los mensajes enviados por un trabajador mediante medios que son de propiedad del empleador, representa una vulneración de los derechos fundamentales del trabajador, si es que este no había sido previamente informado de esta posibilidad (*Barbulescu c. Rumania*, 2017). Asimismo, se señaló que la sola existencia de normas que no permitían que estos sean empleados con fines personales no justificaba los actos de empleador (*Barbulescu c. Rumania*, 2017).

En esa línea, la Gran Sala del TEDH ha establecido los siguientes criterios en el párrafo 120 de la sentencia recaída en el asunto *Bărbulescu c. Rumania* para determinar si es que quien brinda los medios puede fiscalizar las comunicaciones de sus trabajadores: (i) el trabajador debe haber sido informado previamente de las medidas que serán utilizadas, así como del alcance de las mismas, y no basta con informar de forma general sobre la posibilidad de utilizar medidas de vigilancia; (ii) las medidas empleadas deben ser proporcionales, tomando en cuenta el grado de intromisión en la vida personal y familiar del trabajador, así como la preferencia por aplicar la medida menos gravosa; (iii) el empleador debe demostrar que efectivamente existen motivos que sean concretos y previos al control que justifiquen tal medida; y (iv) la medida

debe emplearse antes del inicio del procedimiento disciplinario por parte del empleador (2017).

Como puede comprobarse, queda clara la posición de la Gran Sala a favor de la posibilidad de controlar el contenido de los correos electrónicos desde los medios informáticos otorgados por el empleador si es que se cumple con los criterios antes señalados, los cuales han sido tomados en cuenta por el voto en minoría en la sentencia recaída en el Expediente 0943-2016-PA/TC. Nuevamente, encontramos que lo aquí establecido es contrario a la Casación 14614-2016 (2017) y a la postura que mantiene hasta el momento la jurisprudencia de nuestro Tribunal Constitucional, por lo que la jurisprudencia nacional estaría asumiendo una posición contraria al TEDH y alejada de las nuevas perspectivas que surgen a nivel internacional sobre la facultad de fiscalización del empleador a la luz de las nuevas tecnologías.

IV. NUESTRA POSICIÓN SOBRE EL CONTROL DE LAS COMUNICACIONES CONTENIDAS EN EL CORREO ELECTRÓNICO

Luego de una revisión de la jurisprudencia del Tribunal Constitucional peruano, hemos podido concluir que existe un confuso panorama frente a los límites de la facultad de fiscalización de las comunicaciones contenidas en el correo electrónico institucional. Sin embargo, es claro que una posición que no cumpla con distinguir la protección del correo electrónico personal y el institucional, cerrando la posibilidad de control de forma absoluta, no solo sería contraria a lo señalado por reiterada jurisprudencia española y del TEDH, sino que, además, ignoraría por completo los graves perjuicios que puede traer para el empleador la prohibición de fiscalizar los medios tecnológicos de su propiedad que ha brindado con fines estrictamente laborales.

Es por ese motivo que nuestra posición es la de reconocer la facultad del empleador de fiscalizar e intervenir en el correo electrónico institucional si es que previamente le ha comunicado al trabajador tanto de la posibilidad de control de sus comunicaciones, así como de las condiciones de uso permitido por el centro laboral. En otras palabras, coincidimos con aquella posición que busca un equilibrio dentro de las relaciones de trabajo y que considera que, en el caso del correo electrónico institucional o de cualquier servicio de mensajería proporcionado por el empleador para un uso estrictamente laboral, no es posible alegar una expectativa de secreto o privacidad en sus comunicaciones.

Sin embargo, debemos precisar que dicha intervención debe respetar ciertos criterios que hemos podido determinar a partir de la jurisprudencia internacional y el voto en minoría en la sentencia recaída en el Expediente 0943-2016-PA/TC. Estos se encuentran relacionados con el respeto del principio de proporcionalidad entre el fin que se persigue lograr con dicha intervención y la intensidad de la eventual vulneración o amenaza de violación del derecho fundamental al secreto e inviolabilidad de las comunicaciones.

Nuestra posición se encuentra respaldada por un importante sector de la doctrina, el cual sostiene que

> cualquier medida de vigilancia sobre la correspondencia electrónica debe ser estrictamente proporcional con los fines perseguidos con ficha medida, [de modo que] la intensidad de la actividad de vigilancia sobre el objeto de control, los correos electrónicos, ha de corresponder con el fin que justifica la restricción del derecho del trabajador (Martínez Fons, 2005, p. 225).

Coincide con nuestra posición Aba-Catoira, quien sostiene que "el principio de proporcionalidad es el instrumento aplicable para solucionar estos conflictos en la búsqueda de la armonización de los intereses de ambas partes" (2014, p. 96).

Por lo tanto, nos encontramos en desacuerdo con lo señalado por la Casación 14614-2016 (2017) y con la posición actual que mantiene la jurisprudencia del Tribunal Constitucional de nuestro país. Al respecto, consideramos que ni la Corte Suprema, ni el Tribunal Constitucional deberían mantener una postura contraria a que el reglamento interno de trabajo pueda facultar al empleador a revisar el correo electrónico institucional de sus trabajadores, pues creemos que con una adecuada y previa comunicación sobre las políticas de uso del medio tecnológico y de las formas de control, es posible aceptar una intervención del empleador en las comunicaciones del trabajador sin que se vulneren sus derechos fundamentales.

V. EL CASO DE LAS CONVERSACIONES EN REDES SOCIALES: ¿PUEDE EL EMPLEADOR ACCEDER AL CONTENIDO DE DICHAS CONVERSACIONES SI SE PRODUCEN EN LOS MEDIOS ELECTRÓNICOS DE SU PROPIEDAD BRINDADOS AL TRABAJADOR?

Luego de haber expresado nuestra posición frente a la posibilidad del empleador de intervenir en las conversaciones del correo electrónico institucional si es que se cumple con los criterios antes señalados, es necesario ahora determinar cómo

deben resolverse aquellos casos en los que se produce una intervención por parte del empleador en las conversaciones de un trabajador a través de una red social. En efecto, "una de las cuestiones más actuales responde a la generalización de las redes sociales que suponen un potencial enorme para el desarrollo de la actividad empresarial y laboral sin precedentes" (Aba-Catoira, 2014, p. 105).

Al respecto, debemos partir por resaltar que el voto en minoría sobre la sentencia recaída en el Expediente 0943-2016-PA/TC (2020) muestra un importante análisis en torno a la facultad de fiscalización del empleador sobre las redes sociales de sus trabajadores, específicamente Facebook.

El análisis del voto en minoría que recae sobre la ponencia surge a partir de la demanda de amparo del señor Marco Paucarcaja, quien fue despedido por la empresa Emapa Huaral S.A., debido a que el jefe de logística advirtió que su asistenta sostenía una conversación a través de Facebook Messenger desde la computadora del centro laboral, en la que el señor Paucarcaja le solicitaba las claves de acceso a los sistemas de información confidencial de la empresa.

A partir de este caso, el voto en minoría analiza si la posición a favor de la facultad de fiscalización por parte del empleador del correo electrónico institucional puede ser también aplicada al control sobre conversaciones del trabajador a través de una red social mediante un equipo de cómputo de propiedad de la empresa. Al respecto, el voto en minoría considera lo siguiente

> En ese sentido, no es posible sostener que el hecho [de] que el empleador sea propietario del equipo utilizado para ingresar al Facebook permita considerar que una red social merece un tratamiento similar al de un correo electrónico institucional o cualquier medio de comunicación que forma parte de la empresa o que es creado a pedido de la empresa y que debe utilizarse principalmente para fines laborales. Por lo tanto, al ser Facebook un medio de comunicación externo a los instrumentos que brinda el empleador a su trabajador debe considerarse que cualquier intervención en las conversaciones privadas representa una vulneración del derecho al secreto y a la inviolabilidad de las comunicaciones (Expediente 0943-2016-PA/TC, 2020, fundamento 33).

De este modo, puede comprobarse que el voto en minoría realiza una clara distinción entre la facultad de fiscalización del empleador, por un lado, sobre el correo electrónico institucional u otros medios de comunicación de propiedad de la empresa para fines estrictamente laborales; y, por el otro, sobre las conversaciones sobre redes sociales mediante un equipo de propiedad de la empresa. En ese sentido, concluye que el hecho que Facebook represente un medio de comunicación externo a los instrumentos que brinda el trabajador, permitiría concluir una prohibición absoluta de intervención sobre las redes sociales de los trabajadores (Expediente 0943-2016-PA/TC, 2020).

Asimismo, consideramos de gran importancia resaltar el fundamento de voto del magistrado Ramos Núñez, quien realiza una interesante precisión respecto a la posición desarrollada por el voto en minoría, pues sostiene que no siempre Facebook representa un medio de comunicación externo a los instrumentos que brinda el empleador a sus trabajadores. En ese sentido, considera que "pueden existir trabajos como los de administradores de redes sociales (*community manager*) en los que la principal herramienta de trabajo es, precisamente, el empleo del Facebook, Twitter, u otra clase de plataformas" (Expediente 0943-2016-PA/TC, 2020).

En ese sentido, continúa el magistrado Ramos Núñez que en estos casos el empleador "se encuentre interesado respecto de la forma en que la página de su empresa o institución es administrada, por lo que bien podría fiscalizar los contenidos y las conversaciones que, en el uso de esa cuenta, realice el trabajador" (Expediente 0943-2016-PA/TC, 2020). Por lo tanto, puede verificarse una interesante distinción entre la fiscalización sobre las redes sociales privadas de los trabajadores y aquellas que pertenecen a la empresa, siendo posible el control sobre estas últimas en caso de un uso que pueda afectar los intereses del empleador.

En la búsqueda de poder desarrollar nuestra posición, debemos partir por tomar en cuenta que las redes sociales "comprenden plataformas creadas para intercambiar información, experiencias e intereses y generar espacios de convivencia entre los miembros de las comunidades virtuales que las integran" (Arrieta Zinguer, 2014, p. 20), permitiendo así su acceso a ellas desde cualquier lugar del mundo. En ese sentido, es evidente que se trata de un medio tecnológico ajeno al control del empleador, pues son los mismos usuarios quienes contratan un servicio específico con la empresa que administra la red social.

En esa línea, no es posible que el empleador alegue que cuenta con la posibilidad de intervenir en

las conversaciones producidas en una red social del trabajador por el simple hecho de ser propietario del soporte electrónico que permite su conexión. Ello se debe a que nos encontramos frente a un servicio que se brinda independientemente del equipo que se utilice para conectarse a esta plataforma virtual.

En ese sentido, coincidimos en líneas generales con la posición de la ponencia contemplada en la sentencia recaída en el Expediente 0943-2016-PA/TC y nos encontramos en desacuerdo con sostener que el derecho al secreto e inviolabilidad de las comunicaciones, en el caso de conversaciones realizadas a través de una red social del trabajador, merece el mismo tratamiento que el de un correo electrónico institucional o cualquier medio de comunicación creado por pedido de la empresa y que deba ser de uso estrictamente laboral.

Sin embargo, consideramos necesario también precisar el importante aporte del fundamento de voto del magistrado Ramos Núñez, el cual introduce el análisis sobre la facultad de fiscalización sobre las conversaciones sostenidas por los *community managers* encargados de las redes sociales de la empresa y donde podría encontrarse de por medio la imagen de la empresa o un uso indebido de dichas redes en horario laboral (Expediente 0943-2016-PA/TC, 2020). Por lo tanto, la posición propuesta en el voto en minoría en la sentencia recaída en el Expediente 0943-2016-PA/TC no puede ser entendida como una prohibición absoluta, siendo necesario analizar cada caso concreto en base a la función que cumple la red social dentro de la organización del centro laboral.

En conclusión, creemos que como las redes sociales del trabajador son plataformas externas a los instrumentos que brinda el empleador debe considerarse que cualquier intervención en las conversaciones privadas representa una vulneración del derecho al secreto y a la inviolabilidad de las comunicaciones. Por el contrario, será necesario realizar un análisis del caso concreto en aquellos casos en los que las conversaciones sean realizadas a través de una red social que pertenece al empleador.

Sin duda alguna, las nuevas tecnologías proponen retos de gran complejidad frente a la facultad de fiscalización dentro de las relaciones laborales en la búsqueda de que no se produzca una intervención grave y arbitraria sobre el derecho fundamental al secreto e inviolabilidad de las comunicaciones de los trabajadores. Lamentablemente, resulta imposible analizar todos los supuestos que surgen y seguirán apareciendo en torno a este actual y relevante tema de investigación, sin embargo, esperamos haber aportado algunas aproximaciones desde una perspectiva constitucional que puedan resultar de utilidad.

REFERENCIAS

Aba-Catoira, A. (2011). Los derechos de la generación electrónica en el ámbito laboral. *Revista De Derecho,* (12), 257-279.

(2014). La efectividad de los derechos de los trabajadores y del empresariado desde la implantación de las tecnologías en el ámbito laboral. *AFDUC,* (18), 79-106.

Abad Yupanqui, S. (2012). El derecho al secreto de las comunicaciones: alcances, límites y desarrollo jurisprudencial. *Revista Pensamiento Constitucional*, (16), 11-29.

Arrieta Zinguer, M. (2014). Libertad de expresión y derecho a la información en las redes sociales. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, (12), 1-31. https://doi.org/10.15425/redecom.12.2014.13

Cardona Rubert, M. B. (2015). Intimidad del trabajador y comunicaciones electrónicas según el Tribunal Constitucional. *Lex Social: Revista Jurídica de los Derechos Sociales, 5*(2), 33-51.

Cobos Campos, A. P. (2017). El derecho a la intimidad de los trabajadores y acceso del patrón a los correos electrónicos empresariales y privados. *Espaço Jurídico Journal of Law, 18*(1), 49-64.

Díaz Revorio, J. (2006). El derecho fundamental al secreto de las comunicaciones: una visión desde la jurisprudencia europea y su influencia en el Tribunal Constitucional español. *Derechos Humanos México*, *1*(2), 125-146.

García Bel, M., & García Sánchez, J. D. (2015). El poder de control del empresario sobre el correo electrónico de sus trabajadores. A propósito de la sentencia de la Sala de lo Penal del Tribunal Supremo de 16 de junio de 2014. *Actualidad Jurídica Uría Menéndez* (39), 117-123.

Gimeno Sendra, V. (2011). La intervención de las comunicaciones. En G. Priori (ed.), *Proceso y Constitución*. ARA Editores.

Martínez Fons, D. (2005). El control empresarial del uso de las nuevas tecnologías en la empresa. En S. Del Rey, & M. Luque (eds.), *Relaciones laborales y nuevas tecnologías* (pp. 187-237). La Ley.

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

Bărbulescu c. Rumania, App. No. 61496/08 (septiembre 5, 2017), http://hudoc.echr.coe.int/eng?i=001-180112.

Comisión de Trabajo y Seguridad Social del Congreso de la República, Acta de la segunda sesión ordinaria de la Comisión de Trabajo y Seguridad Social, 24 de setiembre de 2014 (Perú).

Constitución Española [C.E.], B.O.E. n. 311, 29 de diciembre de 1978 (Esp).

Constitución Política del Perú [Const.] (1993) (Perú).

Costituzione [Cost.] (1948) (It.).

Proyecto de Ley 2604/2013-CR, Proyecto de Ley que regula el uso de los medios informáticos de comunicación en los centros laborales, presentado el 3 de septiembre de 2013 (Perú).

Proyecto de Ley 3329/2013-CR, Proyecto de Ley de uso de medios informáticos en el centro de Trabajo, presentado el 1 de abril de 2014 (Perú).

Segunda Sala de Derecho Constitucional y Social Transitoria de la Corte Suprema de Justicia de la República, 10 de marzo de 2017, Casación 14614-2016-Lima (Perú).

S.T.C., 29 de noviembre de 1984 (B.J.C., No. 114/1984) (Esp.).

S.T.C., 17 de diciembre de 2012 (B.J.C., No. 241/2012) (Esp.).

S.T.C., 7 de octubre de 2013 (B.J.C., No. 170/2013) (Esp.).

S.T.S., 26 de septiembre de 2007 (No. 6128/2007) (Esp.).

S.T.S., 6 de octubre de 2011 (No. 8876/2011) (Esp.).

Tribunal Constitucional [T.C], 29 de enero de 2003, sentencia recaída en el Expediente 2863-2002-AA/TC (Perú).

Tribunal Constitucional [T.C], 18 de agosto de 2004, sentencia recaída en el Expediente 1058-2004-AA/TC (Perú).

Tribunal Constitucional [T.C], 19 de julio de 2011, sentencia recaída en el Expediente 04224-2009-PA/TC (Perú).

Tribunal Constitucional [T.C], 10 de enero de 2012, sentencia recaída en el Expediente 03599-2010-AA/TC (Perú).

Tribunal Constitucional [T.C], 10 de enero de 2012, sentencia recaída en el Expediente 00114-2011-PA/TC (Perú).

Tribunal Constitucional [T.C], 17 de julio de 2014, sentencia recaída en el Expediente 00867-2011-PA/TC (Perú).

Tribunal Constitucional [T.C], 14 de diciembre de 2018, sentencia recaída en el Expediente 5532-2014-PA/TC (Perú).

Tribunal Constitucional [T.C], 23 de septiembre de 2020, sentencia recaída en el Expediente 0943-2016-PA/TC (Perú).

MEMORIA INSTITUCIONAL

2020-2

THĒMIS

desde 1965

COMISIÓN DE CONTENIDO

La comisión de Contenido es la encargada de la edición y publicación de THĒMIS-Revista de Derecho. En el ciclo 2020-2, la comisión continuó con su labor de elaborar su tradicional producto, con la excelencia académica que lo caracteriza, buscando acercarse cada vez más a sus objetivos de indización, internacionalización y rigurosidad académica.

La comisión tuvo el agrado de presentar la edición 77 de THĒMIS-Revista de Derecho, número dedicado al eje temático de Arbitraje. Esta entrega estuvo bajo la coordinación académica de los abogados José Daniel Amado (Miranda & Amado) y Martin Doe (Corte Permanente de Arbitraje de la Haya), y contó con la asesoría temática de Fabio Nuñez del Prado (Clifford Chance). En el marco de la internacionalización de la revista, este número reunió 35 artículos –nuestra edición más extensa a la fecha–, de una multiplicidad de autores nacionales e internacionales, escritos tanto en español como en inglés. Las temáticas abordadas por dichos trabajos giraron en torno a la naturaleza y efectos del convenio arbitral; la etapa de las actuaciones arbitrales; la deliberación de los méritos y argumentos presentados por las partes en el laudo arbitral; el *case management*; el arbitraje de inversiones; y los desafíos actuales en el arbitraje. Esta edición tuvo mucho éxito, tanto comercial como académicamente, por lo que no queda duda que será un referente para el debate académico en los años por venir.

En paralelo, la comisión gestionó el proceso editorial de la edición 78, dedicada a la Competencia. Para ello, una vez culminada la convocatoria, se realizó una meticulosa selección de los artículos que conformarán la edición, sobre la base de su pertinencia, novedad, contenido y uso de fuentes bibliográficas. Posteriormente, estos fueron sometidos a un proceso de arbitraje a doble ciego (*double blind peer review*), que permitió evaluar y mejorar su calidad académica. Por último, se realizaron las ediciones en primera del número.

El ciclo acabó con un balance positivo para la comisión de Contenido, la cual logró incorporar exitosamente las nuevas normas de la séptima edición del *Manual de Publicaciones de la American Psychological Association* y de *The Bluebook: A Uniform System of Citation* en sus últimas ediciones, en el marco de su adaptación a los criterios de las indizadoras a las que desea postular.

COMISIÓN DE CURSOS & CAPACITACIONES

En el ciclo 2020-2, la comisión de Cursos y Capacitaciones realizó dos eventos que tuvieron una gran acogida y se caracterizaron por abordar temáticas poco tratadas en el medio, pero de gran vigencia y relevancia para el contexto del momento.

El primer evento realizado en el marco de sus funciones fue “IN & OUT: Curso de Derecho Aduanero y Comercio Exterior”, el cual se desarrolló el 8, 9 y 10 de octubre. Las temáticas de las mesas giraron en torno a los principales cambios normativos y retos que actualmente enfrenta el Derecho Aduanero, con especial énfasis en tributación aduanera, sanciones de la Ley General de Aduanas, control aduanero, aranceles, acuerdos comerciales y medidas de competencia desleal. El evento reunió a especialistas nacionales e internacionales como José Antonio Martel Sanchez (Tribunal Fiscal), Juan José Assereto (Zuzunaga y Assereto Abogados), Germán Pardo Carrero (Universidad del Rosario, Bogotá), Sonia Cabrera Torriani (SUNAT), Fernando Cosio (UNMSM), Sayuri Bayona (Mincetur), César Alva (Estudio Muñiz), Melissa Gómez (Fiscal Adjunta Provincial Penal Titular especializada en delitos aduaneros) y Julio Guadalupe (Rodrigo, Elías & Medrano).

Por otro lado, la comisión se dedicó al planeamiento, organización y publicidad del evento “Dos caras, una moneda: Curso Interdisciplinario de Derecho Civil y Penal”, el cual se realizará, en colaboración con Chipana & Moreno Abogados, el 28, 29 y 30 de enero del 2021.

COMISIÓN DE DESARROLLO SOCIAL

De acuerdo con su misión, durante el ciclo 2020-2 Khuska, el Programa de Desarrollo Social de THĒMIS, ha continuado trabajando permanentemente para promover el desarrollo social a través de la cultura jurídica. Para ello, este ciclo la comisión realizó la tercera edición del proyecto "Llamkay Khuska", esta vez enfocándolo en los derechos laborales de las trabajadoras del hogar. El objetivo de este proyecto fue brindar talleres jurídicos virtuales y gratuitos, en materia laboral, para las trabajadoras del hogar. El evento se llevó a cabo los días 10, 12 y 15 de agosto y contó con la participación de Fabiola del Pilar Rueda (Sunafil), Carlos Espinoza (Rebasa, Alcázar & de las Casas) y Cristina Valega Chipoco (PUCP).

Por otro lado, la comisión lanzó su nuevo segmento "Identidades", con el fin de reconocer el coraje y valentía de las personas que luchan por causas justas. Asimismo, estrenaron su sección "#1minutoconKhuska", segmento en el cual los miembros de la comisión explican sencillamente normas relacionadas con el desarrollo social. Así, en este ciclo, pese a tener menos de un año en la plataforma, el Programa Khuska alcanzó los mil seguidores en Instagram, así como los diez mil en Facebook.

Además, la comisión desarrolló el proyecto "En Línea con mi salud mental", el cual buscó potenciar el conocimiento y la capacidad reflexiva de los y las estudiantes de educación secundaria sobre la salud mental. En adición, en alianza con el Ministerio de Justicia y Derechos Humanos del Perú y la Facultad de Derecho de la PUCP, presentaron el primer concurso nacional de ensayos "Futuro de la Abogacía Peruana", en el cual participaron estudiantes de derecho de todo el país. Más aún, junto con el Grupo Interdisciplinario de Familias PUCP realizaron el conversatorio: "El Matrimonio adolescente y las uniones tempranas en el Perú: un análisis comparado teniendo en cuenta el Derecho Internacional de los Derechos Humanos". Finalmente, colaboraron en la organización de los conversatorios "Ser estudiante de Derecho en esta crisis" y "Radiografía de una crisis política: vacancia presidencial y reacción ciudadana".

COMISIÓN DE ADMINISTRACIÓN

La comisión de Administración es la encargada de la gestión económica y legal de la Asociación Civil THĒMIS. Durante el ciclo 2020-2, en el contexto de la pandemia del COVID-19, la comisión continuó su labor de adaptar los procesos de la Asociación a los desafíos que impone la virtualidad. Esto los llevó a perfeccionar y optimizar los esfuerzos hechos en el primer semestre del año.

En primer lugar, se registró a THĒMIS en la página web Joinnus Market, lo que permitió simplificar el proceso de compra de nuestros productos para los clientes y la emisión de boletas para parte de la Asociación. Además, la incorporación de THĒMIS a Joinnus Market habilitó la posibilidad de usar códigos de descuento especiales, lo que conllevó a la creación de códigos para cada comisión, así como para el RemaTHĒMIS. Este logro de la comisión trajo consigo más exposición para la marca THĒMIS, fomentando y consolidando nuestra presencia en el mercado local.

En segundo lugar, se coordinó y logró instalar un sistema de envíos de productos físicos para las distintas provincias del Perú. Ello fue una conquista que se buscó lograr desde el inicio de la pandemia, cuando por primera vez se implementó el sistema de *delivery* gratuito de productos físicos. Con este nuevo sistema, la labor se trasladó de los miembros THĒMIS, quienes debían gestionar el envío mediante *couriers* independientes, a un tercero contratado, lo que redujo los tiempos de entrega y trámites por realizar.

Estos cambios significativos, sumados al esfuerzo de todos sus miembros, llevaron a que en el ciclo 2020-2 la Asociación obtuviera una gran cantidad de ganancias, lo que a su vez permitirá una mayor inversión en futuros proyectos THĒMIS.

COMISIÓN DE RECURSOS HUMANOS

La comisión de Recursos Humanos cumple el rol de asegurar un ambiente de bienestar y amistad dentro de la Asociación, lo que lleva consigo realizar la función de comisión integradora y fiscalizadora dentro de THĒMIS. Esto incluye organizar actividades en las que los miembros ordinarios de la Asociación puedan conocerse y desarrollar una mayor confianza entre sí; así como velar por el cumplimiento de las normas de conducta dentro de la asociación y sancionar a quienes las transgredan.

En el marco de su función integradora, la comisión realizó la bienvenida para los nuevos miembros en modalidad virtual, vía Zoom. Esta vio a los miembros ordinarios de la Asociación, antiguos y nuevos por igual, participando en una serie de retos, actividades y juegos que permitieron romper con la timidez inicial de algunos. Por otro lado, también se llevó a cabo la despedida para miembros que dejaron THĒMIS en el 2020-1. Esta fue una reunión virtual conmovedora en la que se celebró a aquellos que habían dedicado parte de su vida universitaria a nuestra querida Asociación.

Además, a mediados del ciclo, la comisión organizó la tradicional Semana THĒMIS, cuya temática fue the Ē factor, con los equipos de Grease, High School Musical, Rebelde, Lazytown, Mamma Mía y Charlie y la fábrica de chocolate. A pesar de que nuevamente se tuvo que realizar por modalidad virtual, esta Semana THĒMIS fue un éxito, ya que la comisión pudo probar nuevas actividades y retos.

Por último, en el marco de sus funciones fiscalizadoras, la comisión se encargó de registrar la asistencia a las asambleas virtuales y demás eventos de THĒMIS. Asimismo, se llevaron a cabo entrevistas personales con todos los miembros de la Asociación para asegurar que se sintieran cómodos en THĒMIS.

COMISIÓN DE PUBLICACIONES

En el semestre la comisión de Publicaciones, encargada de la Editorial Jurídica THĒMIS, lanzó diversos proyectos, cumpliendo con su labor de elaborar y publicar libros de vanguardia y gran calidad académica. El primero de ellos fue la segunda edición del libro *Con licencia para anunciar: un tratado de derecho publicitario en el Perú*, bajo la coautoría de Alex Sosa Huapaya y Gustavo Rodríguez García. Esta nueva edición fue más extensa y completa que la anterior, además de contar con contenido actualizado para que sea compatible con la normativa vigente. El libro se comercializó en formato *e-book* y fue presentado en un evento virtual del mismo nombre, que contó con las ponencias de los coautores, así como de los expertos en derecho publicitario, Hugo Gómez Apac y María Antonieta Merino.

Además, la comisión elaboró una tercera edición de *El arte de dar fe*, libro coordinado por la Dra. Elena Vivar. Esta entrega recogió las ponencias de las "IV y V Jornadas de Derecho Registral y Notarial", así como artículos inéditos de autores que posteriormente decidieron ser parte de este proyecto. La venta de este libro fue mediante Amazon, lo que permitió una mayor difusión a nivel internacional. El 31 de octubre se realizó el evento de presentación con ponentes internacionales, titulado: "Experiencia iberoamericana sobre el rol de la función notarial y la tecnología en la pandemia".

En cuanto a productos físicos, la Editorial Jurídica THĒMIS presentó el libro *Mineros de lotería: Análisis de la informalidad laboral en la minería artesanal de Puno*, escrito por Patrick Wieland, Doctor en Derecho por la Universidad de Yale y especialista en derecho ambiental. El evento de presentación para dicha publicación reunió a Roxana Barrantes, Elsa Galarza, Marlene Molero y Pablo Peña.

Finalmente, la comisión organizó el evento "¿Replanteamos el matrimonio? Debate en torno al matrimonio entre personas del mismo sexo", en el marco del relanzamiento del libro del mismo nombre. Este se realizó el 14 de noviembre y contó con dos mesas en las que ponentes nacionales e internacionales enfrentaron sus puntos de vista en un debate académico.

COMISIÓN DE SEMINARIOS

La comisión de Seminarios continuó realizando sus eventos en modalidad virtual a lo largo del ciclo 2020-2, debido a la pandemia del COVID-19. De este modo, cumplió con su misión de contribuir a la difusión de la cultura jurídica en nuestro país. En el ciclo, la comisión organizó dos eventos.

El primero fue "Capacitaciones Solidarias: Reactivación económica", una colaboración realizada en el marco de una iniciativa organizada por Mujeres en la Academia y Alianza Pro Bono. El tema abordado fueron las herramientas normativas que se pueden utilizar para fomentar la reactivación económica, un tópico de gran interés en una época en la que nuestra economía se encontraba casi paralizada. El evento se realizó el jueves 24 de septiembre mediante la plataforma Zoom. Las capacitaciones fueron lideradas por Ljubica Vodanovic (EY Perú), Alberto Ratia Mendoza (Fintechu MX), Lisbeth Benavides (Miranda & Amado), José Enrique Fernández (Miranda & Amado), Renzo Agurto (Miranda & Amado) y Denisse Miralles (ProInversión). La totalidad del dinero recaudado con la venta de entradas fue donada a las ONGs Minkando y Nietos Itinerantes.

El segundo evento del ciclo fue el "II Congreso Internacional de Derecho Mercantil", el cual tuvo una gran acogida, tanto nacional como internacional. Este se realizó en los días 10, 11 y 12 de diciembre, después de una reprogramación a causa de las protestas civiles vividas en noviembre. Los ponentes del seminario fueron: Alex Sosa (PUCP), Juan Luis Hernández (Hernández & Cía.), Moisés Rejanovinschi (Estudio Moisés Rejanovinschi), Javier Pazos (PUCP), Luis Alonso García (Estudio Echecopar), Liliana Navarrete Hayakawa (BID), Diego Harman (Garrigues), Fernando Sam (PUCP), Sergio Amiel (Garrigues), Eileen Infantas (Echecopar), Julio Durand (PUCP), Wendy Ledesma (Indecopi), Mila Guillén Rispa (SBS), Cecilia Kahn (CMS Grau), José Miguel de la Calle Restrepo (Garrigues Colombia), Ana Alba Betancourt (UNAM) y Cristina Mesa (Garrigues España).

Finalmente, en este ciclo la comisión inició la organización y venta para el "Congreso Internacional de Género y Derecho: Avances y retos actuales", que se realizará en enero del 2021.

COMISIÓN DE IMAGEN INSTITUCIONAL

La función de la comisión de Imagen Institucional es promover la marca THĒMIS mediante la elaboración, gestión y difusión de contenido publicitario a través de las redes sociales de la Asociación. Para ello, los comisionados de Imagen Institucional diseñan las líneas gráficas de todas las campañas publicitarias de los productos THĒMIS, sean revistas, libros, cursos, seminarios u otros. Asimismo, tienen a su cargo la realización de las campañas y eventos de la Liga THĒMIS y el tradicional Acércate a THĒMIS.

En este semestre, el tema de la Liga THĒMIS fue el derecho a la educación y el estado del sistema educativo nacional en la situación de aislamiento social obligatorio causado por la pandemia del COVID-19. La campaña se tituló "Liga THĒMIS por el Acceso a la Educación a Distancia". El evento central de la Liga fue el conversatorio "Reconectando: reflexiones sobre la educación a distancia en el Perú", el cual se realizó el 5 de noviembre mediante la plataforma Zoom. Este tuvo como ponentes a Patricia Ames (PUCP), Francisco Eguiguren (CIDH), José Rodríguez y Pilar Butrón (DIGEBR). El conversatorio tuvo una gran acogida, tanto en el evento en sí, como en la transmisión en vivo por Facebook.

Por otro lado, en esta oportunidad se escogió la temática de Aladino para el Acércate a THĒMIS, representando al nuevo mundo al que uno accede cuando ingresa a la asociación. El evento se realizará el 7 de enero del 2021 y contará con los miembros extraordinarios: Fernando Cantuarias, Valeria Osorio, Óscar Montezuma, Uber López y Thalía Villegas.

COMISIÓN DE ACTUALIDAD JURÍDICA

EnfoqueDerecho.com tiene como misión ser un referente en cuanto al devenir cotidiano de los temas vinculados con el derecho en el Perú y el mundo; un portal en el que tanto estudiantes como profesionales pueden plasmar sus opiniones a través de artículos, entrevistas, blogs y demás productos.

En ese sentido, durante el segundo semestre del 2020, EnfoqueDerecho.com realizó semanas temáticas, correspondientes a las temáticas de Tax, Arbitraje y Redes sociales en las que entrevistaron a diversos profesionales de aquellas áreas como Beatriz de la Vega (EY Perú), José Eloy Anzola (Escritorio de Abogados Anzola Raffalli y Rodríguez) y Jairo Cieza Mora (Cieza Abogados). Asimismo, se llevaron a cabo las histerias de "Derecho y Superhéroes" y "Mitología y Derecho; así como los especiales "Habeasdata.com", "Derecho aduanero" y "Fin de la Década". Más aún, la comisión gestionó la apertura de dos nuevos blogs: "Derecho Fandom", un espacio coordinado por el profesor Rómulo Morales; y "Fair Play", un blog colectivo conformado por abogados y especialistas de la revista española *Fair Play* de la Universidad Pompeu Fabra.

Por otro lado, continuaron con la repotenciación de sus redes sociales, inaugurando una nueva línea gráfica que permite el rápido reconocimiento de los productos de la comisión. En ese sentido, lanzaron el producto "Enfoque Semanal" y produjeron nuevas entregas de su podcast, "No todo es Derecho", y de su microprograma "Sin Prejuicio", elaborado en colaboración con la Facultad de Derecho de la PUCP. En adición a ello, realizaron el "Versus Reales" en el que los abogados Francisco Avendaño y Alan Pasco debatieron problemáticas del derecho real. También, junto con Alfredo Bullard, produjeron unas clases de Análisis Económico del Derecho, bajo el título "Enfoque Económico".

En este semestre la comisión realizó diversos conversatorios: "Sistema penal integral en los delitos de corrupción de funcionarios"; "¿Nulidad o ineficacia? A propósito del VIII Pleno Casatorio"; "Novedades al TUO de la Ley de Expropiaciones"; "Ser estudiante de Derecho en esta crisis"; "ABC de la crisis política en el Perú"; "Evolución y competencia: el arbitraje como orden espontáneo"; el debate "¿Es necesaria una reforma constitucional?"; el evento "¿Cambiar el régimen tributario de la Constitución? Diálogos tributarios desde una perspectiva constitucional".

COMISIÓN DE FINANCIAMIENTO

La comisión de Financiamiento tiene como consigna la innovación constante de la marca THĒMIS, un objetivo que han perseguido lo largo del ciclo 2020-2. La comisión supo adaptarse a la coyuntura de la pandemia de COVID-19, trasladando la mayoría de sus funciones al ámbito virtual sin mayor problema.

Como es tradicional, este ciclo, la comisión se dedicó a la búsqueda de auspicios para los diversos productos que ofrece la Asociación. Para ello, se contactaron con diversos estudios de abogados e instituciones y ganaron su apoyo a través del ofrecimiento de diversos beneficiosos. Además, Financiamiento jugó un rol clave en el registro y disponibilidad de los productos THĒMIS en la plataforma de ventas Joinnus Market.

Por otro lado, durante este semestre, los miembros de la comisión diseñaron, gestionaron y produjeron el nuevo *merchandising* de THĒMIS. Este consistió en una nueva línea de tasas y bolsas de tela, que incorporaron ideas de diseño de los demás miembros de la Asociación. Asimismo, en el mes de diciembre se realizó el RemaTHĒMIS, que tuvo mucho éxito y produjo grandes ingresos para la asociación. Por último, la comisión se encuentra gestionando el proyecto de la nueva página web de THĒMIS, la cual incluirá la posibilidad de hacer compras directas para nuestros clientes.

HISTORIA DE LA COMISIÓN DE CONTENIDO

En 1965, **THĒMIS** se fundó con la idea de difundir la cultura jurídica a través de un solo producto que ha perdurado y se ha modernizado a lo largo de los años. Se trata de **THĒMIS-Revista de Derecho**, una publicación editada por alumnos de la Facultad de Derecho de la PUCP, pertenecientes a la Asociación Civil **THĒMIS**. El editor general de **THĒMIS-Revista de Derecho** es el director de la Comisión de Contenido. La edición de nuestro producto bandera ha estado a cargo, desde sus inicios, por los siguientes abogados, académicos y estudiantes de Derecho:

PRIMERA ÉPOCA

THĒMIS 1	Domingo García Belaúnde, Luis Arbulú Alva, Luis Stucchi Díaz
THĒMIS 2	Domingo García Belaúnde, Luis Arbulú Alva, Luis Stucchi Díaz
THĒMIS 3	Domingo García Belaúnde, Luis Arbulú Alva, Luis Stucchi Díaz
THĒMIS 4	Domingo García Belaúnde
THĒMIS 5	Domingo García Belaúnde
THĒMIS 6	Luis Arbulú Alva
THĒMIS 7	Luis Arbulú Alva

SEGUNDA ÉPOCA

THĒMIS 1	José Daniel Amado Vargas, Fernando Arias-Stella Casillo, Eduardo de Rivero Santana, Jacqueline Chappuis Cardich, Gustavo López- Ameri Cáceres
THĒMIS 2	José Daniel Amado Vargas, Fernando Arias-Stella Casillo, Eduardo de Rivero Santana, Jacqueline Chappuis Cardich, Gustavo López- Ameri Cáceres
THĒMIS 3	José Daniel Amado Vargas, Fernando Arias-Stella Casillo, Eduardo de Rivero Santana, Jacqueline Chappuis Cardich, Gustavo López- Ameri Cáceres
THĒMIS 4	José Daniel Amado Vargas, Fernando Arias-Stella Casillo, Eduardo de Rivero Santana, Jacqueline Chappuis Cardich, Gustavo López- Ameri Cáceres
THĒMIS 5	Beatriz Boza Dibós
THĒMIS 6	Beatriz Boza Dibós
THĒMIS 7	Beatriz Boza Dibós
THĒMIS 8	Beatriz Boza Dibós
THĒMIS 9	María Teresa Quiñones Alayza y Juan José Ruda Santolaria
THĒMIS 10	María Teresa Quiñones Alayza y Juan José Ruda Santolaria
THĒMIS 11	María Teresa Quiñones Alayza y Juan José Ruda Santolaria
THĒMIS 12	María Teresa Quiñones Alayza y Juan José Ruda Santolaria
THĒMIS 13	Javier Chocano Portillo y César Parodi Martins
THĒMIS 14	Javier Chocano Portillo y César Parodi Martins
THĒMIS 15	Javier Chocano Portillo
THĒMIS 16	Verónica Zavala Lombardi
THĒMIS 17	Verónica Zavala Lombardi
THĒMIS 18	Martín Mejorada Chauca
THĒMIS 19	Martín Mejorada Chauca
THĒMIS 20	Martín Mejorada Chauca
THĒMIS 21	Eduardo Sotelo Castañeda
THĒMIS 22	Eduardo Sotelo Castañeda

THĒMIS 23	José Ignacio Castro Otero
THĒMIS 24	José Ignacio Castro Otero
THĒMIS 25	Enrique Felices Saavedra
THĒMIS 26	Enrique Felices Saavedra
THĒMIS 27	Enrique Felices Saavedra
THĒMIS 28	Enrique Felices Saavedra
THĒMIS 29	Enrique Felices Saavedra
THĒMIS 30	José Juan Haro Seijas
THĒMIS 31	José Juan Haro Seijas
THĒMIS 32	Juan Antonio Égüez Toledo
THĒMIS 33	Gonzalo Zegarra Mulanovich
THĒMIS 34	Gonzalo Zegarra Mulanovich
THĒMIS 35	Gonzalo Zegarra Mulanovich
THĒMIS 36	Gonzalo Barrionuevo Alba
THĒMIS 37	Gonzalo Barrionuevo Alba
THĒMIS 38	Bruno Amiel Rodríguez-Carpi
THĒMIS 39	Bruno Amiel Rodríguez-Carpi
THĒMIS 40	Bruno Amiel Rodríguez-Carpi
THĒMIS 41	Gilda Spallarossa Lecca
THĒMIS 42	Carlos Arata Delgado
THĒMIS 43	Carlos Arata Delgado
THĒMIS 44	Fernando Berckemeyer Olaechea
THĒMIS 45	Enrique Pasquel Rodríguez
THĒMIS 46	Mirella Miranda Nique
THĒMIS 47	Alejandro Manayalle Chirinos
THĒMIS 48	Alejandro Manayalle Chirinos
THĒMIS 49	Javier Alonso de Belaúnde de Cárdenas
THĒMIS 50	Javier Alonso de Belaúnde de Cárdenas
THĒMIS 51	Óscar Súmar Albújar
THĒMIS 52	Óscar Súmar Albújar
THĒMIS 53	Luis Miguel Velarde Saffer
THĒMIS 54	Luis Miguel Velarde Saffer
THĒMIS 55	Mario Drago Alfaro
THĒMIS 56	Mario Drago Alfaro
THĒMIS 57	María José Higueras Chicot
THĒMIS 58	Claudia Lazarte Abarca y Mariano Peró Mayandía
THĒMIS 59	Mariano Peró Mayandía y Guillermo Arribas Irazola
THĒMIS 60	Guillermo Arribas Irazola
THĒMIS 61	Marco Zaldívar Chauca
THĒMIS 62	Marco Zaldívar Chauca
THĒMIS 63	Carlos Fernando de Trazegnies Valdez
THĒMIS 64	Carlos Fernando de Trazegnies Valdez
THĒMIS 65	Luis Fernando Roca Lizarzaburu
THĒMIS 66	Luis Fernando Roca Lizarzaburu
THĒMIS 67	Gonzalo J. Monge Morales
THĒMIS 68	Carla Regina Odar Chang
THĒMIS 69	Carla Regina Odar Chang y Erick E. Vargas Guevara
THĒMIS 70	Erick E. Vargas Guevara y Ciro Vladimir Ortega Mejía
THĒMIS 71	Ciro Vladimir Ortega Mejía y Joseline Zela Concha
THĒMIS 72	Renzo Augusto Zárate Villantoy y Joseline Zela Concha
THĒMIS 73	Renato Higa Griffin
THĒMIS 74	Gabriela Rosa Pacheco Rodríguez
THĒMIS 75	Axel Valverde Pariasca
THĒMIS 76	Axel Valverde Pariasca y Lucia Beatriz López Gallardo
THĒMIS 77	Lucía Beatríz López Gallardo y Luz Andrea Caycho Cáceres
THĒMIS 78	Luz Andrea Caycho Cáceres y Sol María Guevara Ratto
THĒMIS 79	Chiara Lucía Jacob Camaiora

Exmiembros de la Asociación Civil THĒMIS

Luis Abramovich Ackerman | Carmen María Accinelli Obando | Otto Alonso Acosta Bernedo | Luis Enrique Adrianzén Trint | Úrsula Afán Castillo | Édgar Aguirre Ramos| Guillermo Alarcón Zubiaurr | Omar Alejos Mata | Javier Albán González | César Antonio Alcorta Suero | Jenny Aliaga Aliaga | Luis Aliaga Blanco | Jimena Aliaga Gamarra | María Cristina Alva Noriega | Juan Carlos Alvarado Ortiz | Andrea Valeria Álvarez Tapia | José Daniel Amado Vargas | Marisa Amado Vargas | María José Amado Villacorta | Kathy Ames Valdivieso | Bruno Amiel Rodríguez-Carpi | Alejandra del Carmen Aquije Cornejo | Andrés Avelino Aramburú Piaggio | Carlos Arata Delgado | Agnes Arbaiza Mejía | Marco Antonio Arbayza Obeso | César Arbe Saldaña | Joao Windson Arbildo Caro | Luis Arbulú Alva | Gabriela Arbulú León- Prado | Teresa Arce Coronel | Mario Arce Rodríguez | Diana Arciniega López | Sergio Arellano Gonzales | Fernando Arias- Stella Castillo | Cristina Arizmendi Bellido-Tagle | Ariana Armacanqui Paredes | Guillermo Arribas Irazola | Giancarlo Arrivasplata Núñez | Arturo Arróspide Villarán | Carla Arteaga Alarcón | Sergio Avendaño Bavestrello | Lucía Ávila Bedregal | Carolina Awapara Penalillo | Álvaro Ayllón Bondy | Felipe Ayulo Elejalde | Cecilia Azerrad Urrutia | Inés Baca de la Piedra | Juan Luis Balarezo Revilla | Francesco Balbi Castellano | Fabiola Baquerizo Micheline | Alonso Barreda Ayllón | Jorge Gonzalo Barrionuevo Alba | Ana Cristina Barrionuevo Luna | Manuel Barrios Arbulú| María Barrón Rodríguez | Sebastián Basombrío Dughi | Sandra Basurco García-Zapatero | Ariana Bassino Balta | Jack Batievsky Sapck | Pamela Battifora del Pozo |Andrés Bayly Letts | Kiara Bazán Santillán | Micaela Bedoya Bahamonde | Carmen Luisa Bedoya Eyzaguirre| Eduardo Bedoya Pérez | María del Carmen Bedoya Valdez | Maria Lucía Bellido Bertie | Adriana Bellido Ludowieg | María Fátima Benavides Maza | Ximena Benavides Reverditto | Francisca Benavides Roose | Carla Bengoa Rojas | Úrsula Ben-Hammou Novoa | Licy Benzaquén Gonzalo | Fernando Berckemeyer Olaechea | Gonzalo Bernal Neunmann | Gabriela Bernales Wan | Javier Berrospi Vivar | Sergio Alejandro Berrospi Vivar | María Cecilia Blume Cillóniz | Iván Blume Moore | Miluska Bobadilla Chancafe | Zuly Niskar Bolaños Enríquez | Ramiro Bolaños Flores | Gonzalo Bonifaz Tweddle | Costanza Borea Rieckhof | Lorena Borgo Hannach| Víctor Alfonso Bosleman Córdova | Beatriz Boza Dibós | Guillermo Bracamonte Hinostroza | Laura Bravo Chagua | Ángel Sebastián Bravo Morales |Elizabeth Briones Gómez | Patricia Brocos Duda | Mayra Bryce Alberti | Alfredo Bullard González | Cyndel Caballero Fernández | Daniel Cabrera Morgan | Franco Marco Caccia Arana | Fernando Cáceres Freyre | Franklin Cáceres Freyre | Aldo Cáceres Martínez | Augusto Cáceres Vega | Andrea Cadenas Cachay | Alejandra Calderón Santillán | Ana Calderón Torres | Héctor Calero Ramírez | José Calero Zavaleta | Jorge Calle Brush | Analía Calmell del Solar del Río | Javier Calmell del Solar Monasi | María Jimena Camacho Vega | Andreína Camargo Neyra | Paula Lucía Camino Morgado | Cecilia Cánepa Olaechea | Carlos Alfonso Canevaro Montesinos | Fernando Cantuarias Salaverry | María Fernanda Caparó Beltrán | Alejandro Cardoza Ayllón | Pamela Léia Caro Coria | Mariella Carrasco Gadea | Verónica Carrasco Núñez |Alejandra Sofía Carrillo Ayala | Diego Carrión Álvarez-Calderón | Christian Armando Carvajal Valenzuela | Carlos Casabonne Stoessel | Juan Manuel Casalino Franciskovic | Patricia Casaverde Rodríguez | Julio Casma Rocha | Renzo Castagnino Abásolo | Alejandra Castañeda Andrade | Gian Paul Castañeda Carruitero | Fernando Castañeda Melgar| Marcelo Castilla Báez | José Ignacio Castro Otero | Diego Castro Panez | Evelyn Castro Ramos | Álvaro Castro Reátegui | Junior David Castro Reynoso | Augusto Francisco Cauti Barrantes | Constanza Cavallero Portugal | Alejandro Cavero Alva | Luz Andrea Caycho Cáceres | Mariana Cazorla Quiñones | Daniel Chancafe Rosas | María Fernanda Chanduví Herrera | Daniela Chang Rodríguez | Jackeline Chappuis Cardich | Vanessa Chávarry Meza | Melady Steffania Chávez Macuado | María José Chávez Pozzi-Escott | Mauricio Checa Oliva | Jorge Chiang Belliki | Carolina Chipollini Román | Liz Chirinos Cuadros | Marco Alejandro Chirinos Herrera | Javier Chocano Portillo | Rafaela Chumpitazi Saltarich | Astridt Chuy Colonia | Karina Chung Fernandini | Aldo Renato Cisneros Jirón | Camilo Clavijo Jave | María Andrea Colina Cardoso | Úrsula Collimboy Sayán | Jorge Contreras Condezo | Lorena Cook Llosa | Marcel Cordero

Cabrera | Patricia Córdova Muñaqui | Luis Felipe Cornejo Arenas | Nicolás Cornejo Gerner | Rita Cornejo Lanao | Carlos Cornejo Vargas | Micaela Cortés Cabieses | Iván Cortés Tejada | Mariliha Alejandra Corzo Tueros | Carlos Cotera Solano | Chiara Crestani Queirolo | Juan Carlos Crisanto Vargas | Claudio Cruces Larco | Pablo Cueto Saco | Ana Sofía Cuevas Sánchez | Vera Czichowsky Hinterseer | Jorge Dajes Fleishman| Joanna Dawson Pendavis | Alberto de Belaúnde de Cárdenas | Javier Alonso de Belaúnde de Cárdenas | Luis de Bernardis Llosa | Federico de Cárdenas Romero | Arantxa de la Flor Giuffra | Fernando de la Flor Koechlin | Nicolás de la Flor Puccinelli | José María de la Jara Plaza | Martín de la Jara Plaza | Fernando Damián de la Puente Limay | Javier de la Vega Gómez | Jimena de la Villa Bayona | Camila de Lasa Larrea | Gabriela Lucía de Olazával Aguilar | Milagros de Pomar Saettone | Eduardo de Rivero Santana | Sebastián de Rutté Boisset | Patricio Ato del Avellanal Carrera | Rodrigo del Carpio Alarcón | Enrique del Castillo Fernández | Fernando del Mastro Puccio | María Verónica del Mastro Puccio| José Antonio del Risco Ramírez | Álvaro del Valle Roeder | Óscar del Valle Salinas | Chantal Marie Deleplanque Sánchez | Mariana Delgado Zeppilli | Miguel Denegri Portela | Tomás Denegri Vargas| Kai Díaz-Albertini Northcote | José Díaz del Valle | Margarita Díaz Picasso | Talía Díaz Rodríguez | Nathalie Díaz Silva | Gisella Domecq Garcés | Andrea Domínguez Noriega | Mario Drago Alfaro | Paul Duclós Parodi | Camila Dueñas Quiñones | Enzo Dunayevich Morales | Augusto Durand Palacios | Javier Echecopar Sabogal | Juan Antonio Égüez Toledo | Inés Elías Dupuy | Juan Diego Elías Puelles | Ricardo Elías Puelles | María José Erausquin Herrada | Angela Mérylin Escobar Huanca | Cedrik Hernán Espejo Tello | Stephanie Espejo Espinal | Alessandra Espino Beltrán | Walter Esquivel Valera | Anthony Exebio Mori | Yhasira Elisa Fabián Terreros | Jacqueline Febres Ballón | Enrique Felices Saavedra | Kevin Fernando Fernández Herrera | Enrique Ferrand Rubini | Arturo Ferrari Carrasco | Cristina Ferraro Delgado | Verónica Ferrero Díaz | Manuel Ferreyros Pérez-Ízaga | Pamela Ferro Cornejo | Gustavo Fierro Campos | Alejandra Flecha Corvetto | Rodrigo Flores Benavides | Daniel Flores Consiglieri | Cristina Flores Ligarda | Francisco José Floríndez Aramburú | Hugo Forno Odría | Ian Michael Forsyth Daneri | Laura Francia Acuña | Daniel Francisco Pimentel | José Enrique Frías Amat y León | Sandra Fuentes Ñique | Alexia Gaitán Meléndez | Nicolás Galindo García | Marcos Gallardo Jimenez | Alejandra Estefanía Gallardo Siguas | Patricia Gallegos Quesquén | Susana Gallo Alzamora | Giuseppe Galluccio Tonder | Viviana Gálvez Córdova | Edgardo Gamarra Bellido | Marco Antonio Gamarra Galindo | Nicol Lucero Gaona Buitrón | Carlos Garatea Grau | Adriana Garcés García | Gabriela García Arcía | Domingo García Belaúnde | Víctor Geancarlo García Huamán | Juan García-Montúfar Sarmiento | Alejandra García Oviedo | Frank Fermín García Santos| José Luis Gargurevich Valdez | Mijael Garrido-Lecca Palacios | Rubiela Gaspar Clavo | Bruno Giusti Díaz |Carlos Glave Mavila | Andrés Gómez de la Torre Barrera | Enrique Gómez Ossio | Carlos Andrés Gómez Ramos | Corina Gonzales Barrón | Cristina Gonzales Camarena | Daniel Gonzales La Rosa | Arabella Gonzales Netto | Cinthia Gonzales Ramos | Lucrecia González-Olaechea Dutari | Óscar González Romero | Cristy Layla Gonzales Sifuentes | Gianina Gotuzzo Oliva | José Bernardo Goyburu Vassallo | Carlos Granda Bullón | Agustín Grández Mariño | Daniella Guerrero Menes | Melisa Guevara Paredes | Nydia Guevara Villavicencio | Ian Dolph-Jean Guimaray Vidal | Mauricio Gustín de Olarte | Juan Carlos Gutiérrez Azabache | Carlos Hamman García-Belaúnde | José Juan Haro Seijas | Allan Hennings Marianyi | Mariella del Carmen Hernández Valencia | Ximena Herrera Blácido | Kristiam Herrera-Carrasco Monteagudo | Fanny Herrera Cevasco | Fernando Hesse Alfageme | Alonso Hidalgo Salinas | Renato J. Higa Griffin |María José Higueras Chicot | Gerardo Holguín Salazar | Zoila Horna Zegarra| Ísabo Hospinal Alcántara | Juan Israel Huamán Koo | Mario Huapaya Nava | Camilo Huaroc Chacón | Loana Huerta Hidalgo | Eduardo Hurtado Arrieta | Fernando Hurtado de Mendoza Pomar | Úrsula Indacochea Prevost | Patricia Inga Falcón | Eduardo Gonzalo Iñíguez Ortiz | Gianfranco Iparraguirre Romero | Roy Irribarren Calderón | Rosario Isasi Morales | Katia Cecilia Jacinto Moya | José Alfredo Jiménez García | María Alejandra Justo O'Hara | Baldo Kresalja Roselló | Rúzika Kresalja Santos | Antonio Kuljevan Pagador | Diego La Rosa Gonzales del Riego | Sheila La Serna Jordán | Juan Miguel Labarthe Ferreyros | Félix Labrín Mendoza | Alexa Laguna García | Rafael Lanfranco Gallofré |Fernando Lanfranco Garrido Lecca | Elizabeth Laqui Martínez

| Erick Lau Gastelo | Anthony Laub Benavides | Claudia Lazarte Abarca | Elsa Marina Lazarte Zabarburú | Joaquín Lazo Pérez-Palma | Denise Ledgard Antúnez de Mayolo | Alexandra Lelouch Loebl | Adrián Rodolfo Lengua Parra| Wendy León Espinoza | Sebastián León Saavedra | Alessia Lercari Bueno | Mario Lercari Bueno | Nicolás Lerner von Mallinckrodt | Eliana Gisella Lesem Guerra | Julián Li Díaz | Diego Ignacio Liendo Ganoza | Ariana Lira Delcore | Francisco Lira Miró Quesada | Isabel Lira Miró Quesada | Alejandro Lira Pinedo | Juan Alberto Liu Sánchez | Beatriz Llanos Cabanillas | Pedro Llerena Córdova | Mónica Llosa Gastañeta | Alejandra Llosa Parró| Gustavo López-Ameri Cáceres | José Rodrigo López Castro | Lucia Beatriz López Gallardo | Henrry López Javier | Uber Adán López Montreuil | Julia Loret de Mola Cáceres | Eduardo Loret de Mola Ugarte | Claudia Lovón Benavente | Óscar Lozada Mego | Lucía Luna Negrón | Álvaro Luna-Victoria Saravia | Rosa Isabel Luna-Victoria Jammaers | Roberto Guillermo MacLean Martins | Kiana Maggiolo Cook | Mariana Mallea Quiroz | Elody Malpartida Zamora | Francisco Mamani Ortega | Alejandro Manayalle Chirinos | Renato Manrique Portal | Jonatan Samuel Marcés Everness | Chiara Marinelli Tagliavento | Úrsula Martínez García | Mercedes Martínez Meza | Lucía Martínez Mezón | Juan José Martínez Ortiz | Natalia Martínez Rosado | Flavia Martínez Tarazona | Kathia Martínez Tarazona | Pablo Martínez Valdez | Giuseppe Marzullo Carranza | Verónica Maseda Beaumont | Camila Masini Ortiz | Daniel Masnjak Marín | Paola Massa Belaúnde | Giorgio Massari Figari | Daniela Maurate de la Torre | Elías Maya Zusman | Renzo Kenneth Mayor Mayor | Joaquín Alejandro Mejía Cacho | Juan Carlos Mejía Cornejo | Jorge Melo Vega | Ernesto Mendiola Chirinos | Mariana Mendoza Benza | María del Carmen Mendoza Delgado | Patricia Mendoza Franco | Fiorella Mendoza Graza | Ana Paula Mendoza Rázuri | Daniela Meneses Sala | Marilú Merzthal Shigyo | Diana Milberg Garrido-Lecca | Hector Gianfranco Míñope Ferro | Francisco Miranda Aguilar | Guillermo Miranda Benavides | Renzo Miranda Lucas | Mirella Miranda Nique | Josefina Miró-Quesada Gayoso | Manuela Alejandrina Molina Altamirano | Fernando Molina Rey de Castro | Gonzalo Monge Morales | Luis Javier Montalva Capella | Grecia Montesinos Calero | Rosa María Montero Musso | Juan Francisco Monteverde Vargas | Óscar Montezuma Panez | Giacomo Montiel Ibarguren | Miguel Morachimo Rodríguez | Diego Morales Alferrano | Elva Morán Rodríguez | Sheyla More Sánchez| Andrea Morelli Ferreyros | Jorge Luis Morelli Ferreyros | Giuliana Moreno Horna | Pablo Mori Bregante | Johanna Mosqueira Gonzáles |Vasco Mujica Roggero | Ítalo Muñoz Bazán | Milagros Muñoz Bazán| Jaime Mur Campoverde| Jackeline Murillo Díaz | Valeria Alejandra Murrieta Noly | Milagros Mutsios Ramsay| Alonso Nájar Ramal | Héctor Willman Navarro Toledo | Mariana Negri Mendiola | Aritha Neyra Mejía | Paul Nina Nina | Manuel Noya Sarmiento | Fabio Núñez del Prado Chaves | Manuel Núñez Farfán | Freddy Salvatore Núñez Marmanillo | Mary Cielo Núñez Minaya | Monica Núñez Salas | Raúl Ñato Zevallos | Cecilia O´Neill de la Fuente | Yascila Oblitas Obeso | Diego Ocampo Acuña | Paola Ochoa Olivera | Carla Regina Odar Chang | Lucía Olavarría Salinas | Pilar Olavide Galdós | Pía Gabriela Olea Ubillús | Pilar Oliva Rocca | Antonio Olórtegui Marky | Bernando Ortega Malatesta | Ciro Vladimir Ortega Mejía | Mishel Ortiz Ayala | Katherine Lisseth Ortiz Cornejo | Gonzalo Ortiz de Zevallos Olaechea | Valeria Osorio Véliz| Andrés Osterling Letts | Gabriela Pacheco Rodríguez | Giselle Pacheco Guillén | Claudia Pacora Rodríguez | Rodrigo Padilla Philipps | Ximena Palacios Landauro | Álvaro Palao Carrera | Xavier Palao Carrera | Andrea Marcela Paliza Olivares | Emilio Paliza Ortega | Paola Palma Mormontoy | Susana Paniagua Jara | Valentín Paniagua Jara | Fernando Pardo Segovia | César Augusto Parodi Martins | Andrea Parra Estela | Diego Alonso Parra Ortiz | Mario Pasco Lizárraga | Enrique Pasquel Rodríguez | Carlos Alberto Patrón Salinas | Denisse Paucar Laurencio | Juan Manuel Pazos Aurich | José Pedraza Newton | Milan Pejnovic Delgado | Eduardo Peláez Santillán | Macarena Penny Yrigoyen | Fernando Peña Neves | Miranda Peñaloza Gonzales | Joseline Pérez Cámara | Miguel Ángel Pérez Caruajulca | Carolina Pérez Harm | Diego Pérez Terry | Mariela Pérez-Costa Piscoya | Luz María Pérez-Garland Gamio | Mariano Peró Mayandía | Chiara Pescetto Bustamante | Alejandro Peschiera Bonifaz | Renato Piazzón Falcone | Noé Fernando Nicolás Piérola Castro | Grecia Pillaca Burga | Antonio Pinilla Cisneros | Pilar Pizarro Bustamante | Alfredo Polo Gálvez | Vladimir Popov | Andrea Portaro Pancorvo | José Miguel Porto Urrutia | Diego Portocarrero

Koechlin | Stefany Porudominsky Rotstain | Patricia Pow-Sang Tejada | Rafael Prado Bringas | Bertha Prado Manrique | Angélica Patricia Pretell Gómez | Manuel Privat Colla | Roque Puch de Romaña | Luis Guillermo Puelles Olivera | Juan Sergio Puicón Deza | Rafael Puiggrós Aramburú | Diego Pulgar-Vidal Lehmkemper | Flavia Queirolo Nicollini-Pflucker | Alejandra Quintanilla Gutiérrez | María Teresa Quiñones Alayza | Matías Quiroz Arellano | Carmen Luz Quiroz Romero | Emily Quispe Cullampe | Arturo Magno Quispe Quiroz | Cindy Quispe Valencia | Rodrigo Rabines Matta | Sergio Ismael Ramírez Cárdenas | Pedro Ramírez Pequeño | Roxana Ramírez Ráez | Christian Ramírez-Gastón Durán | Fernando Ramírez-Gastón Lecca | Stacy Ramírez Wong | Gabriela Ramos Traverso | Rodrigo Ramos Vásquez | Silvana Rebagliati Castro | Alberto Rebaza Torres | Aldo Reggiardo Denegri | Fernanda Rénique Vega | Cristina Rey Montes | Claudia Cristina Reyes Juscamaita | Tamara Rezqallah Arón | Virginia Rieckhof Borja | Viviana Ritchie Martínez | Eduardo Reyna Oie | Farid Borhan Rifai Bravo | Carla Rizo-Patrón Labarthe | Ricardo Rizo-Patrón Olaechea | André Robilliard Escobal | Grecia Robles Vila | Alessia Roca Lizarzaburu | Luis Fernando Roca Lizarzaburu | Alessandra Camila Rocca Rodríguez | Lucía Rodrigo Rohrhirsch | Ana Lucía Rodríguez Angulo | Sergio Rodríguez Asencios | Romina Rodríguez Damiani | Brunella Fiamma Rodríguez Giorgio | José Luis Rodríguez Guardamino | Víctor Rodríguez Macedo | Marco Patricio Rodríguez Terry | Darío Rodríguez Uriol | Diana Roig Trelancia | Carlos Rojas Klauer | Diana Romero Rodríguez | Marcelo Roncal Pagador | Miguel Ángel Ronceros Neciosup | Carla Rossini Medina| Juan José Ruda Santolaria | Ángela Ruiz de Somocurcio Cornejo | Milo Ruiz Gonzales | Arturo Ruiz Ortiz | Ignacio Ruiz Valle | Jennifer Saavedra Sáenz | Silvia Ruiz Sandoval | Rosario Saco Oliva | María Gracia Sáenz González | Jhunelly Salazar Briceño | Rafael Salazar Gamarra | Sebastián Salazar Jeaunneau | Michel Salazar Tarazona | Alonso Salazar Zimmermann | Michelle Salcedo Teullet | José Antonio Salgado Silva | Liliana Salomé Resurrección | Marjorie Salvador Chávez | Rafael Sánchez Ríos | Mauricio Santa Cruz Vásquez | Jordi Sardá Paz | Rocío Saux Valdez | Luis Andrés Schrader Mindreau | Christian Schroeder Romero | Michel Seiner Pellny | Claudia Mariana Sequeiros Ugarte | María Teresa Serpa Santos | Karen Sheppard Castillo | Estefanía Shulca Romero | Hernando Domenack Sifuentes | Cynthya Siles Estabridis | Juliana Silva Cabrera | Kerli Solari Díaz | Gerardo Solís Vissher | Sebastián Soltau Salazar | Karla Soria Valeriano | Sara Sotelo Aguilar | Eduardo José Sotelo Castañeda | Martín Sotero Garzón | Gilda Spallarosa Lecca | Brenda Sparrow Alcázar | Patrick Stenning de Lavalle | Luis Stucchi Díaz | Óscar Súmar Albújar | Mitchel Sztrancman Torres | Claudia Sztuden Napadenschi | Deisy Taboada Huamán | Alejandro Tafur Coronel-Zegarra | Adriana del Pilar Tapia Quintanilla | Rossana Pilar Taquia Gutiérrez | Luciana Tataje Villalobos | Martín Tayro Cuba | Isabel Mabila Tello Carbajal | Jaime Thorne León | Edison Tito Peralta | Ludim Toledo Calla | Andrés Fernando Toledo Pérez | María del Pilar Torres | Romina Toso Altamirano | Augusto Townsend Klinge | Josefina Townsend Diez-Canseco | Daniela Tramontana Hinostroza | Carlos Fernando de Trazegnies Valdez | Jorge Trelles Castro-Mendívil | Óscar Trelles de Belaúnde | Gladis Triveño Chan Jan | Mariella Nathalia Trujillo Würtella | Manuel Ugarte Maggiolo | Camila Ugaz Heudebert | Jadhira Unda Valverde | Rafael Urbina Fletcher | Renato Urbina Santillán | Alejandra Uribe del Águila | Jessica Valdivia Amayo | Andrés Valdivia Montes | Fernanda Valdivia Rossel | Renato Martín Valdizán Cervantes | Eduardo Valdizán Sala | Agustín Valencia-Dongo Medina | Axel Valverde Pariasca | Carlos Valverde Reyes | Cristina van Zuiden Pancorvo | Erick E. Vargas Guevara | Luis Ernesto Vargas Loayza | Lucía Varillas Palacios | María Inés Vásquez Albán | Nelly Vásquez Jiménez | Delia Vásquez Llerena | Robinson Vásquez Montes | Katia Vásquez Reyes | Aracelly Vásquez Yrigoín | Miguel Vega Alvear | Nuria Vega Flores | Inés Vega Franco | Rodrigo Vega Méndez| Fernando Vega Sánchez | Jorge Vega Velasco | Claudia Velarde Arnáez | Jorge Velarde Arnáez | Sebastián Velarde Ferreyros | Luis Miguel Velarde Saffer | Pedro Mario Vera Ortiz | Bryan Vera Vargas | Cristina Verano Calero | Verónica Vergaray Béjar | Aaron Verona Badajoz | Inti Vidal Felip | Nancy Vidal Rodríguez | Ramón Vidurrizaga de Amézaga | Crisbeth Lorena Vigo Florián | Vanessa Villalobos Ylizarbe | Rosa Mariela Villalón Orellana | Alessandra Villanueva Aramayo | Micaela Villanueva Carreño | Diego Villanueva Contardo | Gonzalo Villanueva Llanos | Carmen María Villarán Ascenzo | Milagritos Villavicencio Pachas | Jimena Villegas Ingunza | Thalía Villegas Zorrilla | Joyce

Vivas Huaccho | María Teresa Vizcarra Alarcón | María José Vizcarra Pasapera | Percy Wilman Arriarán | Deborah Woll Castañeda | Christian Fernando Wong Vargas | Leonela Yauri Malpica | Rocío Yépez Minaya | Enzo Yturrizaga Aguirre | Rodrigo Zaldívar del Águila | Marco Ismael Zaldívar Chauca | Mayra Zambrano García | Cristian Zamora Dávila | Bruno Zanolo Maggiolo | Avecita del Carmen Zapata Cano | Verónica Zavala Lombardi | Ximena Zavala Lombardi | Sofía Zavala Quiroz | Eliana Zavala Uzuliaga | Gonzalo Alonso Zegarra Mulanovich | Juan Carlos Zegarra Vílchez | Joseline Zela Concha | Carlos Zelada Acuña | Grecia Zorrilla Garay | Gloria Zubizarreta Rondón | Fiorella Zúñiga Dede

MIEMBROS HONORARIOS DE THĒMIS

Giorgio Del Vecchio †| Felipe Osterling Parodi †| Jorge Avendaño Valdez †| César Landa Arroyo | Javier de Belaúnde López de Romaña | Carlos Fernández Sessarego †| Javier Neves Mujica †

AGRADECIMIENTOS

THĒMIS-Revista de Derecho agradece a todas las personas e instituciones que colaboraron con nosotros de distintas maneras, y sin cuyo apoyo, no hubiera sido posible la publicación de la presente edición; en particular a:

Juan Carlos Díaz Colchado, Andreé Castro Arequipeño, César Landa Arroyo, Omar Alvarado Escobar, Lidia Moreno Blesa, Antonio Robles Vargas, Jacqueline St. Laurent del Castillo, Ariel Hernán Vercelli, Juan Flaquer Riutort, Dana Masumura Ynami, Valeria Acosta Chia, María del Rosario Quiroga, Luis Fernando Roca, Carmen Ruíz Hidalgo, Mónica Siota Álvarez, Martín La Rosa Almenara, Tamara Rezqallah Arón, José Villafuerte Mendoza, José A. Jiménez Alemán, Pere Simon Castellano, Gonzalo Hierro Viétiez, Christian Valero Quispe, H. Andrés Izquierdo, María del Carmen Alvarado Bayo, Daniela Supo Calderón, Andrea Von Chrismar Medina, Benjamín Grebe Lira, Isabella Monsante Moy, Ariana Novoa Suárez, Alejandra Quintanilla Gutiérrez, Fiorella Senno Vassallo, José Miguel Porto, Cecilia Calderón Paredes, Iván Blume Moore, Lucía Aragüez Valenzuela, Raúl Feijóo Cambiaso.

Lima Airport Partners; Hugo Sologuren Calmet; Estudio Elías Puelles; Estudio Phillipi, Prietocarrizosa, Ferrero DU & Uría; Estudio Rodrigo Elías y Medrano; Rodríguez Angobaldo Abogados; Martinot Abogados.

Javier Pazos Hayashida, Ismael Canales Negrón y Mario Popuche Llontop.

De manera especial, THĒMIS-Revista de Derecho agradece a Liz Ana María Cachi Delgado, Ariana Valeria Chávez Cortez e Iñigo Carrión Marsano por haber colaborado en la producción de la presente edición.

THĒMIS-Revista de Derecho agradece de forma especial a los miembros que dedicaron parte de su vida universitaria al trabajo de nuestra institución y que se retiran junto con la presente edición; a ellos les deseamos siempre lo mejor:

Alessandra Camila Rocca Rodríguez, Alexia Gaitán Meléndez, Ana Calderón Torres, Ángel Sebastián Bravo Morales, Ariana Armacanqui Paredes, Claudia Mariana Sequeiros Ugarte, Cristina Gonzales Camarena, Denisse Paucar Laurencio, Fanny Herrera Cevasco, Hector Gianfranco Míñope Ferro, Henrry López Javier, Joaquín Alejandro Mejía Cacho, Johanna Mosqueira Gonzáles, Joyce Vivas Huaccho, Juan Alberto Liu Sánchez, Karla Soria Valeriano, Katherine Lisseth Ortiz Cornejo, Kathia Martínez Tarazona, Lucia López Gallardo, Luis Felipe Cornejo Arenas, Luz Caycho Cáceres, María José Erausquin Herrada, Melady Steffania Chávez Macuado, Rubiela Gaspar Clavo, Valeria Alejandra Murrieta Noly.

Normas para los autores para la publicación en THĒMIS

1. THĒMIS-Revista de Derecho considerará para su publicación artículos originales, no publicados en cualquier otro medio nacional o internacional. Los artículos deberán versar sobre temas de contenido jurídico o relacionado con el mundo del Derecho.

2. Los artículos presentados serán evaluados por el sistema de arbitraje por pares a doble ciego, el cual consiste en la evaluación de los artículos por dos árbitros con mayor grado académico que el autor. Asimismo, los árbitros son externos a la Revista y revisan los artículos de forma anónima. Las partes de la Revista que están sometidas a arbitraje por pares a doble ciego son el tema central y las misceláneas.

3. Todos los artículos contarán con una reseña tanto en español como en inglés, llamada gorrito o *abstract*, y que no deberá exceder los 800 caracteres.

4. El formato del artículo será Arial tamaño 11, con espaciado simple y sin sangría. Los subtítulos del artículo serán presentados en el mismo tipo de letra y tamaño y con sangría de 1 centímetro. Los pies de página se presentarán en el mismo tipo de letra, con tamaño 8 y con sangría de 0.5 centímetros. En todos los casos el texto debe estar justificado.

5. Todas las palabras en un idioma distinto del español deben ir en cursivas, salvo los nombres de personas, instituciones y obras.

6. Relieve: Si se pone alguna palabra de relieve, esta deberá ir en negrita.

7. Palabras clave: En español e inglés. Descripción del contenido del trabajo usando cinco palabras clave para su inclusión en los índices nacionales o internacionales. Se presentará al final de la reseña.

8. El formato de las referencias bibliográficas es el APA (American Psychological Association) sétima edición.

9. En la parte final del artículo se deberá incluir un apartado bibliográfico, siguiendo el siguiente orden:

   Referencias

   Colocar las referencias de autores siguiendo el formato APA (sétima edición) y para las referencias legales, The Bluebook: A Uniform System of Citation.

10. Todos los artículos deberán ser presentados con una carátula de acuerdo al modelo que se encuentra en la siguiente página.

11. La edición de todos los artículos será realizada por los miembros del Consejo Ejecutivo, según los criterios de edición de la Revista y bajo el formato de edición escalonada en tres ocasiones.

12. Los miembros, editores, autores, árbitros y demás colaboradores de THĒMIS-Revista de Derecho están sujetos a los Criterios de Ética de la Revista, disponibles vía *web*.

TÍTULO DEL ARTÍCULO

ARTICLE TITLE

Nombre y apellidos del autor*

Institución en la que el autor enseña o labora

En caso corresponda, vínculo del autor con THĒMIS (Miembro honorario, Miembro del Consejo Consultivo, exmiembro, exmiembro del Consejo Ejecutivo, exmiembro del Consejo Directivo o Exeditor General)

Short paragraph on the article, with the object to invite people to read it.

It must be two short paragraphs, in which further details on the article can be mentioned briefly, as well as the themes that the article will develop or the solutions that the author presents to determined issues.

KEYWORDS: Five keywords that allow people to find the article by the themes developed. For instance: Administrative Law; Tax Law; Civil Law; Civil Code; public employment.

Breve reseña sobre el artículo, que invite al público a leerlo.

Deben ser dos párrafos breves, en los que se pueden enunciar algunos breves detalles del artículo y de los temas que éste tratará, o las soluciones que propondrá el autor a determinados problemas.

PALABRAS CLAVE: Cinco palabras clave que permitan al público llegar al artículo por los temas que trata. Por ejemplo: Derecho Administrativo; Derecho Tributario; Derecho Civil; Código Civil; empleo público.

---

* Abogado (u otra profesión ejercida, siempre sin especificación de la institución en la que se obtuvo el título). Grado académico y universidad en la que se obtuvo. Cargos que ha llevado a cabo en el pasado (opcional). Indicar si es profesor y en qué universidad imparte clases. Membresías. Cargo ejercido en la institución en la que se desenvuelve profesionalmente. Contacto: correo del autor para fines académicos.

Nota del Editor: Fecha en que el autor envió la versión final del articulo y fecha en la que el Consejo Ejecutivo de THĒMIS-Revista de Derecho lo aceptó.

THĒMIS-REVISTA DE DERECHO 80

La siguiente edición de THĒMIS-Revista de Derecho tendrá como eje central **Derecho, Políticas Públicas y COVID-19.**

PARTICIPACIÓN EN THĒMIS-REVISTA DE DERECHO

THĒMIS-Revista de Derecho se encuentra en constante convocatoria abierta para recepción de artículos relativos al tema central que el Consejo Ejecutivo elija, o a cualquier otro tema relacionado a la disciplina del Derecho.

Todos los interesados en colaborar con **THĒMIS-Revista de Derecho** mediante sugerencias, comentarios o la publicación de artículos, pueden enviar un correo electrónico a **themisconsejoeditorial@gmail.com**.

THĒMIS-Revista de Derecho agradece todo envío sin comprometerse a su publicación.