

REVISTA DE DERECHO ADMINISTRATIVO N°20

CÍRCULO DE DERECHO ADMINISTRATIVO

Alejandro Huergo – Diego Zegarra – Edgar González – Eduardo Gamero – Felipe Rotondo – Gloriana Alvarado – Gonzalo Ruíz – José Aguilar – José Vida – Laura González – Luis Ortiz – Luz Herrera – Rubén Martínez – Sandra Ortiz – Virginia Nakagawa



Círculo de Derecho
Administrativo



Círculo de Derecho Administrativo

Revista de Derecho Administrativo N° 20

La Revista de Derecho Administrativo (RDA) es editada por la Comisión de Publicaciones del Círculo de Derecho Administrativo - CDA. Es la primera revista especializada en Derecho Administrativo del Perú, sus números de publicación semestral han alcanzado amplio reconocimiento por parte de los más destacados especialistas en la materia; en virtud del quehacer académico en el que alumnos y profesores aportan con la difusión del Derecho Administrativo. A la fecha, han sido publicados 20 números de la RDA, cada una con una temática especializada en las distintas ramas del Derecho Administrativo. Desde el número 18, todo artículo de la sección Doctrina es objeto, al menos, de dos revisiones por pares a doble ciego.

La versión digital de la revista está disponible en <http://revistas.pucp.edu.pe/index.php/derechoadministrativo>

Editorial: Asociación Civil Revista de Derecho Administrativo - CDA

Facultad de Derecho de la Pontificia Universidad Católica del Perú, Segundo piso
Av. Universitaria 1801, San Miguel – Lima, Perú.

Teléfono: 626-2000 Anexo 5625
publicaciones@cda.org.pe
<http://prometheo.pe/>

Diagramación:
Rubí Victtoria Alburqueque Palma

Impresión: Corporación Yachay S.A.C.
Tiraje: 150 ejemplares

Publicado en noviembre 2021. Lima – Perú.

Hecho el Depósito Legal en la Biblioteca Nacional del Perú N° 2019-12741
ISSN: 2074-0956
eISSN: 2708-9886

Derechos Reservados: Decreto Legislativo N° 822
Prohibida la reproducción de este libro por cualquier medio, total o parcialmente, sin permiso expreso de la Asociación Civil Revista de Derecho Administrativo CDA.

El contenido de los artículos publicados en la RDA es responsabilidad exclusiva de los autores.
Cada artículo puede ser referenciado como:

Nombre del autor. (2021). Título del artículo. *Revista de Derecho Administrativo – CDA*, 20, pp. inicio-fin.



Consejo Editorial

Cortés Campos, Josefina (Instituto Tecnológico y de Estudios Superiores de Monterrey)

De la Cruz Ferrer, Juan (Universidad Complutense de Madrid)

Díaz Bravo, Enrique (Universidad Santo Tomás)

Hernández-Mendible, Víctor (Universidad Monteávila)

Huergo Lora, Alejandro (Universidad de Oviedo)

Mondéjar Jiménez, José (Universidad Castilla-La Mancha)

Moreno Molina, José Antonio (Universidad Castilla-La Mancha)

Radovic Córdova, Marcela (Universidad de Chile)

Razquin Lizarraga, Martín María (Universidad Pública de Navarra)

Rivero Ortega, Ricardo (Universidad de Salamanca)

Consejo Consultivo

Baca Oneto, Víctor Sebastián (Universidad de Piura)

Boyer Carrera, Janeyri Elizabeth (Pontificia Universidad Católica del Perú)

Cairampoma Arroyo, Vicente Alberto (Pontificia Universidad Católica del Perú)

Danós Ordóñez, Jorge Elías (Pontificia Universidad Católica del Perú)

Huapaya Tapia, Ramón Alberto (Pontificia Universidad Católica del Perú)

Morón Urbina, Juan Carlos (Pontificia Universidad Católica del Perú)

Sánchez Povis, Lucio (Pontificia Universidad Católica del Perú)

Zegarra Valdivia, Diego Hernando (Pontificia Universidad Católica del Perú)

Zúñiga Fernández, Tania (Pontificia Universidad Católica del Perú)

Coordinador Académico

Diego Hernando Zegarra Valdivia
(Pontificia Universidad Católica del Perú)

Editores Generales

Angélica Mireli Angulo Remuzgo
(Alumna, Pontificia Universidad Católica del Perú)

Ronny André Cuba Montesinos
(Alumno, Pontificia Universidad Católica del Perú)

Consejo Ejecutivo

Ana Lucía Franca Angulo Santos
(Alumna, Pontificia Universidad Católica del Perú)

Anggie Melissa Amaro Zulueta
(Alumna, Pontificia Universidad Católica del Perú)

Claudia Elena Sotomayor Dorival
(Alumna, Pontificia Universidad Católica del Perú)

Gabriela De Los Ángeles Flores Gonzales
(Alumna, Pontificia Universidad Católica del Perú)

Joaquín Patricio Espinoza Escobar
(Alumno, Pontificia Universidad Católica del Perú)

Renzo Augusto Zarate Villantoy
(Alumno, Pontificia Universidad Católica del Perú)

Valeria Prieto La Noire
(Alumna, Pontificia Universidad Católica del Perú)

Valeria Vilcarromero Figueroa
(Alumna, Pontificia Universidad Católica del Perú)

ASAMBLEA 2021 – 1

Consejo Directivo

Ruiz Quispe, Diana Elsa
Directora Ejecutiva

Pahuacho Camarena, Milagros
Directora de Investigación y Actualidad Jurídica

Supo Gavancho, Luis Roberto
Director de Eventos Académicos

Cuba Montesinos, Ronny André
Director de Publicaciones

Atencio Cuadros, Camila Alejandra
Directora de Imagen y Recursos Humanos

Ticlia Huerta, Fiorella Isabel
Directora de Economía y Contabilidad

Comisión de Publicaciones

Angulo Remuzgo, Angélica Mireli

Espinoza Escobar, Joaquín Patricio

Chirinos Liñán, Grecia Nira

Cuba Montesinos, Ronny André

Angulo Santos, Ana Lucía Franca

Amaro Zulueta, Anggie Melissa

Ruiz Moreno, Piero Alexander

Flores González, Gabriela De Los Ángeles

Sotomayor Dorival, Claudia Elena

Comisión de Investigación y Actualidad Jurídica

Gastañeta Bastidas, Adria

Villanueva Cáceres, Gabriela

Martínez Pacheco, Diego

Villafranca Florián, Cristina María

Solís De La Cruz, Valeria Victoria

Pahuacho Camarena, Milagros

Ibarra Serván, Nadia

Maita Uria, Dionel

Comisión de Economía y Financiamiento

Benvenutto Millones, Víctor Andrés

García Araujo, Nátaly

Ticlia Huerta, Fiorella Isabel

Tena Mucha, Marely Luceta

Gamarra Aliaga, Nicole Adriana

Llatas Sánchez, Anghela Fiorela

Zúñiga Domínguez, Leslie Caroline

Comisión de Eventos y Cursos Académicos

Clemente Inga, Brenda Camila

Ramírez Camaná, Valeria Liz

Lapoint Castillo, Andrea

Nolasco Sánchez, Lei-ly Angell Valery

Pereyra Pachas, Allison

Rivas Sú, Leonardo Alfredo

Supo Gavancho, Luis Roberto

Bulnes Lliuya, Justo Alexis

Castillo Santillana, Nicol Brigit

Comisión de Recursos Humanos

Atencio Cuadros, Camila

Delta Matrou, Francisco Alonso

Ramos Maldonado, Jacqueline

Morán Cervantes, María Claudia

Ricapa Yaipén, Karla Zenaida

Revoredo Loayza, Diana Valeria

ASAMBLEA 2021 – 2

Consejo Directivo

Pahuacho Camarena, Milagros
Directora Ejecutiva

Angulo Santos, Ana Lucía Franca
Directora de Publicaciones

Maita Uriá, Dionel
**Director de Investigación y
Actualidad Jurídica**

Ricapa Yaipén, Karla Zenaida
**Directora de Imagen y Recursos
Humanos**

Nolasco Sánchez, Lei-ly Angell Valery
Directora de Eventos Académicos

Gamarra Aliaga, Nicole Adriana
**Directora de Economía y
Contabilidad**

Comisión de Publicaciones

Angulo Remuzgo, Angélica Mireli

Espinoza Escobar, Joaquín Patricio

Angulo Santos, Ana Lucía Franca

Amaro Zulueta, Anggie Melissa

Sotomayor Dorival, Claudia Elena

Flores González, Gabriela De Los Ángeles

Vilcarromero Figueroa, Valeria

Prieto La Noire, Valeria

Zarate Villantoy, Renzo Augusto

Comisión de Investigación y Actualidad Jurídica

Gastañeta Bastidas, Adria

Palomino Díaz, Xenia

Solís De La Cruz, Valeria Victoria

Santiago Rimari, Rosa

Maita Uria, Dionel

Quispe Vera, Erick

Comisión de Economía y Financiamiento

Gamarra Aliaga, Nicole Adriana

García Araujo, Nátaly

Zúñiga Domínguez, Leslie Caroline

Abarca Cusimayta, Almendra

Huaroc Huallanca, Ingrid Jazmín

Comisión de Eventos y Cursos Académicos

Supo Gavancho, Luis Roberto

Ramírez Camaná, Valeria Liz

Castillo Santillana, Nicol Brigit

Nolasco Sánchez, Lei-ly Angell Valery

Manrique Kukurelo, Diana Lucía

Rivas Sú, Leonardo Alfredo

Chaca Tauma, César

Moscoso Enriquez, Robin Alonso

Comisión de Recursos Humanos

Atencio Cuadros, Camila

Revoredo Loayza, Diana Valeria

Ramos Maldonado, Jacqueline

Huayta Ríos, Ariane

Ricapa Yaipén, Karla Zenaida

Requena Vidal, Fabiola

Verástegui Payehuanca, Lucero

PARES REVISORES

Dedicamos esta sección para expresar nuestros mayores agradecimientos a los(as) especialistas que gentilmente apoyaron como árbitros(as) académicos(as) en el proceso de revisión a doble ciego. Así, con benemérito rigor, contribuyeron en la selección de artículos publicables. A continuación, la lista de pares revisores que participaron en el número 20 de la Revista de Derecho Administrativo:

- | | |
|----------------------------------|--|
| 1. Arellano Toledo, Wilma | 10. González Pons, Elisabet |
| 2. Arenas Ramiro, Mónica | 11. Luna Cervantes, Eduardo Javier |
| 3. Ávila Rodríguez, Carmen María | 12. Maldonado Meléndez, Mirko André |
| 4. Barrero Rodríguez, Concepción | 13. Montero Pascual, Juan José |
| 5. Calle D'Aleman, Sol Beatriz | 14. Pedraza Córdoba, Juanita Del Pilar |
| 6. Capdeferro Villagrasa, Óscar | 15. Sanz Larruga, Francisco Javier |
| 7. Cortés Campos, Josefina | 16. Sarasíbar Iriarte, Miren |
| 8. Cubero Marcos, José Ignacio | 17. Schiavi Muñoz, Pablo |
| 9. Gómez-Ferrer Rincón, Rafael | 18. Tassano Velaochaga, Hebert Eduardo |



PRÓLOGO

Prologar la vigésima edición de la Revista de Derecho Administrativo (RDA), constituye una satisfacción personal porque soy testigo del crecimiento del Círculo de Derecho Administrativo de la Pontificia Universidad Católica del Perú, desde que lo inicié en 1999 como un grupo de estudio y que luego, bajo el impulso de los estudiantes, tornó en una asociación, cuya actividad académica ha sido muy importante para difundir, en el ámbito universitario y profesional peruano, el Derecho Administrativo a través de seminarios, conversatorios y, de la edición de una revista, cuya primera entrega vio la luz el año 2006.

En estos 15 años que lleva de andadura, la RDA ha evolucionado no sólo en su temática, la misma que ha recogido una orientación preponderantemente monográfica, sino que además ha entrado en un riguroso, pero necesario proceso de indexación, con el objetivo de ser listada como una publicación periódica de investigación de alta calidad en repertorios de consulta global en el ámbito jurídico. La presente edición no ha estado exenta de cumplir con los requisitos de una publicación de esta naturaleza, por lo que, luego de recibir colaboraciones originales, procedió a su arbitraje por un doble par ciego a través de revisores, aspecto este último que constituye una garantía para el alcance de los artículos que incorpora esta edición de la revista.

La temática que las colaboraciones han seguido, se ha situado en el ámbito de las telecomunicaciones, la protección de datos personales y las TICs y el Derecho Administrativo, en los que, por la impronta de la pandemia del COVID-19, se han generado cuestionamientos y desafíos y se han planteado desarrollos urgentes, los que han sido abordados desde una perspectiva académica en la casi totalidad de los trabajos.

En el grupo de artículos que abordan la temática de las telecomunicaciones, la Profesora Sandra Milena Ortiz Laverde realiza un desarrollo de la experiencias de la Unión Europea, colombiana y peruana de los mecanismos de acceso, destacando – en sus palabras - la importancia que tiene contar con un modelo de Habilitación General para la prestación de los servicios y la instalación o explotación de redes de telecomunicaciones, como un mecanismo efectivo para lograr la participación de nuevos agentes en este mercado y, proyectando cómo el modelo vigente en el Perú puede modificarse de cara a las transformaciones que ha tenido el sector y la necesidad de eliminación de las barreras de entrada asociadas con las concesiones y demás títulos habilitantes que no permiten el ingreso de nuevos agentes. De este importante estudio comparado, nos situamos luego en la colaboración del Profesor Luis Ortiz Zamora y de Gloriana Alvarado León, en el que se pasa revista del proceso de apertura del sector de las telecomunicaciones en Costa Rica y de cuáles han sido las piedras angulares del cambio de paradigma de monopolio a mercado en competencia, a saber: la convergencia y la neutralidad tecnológica, el papel del regulador, el servicio universal y el régimen de acceso e interconexión; para luego realizar un balance de los 10 años transcurridos en el mercado de las telecomunicaciones costarricense, respecto del cual concluyen que la regulación para la competencia debe ser profunda, incisiva y constante para “evitar (...) seguir viviendo en un sistema creyendo estar en otro”.

A las dos colaboraciones que hemos reseñado se suma la de Virginia Nakagawa Morales y José Aguilar Reátegui, autores que, desde una perspectiva de política regulatoria, promueven la configuración de un Sandbox Regulatorio que haga posible, a los distintos actores del sector telecomunicaciones, generar propuestas innovadoras que permitan

ofrecer nuevos servicios, bajo una “burbuja regulatoria” que genere predictibilidad y permita presentar casos de negocio en un marco de confianza y colaboración público-privada. Es parte de esta sección el trabajo de las Profesoras Luz Mónica Herrera Zapata y Laura Daniela González Rozo, quienes abordan desde la experiencia y el marco normativo colombiano la temática del acceso y el servicio universal como herramientas para lograr la inclusión digital de la población, partiendo de la constatación de la existencia de una brecha digital que limita a la población de la posibilidad de beneficiarse de las tecnologías de la información y las comunicaciones vulnerándose por ello sus derechos fundamentales. En su estudio, incluyen referencias comparadas de la situación del Perú, con respecto a las prácticas que se han implementado con el objetivo de garantizar el servicio universal y la calidad del mismo; formulan también recomendaciones para que se evalúen periódicamente la eficiencia, eficacia e impacto de los planes, programas y proyectos orientados a cerrar la brecha digital.

Desde una perspectiva económica, cierra la temática de las telecomunicaciones el trabajo del Profesor Gonzalo Ruiz, en el que realiza un análisis de la autonomía del organismo regulador de las telecomunicaciones en el Perú (OSIPTEL), en la base de metodologías proyectadas sobre la autonomía formal y respecto de la autonomía “de facto” que en este último supuesto lo llevan a concluir que los niveles de autonomía son inferiores comparados con los obtenidos en el caso de autonomía formal debido principalmente a la influencia del Poder Ejecutivo en las decisiones de carácter presupuestal y organizacional del regulador.

En la sección que esta entrega dedica a la protección de datos personales, se ubica un trabajo de mi autoría en el que se analiza, en el marco de la vigente normativa de protección de datos, algunos de los supuestos en que el uso variado de tecnologías por parte del Estado y las empresas para hacer frente a la propagación de la pandemia del COVID-19 y proteger la salud de las personas, ha impactado en el derecho fundamental a la protección de datos personales. Sobre esta base, se identifican, a partir del análisis de las bases de legitimación del tratamiento de datos de salud o de geolocalización de las personas, aquellos aspectos necesarios para reforzar la garantía del derecho fundamental a la protección de datos frente a los riesgos y afectaciones que genera el uso de herramientas tecnológicas en los ámbitos que han sido implementadas (información y diagnóstico del virus, geolocalización y seguimiento de contagios y medición masiva de temperatura en espacios públicos).

La actualidad de la aplicación de los algoritmos en el ámbito jurídico es la materia estudiada por el Profesor Alejandro Huergo Lora. El trabajo aborda las principales concepciones del término algoritmo, explicando su relación con las predicciones basadas en datos y con los conceptos de inteligencia artificial, digitalización y automatización, así como sus principales características y diferencias. Asimismo, se analiza la aplicación de la inteligencia artificial en la creación y aplicación del Derecho y la injerencia de la regulación de datos personales en la utilización de algoritmos y el rol de la Administración Pública. Completa esta segunda sección el trabajo del Profesor Felipe Rotondo en el que analiza la incidencia del uso de las TIC en Derecho administrativo y su vinculación con el uso de datos masivos (big data) y respecto del derecho a la protección de datos personales. De esta forma, considera la importancia de un uso responsable que involucre dimensiones de índole ética, jurídica, técnica y social que permitan una transformación digital que habilite, legítimamente a las necesidades de las personas y prevenir situaciones problemáticas.

El estudio de los elementos para la configuración de las denominada Administración Digital, es la temática que aborda el trabajo del Profesor Rubén Martínez Gutiérrez en la tercera sección de esta vigésima entrega de la Revista de Derecho Administrativo. El punto de partida del autor es el de afirmar que la transformación digital de las Administraciones Públicas requiere de sólidas bases conceptuales y normativas, por lo que profundiza en aquellas cuestiones que considera como estructurales en modelo de e-Administración: los principios de interoperabilidad y seguridad; instrumentos como la sede electrónica, registros, gestión documental electrónica e identificación y firma. Incorpora además una propuesta de modelo de regulación legal en el que no sólo identifica las características del modelo de e-Administración español y del procedimiento administrativo electrónico, sino que realiza una caracterización general de la regulación adoptada por el legislador peruano a través de la Ley de Gobierno Digital y de su reciente reglamentación.

Los derechos digitales fundamentales o derechos de la sociedad digital son la materia de estudio del trabajo del Profesor Edgard González López, a través del cual, se plantea dilucidar si los mismos requieren de una protección distinta a la que ordinariamente se les otorga, para ello, analiza la relación entre los derechos humanos y el internet, la dimensión de este último como servicio de interés general o de servicio público y las discusiones sobre la libertad absoluta o su regulación; y, evalúa si es necesaria la configuración de los derechos digitales en el ordenamiento constitucional o legal, por tratarse de nuevos derechos o nuevas reconfiguraciones de los existentes.

Es parte de esta sección, el trabajo del Profesor Eduardo Gamero Casado, en el que analiza desde un enfoque del derecho de la Unión Europea, el desarrollo de los sistemas de inteligencia artificial (IA) y las expectativas económicas y sociales que el mismo plantea, por las sensibles mejoras de prestaciones y servicios tanto en el sector público como en el privado y por los grandes dilemas éticos y jurídicos. El autor, luego de revisar las bases del enfoque europeo de la IA, realiza una caracterización jurídica del modelo normativo europeo que se pretende proyectar sobre la IA de manera que considera que el mismo promueve la seguridad jurídica, tiene su base en los valores europeos y preserva los derechos fundamentales, efectúa una valoración del mismo, considerando que puede suponer una desventaja competitiva frente a otros lugares del mundo en el que no existan limitaciones y cargas regulatorias.

Cierra esta edición, un trabajo no menos importante, como lo es la colaboración del Profesor José Vida Fernández, en el que aborda el impacto que ha generado en la tradicional delimitación del entorno digital en sectores de referencia como son las telecomunicaciones, el audiovisual y los servicios de la sociedad de la información, la aparición de innumerables servicios prestados a través del internet (servicios over the top - OTT) que ofrecen funcionalidades propias de estos servicios pero que no encajan en su definición, por lo que están excluidos de la aplicación de su régimen jurídico. El autor analiza, a partir de ello, la alteración del equilibrio de los citados sectores originada por los denominados servicios OTT, así como las medidas que la Unión Europea ha implementado para incluirlos en el régimen correspondiente, someterlos a obligaciones y garantizar sean alcanzados objetivos de interés público.

La reseña de las colaboraciones de esta vigésima edición, nos han permitido no sólo introducir al lector de esta entrega sobre el contenido de las mismas, sino también formular una valoración respecto al importante aporte académico de todos y cada uno de los trabajos que forman parte de la misma, tanto por la rigurosidad y originalidad, como por la actualidad de la temática tratada por sus autores, aspectos estos últimos

que permiten caracterizar a esta edición de la RDA como una publicación periódica de investigación de alta calidad. Corresponde por tanto seguir promoviendo y respaldando la actividad académica del Círculo de Derecho Administrativo por la contribución que a través de la misma se realiza a la investigación en esta área de conocimiento.

Diego Zegarra Valdivia PhD
Profesor Principal de Derecho Administrativo
Pontificia Universidad Católica del Perú

ÍNDICE

Revista de Derecho Administrativo N° 20 – CDA

Telecomunicaciones, Datos Personales y Tecnologías de la Información

Prólogo

Diego Zegarra Valdivia

TELECOMUNICACIONES

1. Acceso al mercado de las telecomunicaciones y ejercicio de la actividad. Revisión de la experiencia de la unión europea y española y su incidencia en las legislaciones colombiana y peruana 16
Sandra Milena Ortiz Laverde
2. Regulación para la competencia en el mercado de las telecomunicaciones en Costa Rica. Un cambio de paradigma 46
Luis A. Ortiz Zamora y Gloriana Alvarado León
3. De los sandbox regulatorios y otros medios (demonios) de crecer el acceso a internet en Perú. 68
Virginia Nakagawa Morales y José Aguilar Reátegui
4. La universalidad hacia las TIC en Colombia 94
Luz Mónica Herrera Zapata y Laura Daniela González Rozo
5. La autonomía de facto del regulador de las telecomunicaciones 118
Gonzalo Ruiz Díaz

DATOS PERSONALES

6. El uso de herramientas tecnológicas en la lucha contra el COVID-19 y sus implicancias en el derecho fundamental a la protección de datos personales: una aproximación 142
Diego Zegarra Valdivia
7. El uso de algoritmos y su impacto en los datos personales 166
Alejandro Huergo Lora
8. Derecho Administrativo, big data y protección de datos personales 194
Felipe Rotondo Tornaría

TICs Y DERECHO ADMINISTRATIVO

9. Elementos para la configuración de la administración digital 212
Rubén Martínez Gutiérrez

10. Los derechos digitales fundamentales: ¿es necesaria su reconfiguración en el ordenamiento jurídico? 234
Edgar González López
11. El enfoque europeo de Inteligencia Artificial 268
Eduardo Gamero Casado
12. La articulación jurídica del entorno digital: insuficiencias y soluciones en la delimitación de los sectores de referencia ante el desafío de los servicios over the top (OIT). 290
José Vida Fernández



ACCESO AL MERCADO DE LAS TELECOMUNICACIONES Y EJERCICIO DE LA ACTIVIDAD REVISIÓN DE LA EXPERIENCIA DE LA UNIÓN EUROPEA Y ESPAÑOLA Y SU INCIDENCIA EN LAS LEGISLACIONES COLOMBIANA Y PERUANA

ACCESS TO THE TELECOMMUNICATIONS MARKET AND EXERCISE OF THE ACTIVITY REVIEW OF THE EXPERIENCE OF THE EUROPEAN AND SPANISH UNION AND ITS IMPACT ON COLOMBIAN AND PERUVIAN LEGISLATION

SANDRA MILENA ORTIZ LAVERDE¹

RESUMEN

La transformación que en los últimos años ha sufrido el sector de las telecomunicaciones, asociado con la posibilidad de contar con un número amplio de operadores encargados de la prestación de los servicios de comunicaciones y que la competencia sea un factor determinante para la satisfacción de los intereses colectivos, son las piedras angulares sobre las cuales se ha edificado la legislación tanto Comunitaria, española, colombiana y peruana, donde se ha considerado que la liberalización de los servicios de telecomunicaciones debe estar dotada de una serie de principios y de garantías asociadas con la libertad de concurrencia y que las barreras de ingreso previstas para los operadores se limitaran y flexibilizaran, con el fin de poder dar respuesta a los vertiginosos cambios derivados de la convergencia tecnológica.

El objetivo de este pequeña disertación académica es analizar el por qué desde el contexto comunitario desde el año 1997, se consideró necesaria la eliminación de los permisos para la prestación de los servicios de comunicaciones, trayendo consigo la modificación del modelo vigente en materia de concesiones y permisos, a un

ABSTRACT

The transformation that the telecommunications sector has undergone in recent years, associated with the possibility of having a large number of operators in charge of providing communications services and that competition is a determining factor for the satisfaction of collective interests, are the cornerstones on which the Community, Spanish, Colombian and Peruvian legislation has been built, where it has been considered that the liberalization of telecommunications services should be endowed with a series of principles and guarantees associated with the freedom of competition is guaranteed and that the entry barriers destined for the operators will be limited and made more flexible, in order to be able to respond to the vertiginous changes derived from the technological convergence.

The objective of this short academic dissertation is to analyze why from the community context since 1997, the elimination of permits for the provision of communications services was considered necessary, bringing with it the modification of the current model in terms of concessions and permits, to a model of General Authorizations or

1 Abogada de la Universidad Externado de Colombia. Especialista en Regulación y Gestión de las Telecomunicaciones y Nuevas Tecnologías de la misma Universidad. Magister en Arts Derecho, Economía y Políticas Públicas del Instituto Universitario de Investigación Ortega y Gasset adscrito a la Universidad Complutense de Madrid. Máster en Derecho Público, especialidad Derecho Administrativo de la Universidad Complutense de Madrid. Doctora en Derecho por la Universidad Complutense de Madrid. Docente investigadora del Departamento de Derecho de las Telecomunicaciones. Correo electrónico: Sandra.ortiz@uexternado.edu.co

modelo de Habilitaciones o Autorizaciones generales, en consideración a la existencia de un único mercado, el mercado de las comunicaciones electrónicas y donde era conveniente recurrir a otras formas de ingreso al mercado y que fuera este el que determinará su permanencia o no.

Este nuevo modelo de autorización que fue transpuesto por parte del legislador español, conforme a la evolución del modelo previsto en el paquete de Directivas expedidas por el Consejo y Parlamento Europeo en el 2002, no fue ajeno a Colombia, y es así como en el proceso de construcción de la Ley para el sector TIC, la figura de habilitación general fue incorporada, teniendo como referente la legislación española, ampliando esta figura al sector de la televisión en la reforma del año 2019, atendiendo al modelo convergente que trajo consigo la nueva Ley, de allí la conveniencia de contar con este modelo para el ingreso al mercado TIC y Audiovisual.

La finalidad del artículo es determinar cuál es la importancia que tiene contar con un modelo de Habilitación General para la prestación de los servicios y la instalación o explotación de redes de telecomunicaciones, como un mecanismo efectivo para lograr la participación de nuevos agentes en este mercado y como el modelo vigente en Perú puede modificarse de cara las transformaciones que ha tenido el sector y la necesidad de eliminación de las barreras de entrada asociadas con la concesiones y demás títulos habilitantes que no permiten el ingreso de nuevos agentes a este sector.

PALABRAS CLAVE

Competencia | Habilitación General | Licencias | Concesión | Registro de Operadores

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 6 de mayo de 2021 y aprobado para su publicación el 16 de agosto de 2021.

Authorizations, in consideration of the existence of a single market, that of the electronic communications market and where it was convenient to resort to other forms of income so that agents could enter the market and that this was the that will determine its permanence or not.

This new authorization model, which was transposed by the Spanish legislator, and in accordance with the evolution of the model provided for in the package of Directives issued by the Council and European Parliament in 2002, was not alien to Colombia, and this is how the In the process of construction of the Law for the ICT sector, the figure of general authorization was incorporated, taking Spanish legislation as a reference, expanding this framework and in the most recent reform this figure was extended to the television sector in the reform of the year 2019, taking into account the convergent model that the new Law brought with it, hence the convenience of having this model for entering the ICT and Audiovisual market.

The purpose of the article is to determine the importance of having a General Qualification model for the provision of services and the installation or operation of telecommunications networks, as an effective mechanism to achieve the participation of new agents in this market and As the current model in Peru, it can be modified in the face of the transformations that the sector has undergone and the need to eliminate entry barriers associated with concessions and other enabling titles that do not allow the entry of new agents into this sector.

KEYWORDS

Competition | General Qualification | Licenses | Concession | Operators Registry

CONTENIDO

Introducción; **1.** Antecedentes. **1.1.** Unión europea. **1.2.** España. **1.3.** Colombia; **2.** Habilitación General en Colombia. Ley 1341 de 2009; **3.** Habilitación General de 1978 de 2019; **4.** La conveniencia para el modelo peruano; **5.** Conclusiones.

INTRODUCCIÓN

La transformación del modelo de los títulos habilitantes previstos para la prestación de los servicios de telecomunicaciones, responde a la misma evolución misma del sector y como desde la concepción que se tuvo que el modelo de prestación del servicio por parte de un solo agente, cambiara por un modelo donde la regulación y la prestación del servicio se hicieran de manera independiente y donde la competencia se configuraba en un elemento fundamental para la consecución de este objetivo. Bajo estas premisas, se estableció una separación entre los servicios de telecomunicaciones trayendo consigo un sistema de clasificación y de separación entre redes y servicios básicos y otras redes, equipamientos y servicios, que se vieron reflejados en distintas legislaciones, que recogieron estos mandatos, conservando en un primer momento, los modelos de exclusividad, para posteriormente, generar un modelo regulatorio basado en la competencia y de nuevas reglas para el ingreso al mercado para la prestación de los servicios de telecomunicaciones.

La concepción Europea de concebir un marco común en materia de autorizaciones generales y licencias individuales en el ámbito de los servicios de telecomunicaciones, tal como fue concebido en la Directiva 97/13/CE del Parlamento Europeo y del Consejo de 10 de abril de 1997 y que se perfecciona en la Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización), reflejan la evolución del modelo diseñado de la liberalización y a las dinámicas propias de la competencia como el mecanismo más óptimo para garantizar el acceso de nuevos agentes, eliminando la principal barrera que eran las concesiones y permisos como forma de acceso al mercado y ejercicio de la actividad.

Es por estas razones, que esta experiencia es fundamental para analizar el modelo previsto en el ordenamiento colombiano, que desde el año 2009 a través de la Ley 1341 de 2009 y se ratifica y extiende al sector de televisión a través de la Ley 1978 de 2019, donde se liberalizan los servicios de telecomunicaciones, con la particularidad que continuar siendo actividades sujetas que control y vigilancia por parte del Estado, como un mecanismo óptimo para garantizar la competencia en un modelo convergente. En lo que respecta al uso del espectro radioeléctrico para aquellos servicios que lo requerían, atendiendo al modelo diseñado tanto en la legislación europea como española, y que fue incorporada en la legislación colombiana, el nuevo marco de habilitación incorpora un nuevo conjunto de reglas específicas respecto al procedimiento para el uso de este recurso.

La finalidad del artículo, es analizar diversas experiencias y cuál podría ser su incidencia en un proceso pleno de liberalización en Perú y como este puede contribuir a que el mercado evolucione, cuente con nuevos agentes en el mercado, y de esta manera se pueda garantizar el acceso a las comunicaciones a los usuarios y satisfacer el interés general.

Ahora bien, el artículo, se articula en cuatro partes a saber, la primera de ellas en la que se revisan los antecedentes desde el contexto de la Unión Europea, su transposición a la legislación española, a través de sus tres leyes de comunicaciones, la proferida en el

año 1997 donde hay una aproximación a la figura, la del 2003, donde se parte de los avances dados en la legislación del año 1997 y como la Directiva de Autorización inciden en el modelo, la cual es ratificada la Ley 3 de 2014, donde se el modelo concebido en sede comunitaria tiene plena vigencia para España, para posteriormente, y teniendo como referente estos dos modelos revisar la experiencia de Colombia, quien adopta un modelo de Habilitación General previsto dentro del conjunto de disposiciones contenidas en la primera Ley que regulaba el sector de las telecomunicaciones de manera íntegra como es la Ley 1341 de 2019, lo que permitirá analizar el modelo de habilitaciones diseñados en las dos leyes que rigen al sector TIC desde el año 2009 y 2019 y como este modelo puede ser replicado en la legislación peruana donde se ha definido a las telecomunicaciones como actividades económicas de interés general, como la introducción de un mecanismo de esta naturaleza permitirá entrar en una nueva etapa del proceso de liberalización plena del sector de las telecomunicaciones y estar a la vanguardia de los modelos regulatorios, inspirados en el modelo europeo.

1. ANTECEDENTES.

Tal como se indicó previamente, el proceso de liberalización adelantado en la Unión Europea a finales de la década de los años ochenta y teniendo su punto más importante en la década de los años noventas, trajo consigo una transformación respecto a las formas como se prestaban los servicios públicos y por consiguiente la apertura parcial y posteriormente plena al sector privado de actividades, productos o recursos que anteriormente se encontraban reservados a la Administración, de allí que los permisos y concesiones, fueran revisados con el fin de poder cumplimiento al plan de liberalización que fue diseñado para lograr una verdaderamente descualificación general de una actividad o servicio, en nuestro caso concreto para el sector de las telecomunicaciones o como se ha denominado en contexto comunitarios de las comunicaciones electrónicas (Saura Fructuoso, 2015).

Esta nueva concepción, trajo consigo que el legislador europeo con el fin de lograr no sola la libertad de concurrencia y la incorporación de nuevo operadores, sino de la visión marco de crear y consolidar un mercado único europeo, trajo consigo la necesidad de modificar la forma como los operadores podrían ingresar al mercado, de allí que fuera conveniente revisar el modelo tanto de concesiones y de permisos previstos en las legislaciones nacionales, para crear un modelo de autorización general para que la prestación de los servicios de comunicaciones, de allí, que sea conveniente revisar las dos Directivas expedidas sobre las autorizaciones y permisos para la prestación de los servicios de comunicaciones, la primera proferida en el año 1997 (Parlamento y Consejo Europeo, 1997) y la segunda 2002 (Comunidades Europeas, 2002) y como estos dos instrumentos normativos permearon no solo las legislaciones de los países miembros de la Unión Europea, si en las legislaciones latinoamericanas entre ellas la Colombiana.

Como primer elemento es conveniente efectuar una revisión sobre los conceptos de concesión y licencias, con el fin de determinar el porqué de la se consideró conveniente introducir el modelo de la autorización general para la provisión de redes y servicios de comunicaciones electrónicas, como una respuesta al fenómeno de la convergencia como fenómeno dinamizador del mercado.

Tradicionalmente, los legisladores y las autoridades administrativas, definieron a las licencias de telecomunicaciones, como una autorización por medio de la cual una entidad de carácter administrativo autorizaba a un proveedor para prestar o explotar un servicio de comunicaciones (Intven & Tétrault, 2000).

Ese título, no solo incluía los derechos asociados con la autorización, sino con los derechos y obligaciones del operador, conforme al servicio que le había sido autorizado prestar y la red vinculado al servicio, atendiendo a que el modelo diseñado antes y durante los primeros años de la liberalización estaba asociado a la relación intrínseca entre la red y el servicio.

Ahora bien, dentro de esos títulos previstos para la prestación de los servicios de comunicaciones, modelo que no fue ajeno a la tradición de los países que adoptamos la teoría del servicio público (De La Quadra-Salcedo, 2010). De allí que la concesión de licencias, fuera otro de los modelos escogidos para el ingreso al mercado de las telecomunicaciones y como una modalidad de contrato regulado por las Leyes especiales de contratación, donde se incorporaban las particularidades de la figura.

Adicionalmente, de acuerdo con nuestra construcción general del Derecho Administrativo, existe una diferenciación entre concesiones (para un régimen no liberalizado), y autorizaciones –o licencias- y comunicaciones (en un entorno liberalizado). Es decir que, con carácter general, un servicio puede estar liberalizado (es decir, prestarse en un régimen de libre competencia) y su prestación sujetarse a la obtención de una autorización (o licencia) o a la realización de una comunicación, pero no a la obtención de una concesión (que sería propia de un régimen no liberalizado).

Las concesiones de licencias, son procedimientos donde la administración a través de un procedimiento y conforme al modelo diseñado para la prestación de nuevos servicios en los que se determinaban los parámetros de ingreso, los derechos y obligaciones para la prestación de un servicio en concreto, instrumento que fue utilizado en contexto europeo y colombiano durante las décadas de los años noventa y la primera década del siglo XIX y de un modelo de nuevos ingresos para el sector en razón de su apertura y del número de agentes participantes en el mercado.

Tal como indican (Intven & Tétrault, 2000, p. 2), hay un conjunto de principios vinculados al modelo de concesión de licencias, como lo era la reglamentación de la provisión de un servicio público esencial, privatización o comercialización, reglamentación del mercado, establecimiento de un marco de competencia, asignación de recursos escasos, generación de ingresos para el Estado, protección del consumidor y certeza sobre el marco reglamentario.

Bajo este modelo tanto Colombia, como Perú edificaron su modelo de ingreso al mercado y conforme a diversas leyes asociados a los diversos servicios como los de telefonía móvil celular, los servicios de televisión, que determinaron la forma como se ingresaba al mercado, la duración de la concesión y los derechos asociados a la prestación del servicio.

Colombia en el 2009, abandona este modelo incorporando un régimen de transición para que aquellos operadores que se encontraban sujetos al modelo concesional migraran al modelo de habilitación general, modelo que se replicó en el año 2019, con el servicio de televisión.

Pero con el fin de precisar la evolución de la autorización o habilitación general, es necesario revisar la experiencia europea, que sirve como modelo a seguir respecto a la transformación propia de los títulos habilitantes para el sector TIC.

1.1. UNIÓN EUROPEA.

La construcción de un Mercado Interior de Servicios de Comunicaciones, trajo consigo una revisión de los modelos vigentes en cada uno de los países con el fin de crear reglas uniformes y generales en el seno de las Comunidades Europeas, hoy conocida

como Unión Europea. Es así como desde 1990, el legislador comunitario empezó a incorporar modificaciones o nuevos parámetros cuya finalidad era la ejecución del plan de liberalización concebido desde 1987 a través del Libro Verde de Telecomunicaciones que se materializan diversas directivas cuyo propósito era crear un marco general para el sector de las telecomunicaciones.

Es así como en la Directiva 90/387/CEE, del Consejo, de 28 de junio de 1990, relativa al establecimiento del mercado interior de los servicios de telecomunicaciones, mediante la realización de la oferta de una red abierta de telecomunicaciones; en la Directiva 97/51/CE, del Parlamento Europeo y del Consejo, de 6 de octubre de 1997, por la que se modifica la inicialmente citada y la 92/44/CEE para su adaptación a un entorno competitivo en el sector de las telecomunicaciones; en la Directiva 92/44/CEE, del Consejo, de 5 de junio de 1992, relativa a la aplicación de la oferta de red abierta a las líneas alquiladas; en la Directiva 95/62/CE, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1995, relativa a la aplicación de la oferta de red abierta (ONP) a la telefonía vocal, cuya modificación prevé la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la aplicación de una red abierta (ONP) a la telefonía vocal y sobre el servicio universal en las telecomunicaciones en un entorno competitivo; en la Directiva 96/19/CE, de la Comisión, de 13 de marzo de 1996, por la que se modifica la Directiva 90/388/CEE en lo relativo a la instauración de la plena competencia en los mercados de telecomunicaciones; en la Directiva 97/13/CE, del Parlamento Europeo y del Consejo, de 10 de abril de 1997, relativa a un marco común en materia de autorizaciones generales y de licencias individuales en el ámbito de los servicios de telecomunicaciones; en la Directiva 97/33/CE, del Parlamento Europeo y del Consejo, de 30 de junio de 1997, relativa a la interconexión en las redes de telecomunicaciones, para garantizar el servicio universal y la interoperabilidad, mediante la aplicación de los principios de la oferta de red abierta (ONP) y en la Directiva 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad.

Ahora bien, en la construcción de ese marco normativo y de garantizar la libertad de concurrencia, se expide la Directiva 97/13/CE, del Parlamento Europeo y del Consejo, de 10 de abril de 1997, relativa a un marco común en materia de autorizaciones generales y de licencias individuales en el ámbito de los servicios de telecomunicaciones (Parlamento y Consejo Europeo, 1997), configurándose de esta manera como un verdadero instrumento para el libre acceso al mercado, al incorporar un régimen y marco común en materia de autorizaciones y licencias individuales en el ámbito de los servicios individuales en el ámbito de los servicios de telecomunicaciones.

El modelo de autorización que incorpora esta Directiva, tenía como propósito tal como veremos en la Directiva de Autorización del año 2002, el de alcanzar los objetivos de interés público en beneficio de los usuarios de las telecomunicaciones, de crear un nuevo modelo de autorizaciones diferentes a los modelos previstos en materia de concesión, licencias y permisos, coherentes con el sistema propio de la Unión Europea, donde se garantizara los principios de libertad de establecimiento y libertad de prestación de servicios, debiendo tener en cuenta la necesidad de facilitar la introducción de nuevos servicios y la aplicación generalizada de las innovaciones tecnológicas y la tener un marco armónico que garantizará el ingreso al mercado, diferente al modelo de concesión administrativa, que no era compatible con el modelo que inspiraba la Unión Europea.

El aspecto más determinante de esta Directiva, a juicio del legislador comunitario, era que los regímenes tal como habían sido concebidos en materia tanto de concesión de autorizaciones generales y licencias individuales, eran muy complejos, y por ende

configuraban una fuerte barrera de entrada al mercado, por consiguiente la regulación debería orientarse a contar con marcos más simples en materia de concesiones y autorizaciones, tal como se precisó en los considerandos de la Directiva, la no exigencia a los Estados de nuevas reglas o mecanismos de autorización para la prestación de nuevos servicios de comunicaciones².

La finalidad en sí, era la simplificación de los mecanismos para garantizar el acceso de nuevos operados para la prestación de nuevos servicios de comunicaciones por parte de los usuarios y de esta manera facilitar la prestación de servicios de telecomunicaciones, la conveniencia de crear regímenes de acceso al mercado que no exijan autorizaciones o que estén basados en autorizaciones generales, y no licencias individuales. En síntesis, lo que se busca es que, mediante un modelo de autorizaciones generales, se pudiera prestar un determinado servicio, sin que mediara el permiso o licencia de una determinada autoridad, mediante el establecimiento de un conjunto de condiciones específicas definidas previamente de un modo general, las cuales podrían ser licencias por categorías, o en una legislación general que permita la prestación del servicio y el establecimiento o la explotación de la red.

Atendiendo al preámbulo la Directiva (Parlamento y Consejo Europeo, 1997), las figuras de autorización general y figura de licencias previas, fueron reconocidos como nuevos instrumentos orientados a flexibilizar el modelo de concesiones y permisos y la reducción de las barreras existentes en el sector de las telecomunicaciones. Los dos modelos pueden explicarse de manera gráfica de la siguiente manera:

| Tipo de Autorización | Definición |
|------------------------|--|
| Autorización General | Entendida como toda autorización, con independencia de que se rija por una «licencia por categoría» o por disposiciones legales de carácter general y que disponga o no la obligación de registro, que no exija a la empresa interesada que recabe una decisión expresa de la autoridad nacional de reglamentación antes de ejercer los derechos que se derivan de la autorización. |
| Licencias Individuales | Entendida como toda autorización concedida por una autoridad nacional de reglamentación que confiera derechos específicos a una empresa o que imponga a dicha empresa obligaciones específicas que complementen, cuando proceda, la autorización general, cuando la empresa no pueda ejercer dichos derechos hasta que se le haya comunicado la decisión de la autoridad nacional de reglamentación. |

Creación propia basado en: Parlamento y Consejo Europeo, 1997.

En cuanto al procedimiento, se determinó que serán los Estados miembros los que determinaran qué tipo de servicios podrían someterse a una u otra figura, así como las limitantes en cuanto al número de licencias individuales en cabeza de los operadores

2 ZEGARRA VALDIVIA, Servicio Público y Regulación Marco Institucional de las Telecomunicaciones en el Perú, 2005, p. 367: "Esta adaptabilidad, que como sabemos se realizó en el ámbito comunitario , tiene como una de sus fuentes principales aquellos elementos de análisis que desde la economía se plantean y que proporcionan al ámbito del Derecho administrativo muchos elementos de reflexión y de análisis para renovar los mecanismos de intervención pública, tanto en el ámbito regulatorio como en el prestacional."

de servicios de comunicaciones, así como la incorporación de una serie de condiciones previstas en el anexo de esta Directiva, atendiendo siempre a los principios de proporcionalidad y no discriminación. Sumado a los anteriores criterios, se consideró oportuno crear una ventanilla única, para dar trámite a las licencias individuales o autorizaciones generales, como un mecanismo óptimo para dar respuesta a las solicitudes y a los procedimientos previstos para dar este tipo de autorizaciones, lo cual se constituyó en gran avance para la configuración de un mercado único de comunicaciones y donde el ingreso de agentes en escenarios competitivos requería de este tipo de mecanismos.

Ahora bien, se lograron significativos avances bajo este nuevo modelo, al identificarse las barreras que limitaban el ingreso de nuevos agentes al mercado, es por esta razón que dentro del Paquete de Directivas expedidas en el año 2002 o como se le ha denominado en la doctrina el Paquete Teleco, se expidió la Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización) (Comunidades Europeas, 2002), de ampliar el modelo vigente y crear un modelo de autorización general.

Como antecedente a este nuevo modelo que se incorpora en la Directiva de Autorización, se debe tener los comentarios de los diferentes agentes del sector quienes coincidieron en la conveniencia de generar un modelo único en materia de regulación del acceso al mercado de redes y servicios de comunicaciones electrónicas con el fin de que este fuera más armonizado, del reconocimiento de la convergencia como fenómeno y la integración entre redes y servicios de comunicaciones electrónicas y sus tecnologías, lo que hacían necesaria la configuración de un modelo único de autorización para los servicios, independiente de las tecnologías utilizadas por parte de los operadores.

Por consiguiente, la finalidad de la Directiva 2002/20/CE, era de determinar un marco de acceso y de autorización para la prestación de servicios y redes de comunicaciones, de acuerdo con las condiciones que en dicho instrumento se determinarán. La autorización contenida en la Directiva, comprende todos los servicios y redes de comunicaciones electrónicas, se suministren o no al público.

El nuevo modelo de autorización general para las redes y todos los servicios de comunicaciones electrónicas, precisa que no la autorización no debe estar sujeto a decisión o un acto administrativo explícitos de la autoridad nacional de reglamentación, lo que implica que debe existir una mera notificación por parte de los suministradores de redes o servicios de comunicaciones electrónica del inicio de sus actividades, sin ser considerado como un acto administrativo. Tal como fue concebido en el articulado de la Directiva, el trámite de notificación, consiste en una declaración por parte de una persona física o jurídica ante la autoridad nacional de reglamentación de su intención de iniciar el suministro de redes o servicios de comunicaciones electrónicas y la entrega de la información mínima necesaria para que la autoridad nacional de reglamentación pueda mantener un registro o una lista de suministradores de redes y servicios de comunicaciones electrónicas (De La Quadra-Salcedo, 2010).

La autorización general, no puede generar o derivar otro tipo de tasas, más allá del pago de las tasas derivadas por la autorización de derechos de uso de números, frecuencias de radio y derechos de instalar recursos.

Es así como, como en la Directiva de Autorización, se viene a definir y reconocer la autorización general, como:

...toda disposición de los Estados miembros que otorgue derechos para el suministro de redes y servicios de comunicaciones electrónicas que establezca

obligaciones específicas al sector que podrán aplicarse a todos o a determinados tipos de redes y servicios de comunicaciones electrónicas, de conformidad con la presente Directiva. (Comunidades Europeas, 2002).

De la anterior definición se puede precisar que todos los Estados miembros estaban en la obligación de garantizar la libertad de suministrar redes y servicios de comunicaciones electrónicas, y no podrán impedir que una empresa suministre redes o servicios de comunicaciones electrónicas.

Lo anterior, no impide que las autoridades de reglamentación pudieran solicitar información a cada suministrador de redes y servicios de comunicaciones o solicitar el cumplimiento de las condiciones de la autorización general o los derechos de uso y de obligaciones específicas.

Finalmente, el modelo que fue diseñado desde el año 1997, viene a confluir en un solo instrumento normativo denominado Código Único de Comunicaciones de la Unión Europea (Parlamento y Consejo Europeo, 2018), que recoge lo dispuesto en materia de autorización general, por consiguiente y previo cumplimiento de los requisitos previstos, autorización general, las reglas previstas sobre el particular continúan vigentes el contexto de la Unión Europea.

Con este modelo incorporado a través de Directivas, surge la obligación de los países miembros de transponer este instrumento normativo a cada una de sus legislaciones, es así como en el contexto español desde el año 1998 a la fecha se han expedido tres leyes donde la figura de la autorización general y del registro de los suministradores de redes y servicios de comunicaciones fue incorporado en cada una de ellas.

Por la afinidad e incidencia que ha tenido la legislación colombiana, será el modelo por revisar en este documento.

1.2. ESPAÑA.

Es mediante la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, que se transpone la Directiva 97/13/CE, del Parlamento Europeo y del Consejo, de 10 de abril de 1997, relativa a un marco común en materia de autorizaciones generales y de licencias individuales en el ámbito de los servicios de telecomunicaciones (Parlamento y Consejo Europeo, 1997), la cual incorpora el modelo de autorizaciones generales y de licencias individuales para la prestación de los servicios y la instalación o explotación de redes de telecomunicaciones, modificando así el modelo de concesiones y de autorizaciones administrativas, al régimen para el otorgamiento de títulos habilitantes, impuesto por las Directivas Comunitarias.

Es así, como el legislador español, matiza la figura de los Títulos habilitantes y los supuestos en los que no es preceptiva su obtención, para tal efecto, se precisó en su momento que para la prestación de los servicios y el establecimiento o explotación de las redes de telecomunicaciones se requerirá la previa obtención del correspondiente título habilitante que, según el tipo de servicio que se pretenda prestar o de la red que se pretenda instalar o explotar, consistirá, conforme a este Título, en una autorización general o en una licencia individual. Ambos títulos habilitantes, podrán permitir la prestación de servicios de telecomunicaciones en los distintos Estados miembros de la Unión Europea.

Asimismo, incorporó un listado de servicios excluidos del modelo autorizaciones y licencias previstos en la misma ley, para los siguientes servicios:

- a) Los servicios de telecomunicaciones y las instalaciones de seguridad o intercomunicación que, sin conexión a redes exteriores y sin utilizar el dominio público radioeléctrico, presten servicio a un inmueble, a una comunidad de propietarios o dentro de una misma propiedad privada.
- b) Los servicios de telecomunicaciones establecidos entre predios de un mismo titular que no utilicen el dominio público radioeléctrico.
- c) Las instalaciones o equipos que utilicen el dominio público radioeléctrico, mediante su uso común general.

También se incorporó el modelo previsto en la misma Directiva referente a las autorizaciones generales para la prestación de los servicios y el establecimiento o explotación de redes telecomunicaciones, las cuales no estaba sujetas al otorgamiento de licencias de carácter individual. Para tal efecto, se establecieron un conjunto de condiciones para el otorgamiento de dichas autorizaciones, partiendo de la premisa de que estas autorizaciones se otorgan de forma reglada y el operador debería garantizar lo siguiente:

1. El cumplimiento por el titular autorizado de los requisitos esenciales exigibles para la adecuada prestación del servicio o la correcta explotación de la red, así como de los demás requisitos técnicos y de calidad que se establezcan, para el ejercicio de su actividad.
2. El comportamiento competitivo de los operadores en los mercados de telecomunicaciones.
3. La utilización efectiva y eficaz de la capacidad numérica.
4. La protección de los usuarios.
5. El encaminamiento de las llamadas a los servicios de emergencia.
6. El acceso a los servicios de telecomunicaciones por parte de personas discapacitadas o con necesidades especiales.
7. La interconexión de las redes y la interoperabilidad de los servicios.
8. La protección de los intereses de la defensa nacional y de la seguridad pública.

Deberán aportar, asimismo, toda la información necesaria sobre la prestación del servicio o sobre la explotación o el establecimiento de la red.

En cuanto a los requisitos, se estableció por parte del mismo legislador, que los datos del solicitante de dicha autorización, debería estar registrado, para poder dar inicio a la prestación del servicio o las actividades conducentes al establecimiento o a la explotación de la red, y solo que se tuviera la inscripción podría dar el inicio de la prestación de las actividades. El certificado de la inscripción, constituiría la simple existencia de la autorización.

Efectuando una revisión del modelo previsto en el contexto español, y con el fin de garantizar la intervención administrativa del Estado, a juicio del legislador español, se estableció como regla general las autorizaciones generales y como excepción las licencias individuales, esto es el previo cumplimiento de una serie de requisitos establecidos en la Orden Ministerial de Autorizaciones Generales, lo cual implicaba la capacidad de

la autoridad administrativa de condicionar el otorgamiento de la autorización, siendo exigible para la prestación de servicios de telecomunicaciones a terceros.

El encargado de conceder este tipo de autorizaciones fue asignado en ese entonces la a Comisión del Mercado de las Telecomunicaciones CMT, entidad que contaba con un carácter reglado para cada categoría de red y servicio y dicha autorización solo podría ser revocada solo cuando se diera un incumplimiento grave por parte del operador. Adicionalmente, la autorización no era automática, sino que esta se daba previo cumplimiento de los requisitos establecidos en la Orden Ministerial, que daban paso a la denegación de esta.

Adicionalmente, era indispensable que se diera un registro especial de los titulares de las autorizaciones, con el fin que una vez se procediera a la inscripción, se pudiera dar inicio a la prestación de los servicios correspondientes.

En lo que respecta a las Licencias individuales, se limitaron los supuestos para su otorgamiento, siendo estos: el establecimiento o explotación de redes públicas de telecomunicaciones, la prestación del servicio telefónico disponible al público, y la prestación de servicios o el establecimiento o explotación de redes de telecomunicaciones que impliquen el uso del dominio público radioeléctrico. Como el cumplimiento de unos requisitos para su concesión por parte de la autoridad de reglamentación, lo que nos permite indicar que era un título habilitante reglado, sujeto a un número de licencias que podrían ser conferidas y el procedimiento establecido para su otorgamiento.

Dentro de las particularidades a destacar, es que debería existir una manifestación expresa por parte de la administración para su otorgamiento, en este caso en particular, no operaba la figura del silencio administrativo negativo; la segunda particularidad, es que era una licencia hecha a la medida de los operadores, lo cual delimitaba efectivamente su actuación, como la actuación de la administración (Montero Pascual, 2007).

Tal como sucedían con las autorizaciones generales, su otorgamiento se daba por parte de la Comisión del Mercado de las Telecomunicaciones y existía una tipología respecto a las mismas que se encontraba consagrada en la Orden Ministerial del 29 de septiembre de 1998, donde se indicaba el carácter de la actividad que iba a ser licenciada. Sobre el particular, se distinguían licencias asociadas con el establecimiento o explotación de redes públicas de telecomunicaciones, las segundas licencias que habilitaban para la explotación de redes de servicios de telecomunicaciones que impliquen el uso del dominio público o explotación de redes de telecomunicaciones que impliquen el uso del dominio público radioeléctrico, y por último, dentro de esta clasificación licencias que habilitaban la realización de pruebas técnicas o eventos o acontecimientos de corta duración.

De acuerdo con la evolución propia de los mercados y de la misma regulación que se incorpora en la Directiva de Autorización (Comunidades Europeas, 2002), se expide la Ley 32/2003 (Jefatura del Estado, 2003), que incorpora un nuevo modelo de explotación de redes de prestación servicios de comunicaciones electrónicas en régimen de competencia, atendiendo a que el objetivo de la Directiva el cual era garantizar la libertad de concurrencia en un ambiente de convergencia.

Es por esta razón que el título II de la Ley 32/2003 (Jefatura del Estado, 2003), en su artículo quinto, incorpora el principio general de libre competencia en la explotación de redes y la prestación de servicios de electrónicas (Lavilla Rubira, Artículo 5. Principios aplicables, 2004) que, si bien habían sido incorporados en la anterior, es mediante la nueva modificación que se da en el seno comunitario y atendiendo a la convergencia, donde se consideró oportuno y necesario para lograr la concurrencia efectiva, nuevos operadores.

Tal como lo indica (Lavilla Rubira, Artículo 5. Principios aplicables, 2004, pp. 82-83), la primera Ley expedida en el año de 1987 reguló gradualmente la apertura a los servicios de comunicaciones, de allí que existirá una regulación por cada uno de los servicios y se otorgarán habilitaciones o concesiones específicas en razón a cada uno de los servicios, limitando el acceso al mercado en razón al número de concesiones previstas por parte de la administración.

Es a partir del año de 1998, producto de los cambios introducidos en respecto a la definición de la categoría de servicio público en el seno de la Comunidad Europea y la creación de una categoría superior a la que se le denominó servicios de interés general (De La Quadra-Salcedo, 2010), que amplió de manera sustancial la libre iniciativa y por consiguiente que el principio de libre competencia se convirtiera en elemento fundamental para la configuración de un mercado único de las comunicaciones, aspecto que es consagrado en el paquete de directivas expedidas en el año 2002. Lo anterior, implica que no solo se garantice que cual agente económico pueda adquirir la calidad de operador, sino que para que existiera la competencia en el mercado era necesario contar con los mismos parámetros, esto es condiciones de igualdad para todos los agentes, principalmente para su ingreso al mercado.

Bajo estas consideraciones se edifica el modelo de autorizaciones generales modificando el régimen vigente de licencias individuales o el de concesión de licencias para la prestación de los servicios, en virtud de este principio, con una serie de limitaciones asociadas generalmente con los recursos escasos y la limitación por el acceso al uso del espectro.

Adicionalmente, se indica que las autorizaciones previas no son autorizaciones sino comunicaciones previas, seguidas de la inscripción registral, lo que nos permite concluir que la notificación realizada no puede supeditarse a la obtención del acto administrativo otorgado por la autoridad. Es entonces responsabilidad del operador, atendiendo al marco previsto en la ley, de efectuar dicha notificación y el papel que viene a desempeñar la Administración es la de validar la notificación, previo a la existencia de un procedimiento que le permite a la autoridad asignada la posibilidad de solicitar modificaciones al proyecto de autorización o dar su prohibición.

Ahora bien, la gran modificación que se incorpora en la Ley 32/2003, es la figura de la habilitación directa para la prestación del servicio, en régimen anterior, era necesario contar con un título habilitante en razón al servicio o red, contando con un sistema reglado para contar con ese título habilitante y con una participación de la administración. Es así como en el artículo 6 y atendiendo al marco general previsto en la Directiva de Autorización (Comunidades Europeas, 2002), que quienes cumpliendo unos determinados requisitos tanto objetivos como subjetivos, podían proveer los servicios de comunicaciones electrónicas o explotar una red, atendiendo la habilitación directa que se incorporó en el ordenamiento español, previa notificación por parte de la autoridad de administrativa de la citada habilitación para el comienzo o bien de la explotación o prestación del servicio, garantizado un acceso con la mínima intervención de la administración.

En cuanto a los requisitos previstos para acceder a la habilitación, uno de ellos era que la solicitud fuera realizada o bien por una persona jurídica o bien por una persona natural, no personas que no cuenten con personalidad jurídica. Asimismo, el procedimiento previsto es que la persona natural o jurídica interesada en la explotación de una determinada red o prestación de un determinado servicio de comunicaciones, notificará al organismo regulador sobre su intención de realizar la actividad.

Es necesario precisar que si bien realizada la notificación por parte del operador, esto no impedía que el órgano encargado de su gestión, pudiera adoptar las siguientes decisiones sobre el particular, como la de dictar una resolución no teniendo por realizada dicha notificación o proceder a la inscripción en el Registro de Operadores. En el caso particular que no fuera aprobada la notificación, nos viene a precisar que, si bien la intervención mínima por parte de la autoridad correspondiente en validar el cumplimiento de los requisitos previstos en la ley, con el fin de que puedan ser subsanados y de esta manera proceder a su registro, en el caso contrario de no allegar la información se entenderá no realizada la notificación (Lavilla Rubira, Artículo 5. Principios aplicables, 2004, pp. 97-98).

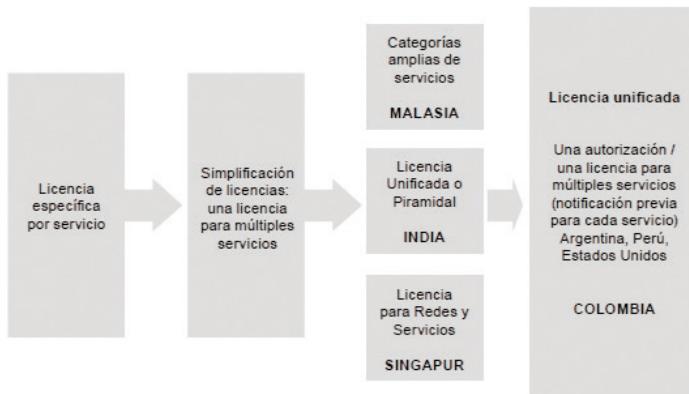
Ahora bien, en la última reforma a la legislación en materia de comunicaciones de España, realizada a través de la Ley 9/2014, el legislador español recoge la figura incorporada en las leyes que la anteceden, replica la fórmula incorporada en los artículos 6 y 7 de la anterior, no sólo como un mecanismo para garantizar la competencia en el sector de las comunicaciones electrónicas, sino como el mecanismo más eficiente para garantizar el fenómeno de la convergencia.

1.3. COLOMBIA.

Tal como se indicó previamente, el mercado de las comunicaciones en Colombia, se edificó a través de un modelo de concesiones basado en la clasificación de servicios prestados a través de redes diferenciales, conforme a la clasificación prevista en el Decreto 1900/1990, donde se incorporaron tres grandes categorías: servicios básicos dentro de los que se incluían los servicios de portador, telefonía y telegrafía, los servicios de radiodifusión dentro de los que estaba la radio y la televisión y los demás servicios denominados de valor agregado y telemáticos.

Bajo ese marco general, se expedieron normas específicas para prestar cada uno de los servicios previstos en dicha clasificación, es así como en la década de los noventa, se expedieron diferentes leyes, asociadas a estos servicios, donde se precisaba la forma de ingreso al mercado, los derechos y obligaciones, en el marco de las competencias asignadas al Estado para determinar las condiciones de acceso al mercado, la forma como debían prestarse los servicios entre otros (Guerra De la Espriella, 2010). Sin perjuicio de lo anterior, el modelo de acceso al mercado se estructuró bajo el modelo de licencias, entendidas estas como actos administrativos y contratos de concesión, atendiendo al tipo de servicio se podía prestar el servicio, restringiendo de alguna manera el ingreso de nuevos agentes al mercado. Tal como se puede evidenciar en la siguiente gráfica:

GRÁFICO III.1
VISIÓN INTERNACIONAL DE AJUSTES LEGALES EN MATERIA DE HABILITACIÓN



Fuente: elaboración propia con base en *Creating a Regulatory Framework for New Technologies: Legal and Institutional Challenges*, Hong Kong, China 2-3 December 2006, TMG.

Tomado de: Guerra de la Espriella & Oviedo Arango, 2011, p. 43.

A la evolución misma del mercado, de la irrupción de la telefonía móvil, los tratos diferenciales con los servicios de telefonía básica y los mecanismos previstos para su ingreso, al ser considerados los segundos como esenciales, trajeron consigo diferencias sustanciales, que vendría a ser solventadas con la expedición de la Ley 1341 de 2009.

Dada la importancia de garantizar la competencia y atendiendo a las dinámicas y evolución de la legislación comunitaria y de la legislación española y de la creación de marcos legales compatibles con la convergencia como fenómeno donde la confluencia de los servicios de tecnologías y las comunicaciones y sus implicaciones tanto normativas como económicas trajeron consigo reevaluar no solo la estructura del mercado, sino las formas de ingreso al mismo, y la reducción significativa de barreras de entrada para el ingreso de nuevos agentes al mercado (Guerra de la Espriella & Oviedo Arango, 2011, p. 43).

No se pueden desconocer los efectos beneficiosos de la convergencia para los mercados, que por consiguiente debían verse reflejados en los marcos legales que respondieran al fenómeno de la convergencia, en los siguientes aspectos:

- Facilita entornos de diferentes servicios a través de múltiples plataformas;
- Permite la provisión de múltiples servicios sin incurrir en altos costos de transacción;
- **Define regímenes integrales en materia de habilitación**, gestión del espectro radioeléctrico, interconexión de redes y promoción del acceso/servicio universal. (Guerra De la Espriella, 2010, p. 79). Negrilla fuera del texto original.

Bajo este preámbulo, Colombia evidenció la necesidad de revisar su regulación en materia de comunicaciones, con el fin de lograr un acercamiento a un modelo único respecto de los regímenes vigentes para la prestación de servicios y que respondieron un modelo de convergencia, como la creación de una autoridad encargada en la gestión del espectro en

cabeza de la Agencia Nacional del Espectro y de nuevas competencias y atribuciones en cabeza de la Comisión de Regulación de Comunicaciones CRC (Congreso de la República de Colombia, 2009).

Antes de abordar el régimen es conveniente hacer unas precisiones sobre la titularidad de los servicios de telecomunicaciones en Colombia y por qué al ser un servicio liberalizado no se acogió la fórmula de la Unión Europea de considerarlos como servicios de interés general y continuar con la definición tradicional de servicio público.

Dentro de las modificaciones más importantes y sustanciales al modelo vigente está la contenida en el Artículo 10 de la ley, mediante la cual se incorpora en el ordenamiento colombiano el régimen integral de habilitación general de servicios de telecomunicaciones.

La existencia de barreras de ingreso al mercado, tienen repercusiones en las tarifas, atendiendo a los costos asociados para el ingreso deberían ser revertidos en las tarifas finales de los usuarios y producto de los servicios convergentes y las modificaciones dadas en el contexto comunitario y español, se consideró conveniente y oportuno para la creación de un mercado en condiciones ingreso para garantizar la competencia, la simplificación de las licencias y la incorporación de un régimen de habilitación general, sujeta a un régimen de transición y de un modelo de habilitaciones individuales para casos especiales cuando fuera necesario el uso del espectro radioeléctrico, los cuales estarían sujetos a un procedimiento específico para su asignación, como se encuentra contenido en la misma ley.

La filosofía que inspira el artículo es que mediante el modelo de habilitación general, se permite a los proveedores de redes y servicios de comunicaciones la prestación de los servicios, bajo un régimen uniforme de derechos y obligaciones para todos los proveedores y servicios de comunicaciones. La particularidad es que la habilitación solo quedará surtida una vez el proveedor de redes y servicios de comunicaciones se inscriba en el registro creado para tal fin, administrado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

2. HABILITACIÓN GENERAL EN COLOMBIA. LEY 1341 DE 2009.

Antes de la expedición de la Ley 1341 de 2009 y atendiendo al fenómeno de la convergencia, una de las respuestas dadas por la administración fue la de crear un título habilitante convergente previsto en el Decreto 2870 de 2007 (Presidencia de la República de Colombia, 2007), como una nueva forma de permitir el ingreso al mercado diferente al modelo establecido de contratos de concesión y licencias previstos desde los años noventa (De La Rosa, 2010), salvo las excepciones previstas en la misma definición de lo que se entiende como Título Único Convergente.

Para tal efecto, se definió como Título Único Convergente lo siguiente:

Título Habilitante Convergente: esta denominación comprende las licencias y concesiones para la prestación de servicios públicos de telecomunicaciones de que tratan el Decreto-ley 1900 de 1990 y el inciso cuarto del artículo 33 de la Ley 80 de 1993. Se exceptúan los servicios de Televisión consagrados en la Ley 182 de 1995 y sus modificaciones, los servicios de Radiodifusión Sonora, Auxiliares de Ayuda y Especiales de que trata el Decreto-ley 1900 de 1990, los servicios de Telefonía Móvil Celular -TMC- y de Comunicación Personal -PCS- definidos en las Leyes 37 de 1993 y 555 de 2000, respectivamente, y los servicios de Telefonía Pública Básica Commutada Local, Local Extendida y Telefonía Móvil Rural contemplados en la Ley 142 de 1994.

Tal como se indicó en el apartado referente al modelo de la Unión Europea, para la obtención de este tipo de Título Habilitante Convergente, los solicitantes deberían cumplir un conjunto de requisitos para su otorgamiento, un poco extensos y que no responden a la misma dinámica del ingreso del mercado, tales como la de ser persona jurídica constituida conforme a la legislación colombiana, cuyo objeto social incluya la prestación de servicios de telecomunicaciones, no estar inciso de inhabilidad, incompatibilidad y prohibición y la presentación de una solicitud formal por parte del representante legal y/o apoderado, acompañada de la prueba que acredite la existencia y representación legal de la sociedad, en la cual conste que su vigencia es igual al término de duración del Título Habilitante Convergente y un (1) año más, y en la que incluya, además de sus datos de correspondencia, un correo electrónico para los efectos a que hubiere lugar. Adicionalmente, debería relacionar los servicios de telecomunicaciones que serán prestados en virtud de dicho Título y la cobertura o el área de servicio donde se prestarán y abonar el pago de la contraprestación por la expedición del Título Habilitante Convergente.

El modelo como tal no está las particularidades del modelo europeo, en el entendido que se le concedió, dos meses al Ministerio, para otorgar el mencionado Título Habilitante Convergente y registrarlos los servicios, previa verificación del cumplimiento de los requisitos establecidos en el presente artículo y demás normatividad vigente aplicable a cada servicio.

El otorgamiento del título convergente generaba una serie de contraprestaciones a saber, como eran el pago correspondiente de la contraprestación por la expedición del título habilitante convergente, consistente en tres salarios mínimos mensuales vigentes, pagaderos una sola vez, así como el pago de dos tipos de contraprestaciones una periódica, atendiendo a las normas asociadas a la prestación de dicho servicio y la segunda la prórroga o cesión del título convergente, equivalente a un salario mínimos.

Tal como lo indicábamos la Ley 1341 de 2009, incorpora la libertad de empresa y el régimen de competencia como principios y fines que orientan la Ley, y para su consecución incorpora la figura de la habilitación general, como una forma de prestar y proveer los servicios de comunicaciones, atendiendo a que esta Ley, no elimina la categoría de servicio público, sino que incorpora esta figura como una forma para garantizar el ingreso de nuevos agentes, de nuevos servicios en beneficio de los usuarios.

Sobre este último aspecto es conveniente analizar el alcance que tiene la clasificación de los servicios de telecomunicaciones como servicio público y la titularidad del Estado sobre estas atendiendo a la incorporación de la figura de la habilitación general como modelo vigente en los países donde existe una liberalización plena en la prestación de los servicios tal como se dio en la Unión Europea.

Tal como afirma (Montaña Plata, 2010), el legislador colombiano en el artículo 4 de la Ley 1341 de 2009, pone que las telecomunicaciones son un servicio público donde el Estado no ha perdido su titularidad, aspecto que puede ser contradictoria con la lógica que inspiró el proceso de liberalización y particularmente la inclusión del modelo de habilitación general que se incorpora en la Ley TIC.

Sobre el particular el autor (Montaña Plata, p. 177 y ss.), precisa que la existencia del concepto tan arraigado en el contexto colombiano, como lo es el concepto de servicio público, el proceso de liberalización y el surgimiento de nuevas categorías producto de la incorporación de la libre competencia y el libre mercado, trajo consigo una profunda reflexión sobre el contenido y alcance del concepto de servicio público y la relación intrínseca con la satisfacción del interés general y de la creación de un sector económico como el de las telecomunicaciones, lo cual no deriva en que el papel del Estado se desdibuje,

sino que su intervención este orientada a la satisfacción de unas necesidades que tienen una correlación directa con los fines del Estado, específicamente con la satisfacción de las necesidades básicas de la colectividad.

La respuesta dada por el legislador colombiano, fue la de ajustar las nuevas categorías de servicio público y de actividades económicas de interés general, que tienen matices tanto públicos como privados, donde la misma Constitución y el modelo que ella incorpora reconoce a los servicios públicos, como actividades económicas inherentes a la finalidad social del Estado, de allí que se necesaria la intervención en la prestación eficiente de los servicios TIC. Esa adaptación de la figura lo que busca es que fuera compatible con el reconocimiento de un mercado y de la libre competencia.

En lo que respecta a la habilitación general, significó la abolición de los títulos habilitantes, para la prestación de los servicios de comunicaciones; esto es que independiente de la habilitación que debe tener para el uso del espectro radioeléctrico para determinados servicios, aspecto sobre el cual volveremos posteriormente, no es necesario la celebración de ningún tipo de contrato, o licencia proferida por parte de la autoridad para la prestación de los servicios de comunicaciones, sino contar con la habilitación expresa que incorpora la legislación.

Si bien existe una aparente contradicción entre la liberalización de los servicios de telecomunicaciones y a la titularidad que predica los mismo en la ley parte del Estado, se debe apelar como lo indica Montaña Plata (pp. 191-192), a lo previsto en 365 de la Constitución Colombiana para poder solventar la aparente contradicción que la misma ley trajo. Para tal efecto, se indica que el Estado puede prestar de forma directa o indirecta los servicios públicos y en el supuesto de prestarlos de manera indirecta, sin que medie título habilitante como sucedía en el régimen anterior, es entonces la misma Ley, que conforme a la interpretación que se hace de la Constitución es la que permite que exista este tipo de habilitación para ingresar al mercado.

Finalmente, como lo precisa Montaña, y atendiendo a un criterio interpretativo, la habilitación general es válida en el ordenamiento colombiano por:

De esta manera, lo prescrito en la disposición legal que se comenta, en nuestra opinión, aunque extraño, no resulta contrario a la Constitución, y se explicaría en el sentido de que los servicios públicos de telecomunicaciones, con la comprensión de la Ley 1341 de 2009, son de titularidad estatal, que los presta de manera indirecta, en virtud de una habilitación general de la que se desprende la posibilidad de su prestación por sujetos públicos, privados o mixtos, es la ley entonces el título habilitante, que se presupone debe existir en un modelo de servicios públicos de telecomunicaciones de titularidad estatal. (p. 192)

Con este marco conceptual, procederemos a analizar la figura de la Habilitación General y del Registro de Proveedores de redes y servicios de telecomunicaciones, en los siguientes términos:

Texto original de la Ley 1341 de 2009:

ARTÍCULO 10. A partir de la vigencia de la presente ley, la provisión de redes y servicios de telecomunicaciones, que es un servicio público bajo la titularidad del Estado, se habilita de manera general, y causará una contraprestación periódica a favor del Fondo de las Tecnologías de la Información y las Comunicaciones. Esta habilitación comprende, a su vez, la autorización para la instalación, ampliación, modificación, operación y explotación de redes de telecomunicaciones, se

suministren o no al público. La habilitación a que hace referencia el presente artículo no incluye el derecho al uso del espectro radioeléctrico.

Y del registro de proveedores de redes y servicios de telecomunicaciones, como un requisito para que quedara formalmente surtida la Habilitación General:

ARTÍCULO 15. REGISTRO DE PROVEEDORES DE REDES Y SERVICIOS DE TELECOMUNICACIONES. Creación del registro de TIC. El Ministerio de Tecnologías de la Información y las Comunicaciones llevará el registro de la información relevante de redes, habilitaciones, autorizaciones y permisos conforme determine el reglamento. Deben inscribirse y quedar incorporados en el Registro los proveedores de redes y servicios, los titulares de permisos para el uso de recursos escasos, indicando sus socios; que deberán cumplir con esta obligación incluyendo y actualizando la información periódicamente.

En el caso de las sociedades anónimas sólo se indicará su representante legal y los miembros de su junta directiva. Este registro será público y en línea, sin perjuicio de las reservas de orden constitucional y legal.

Con el registro de que aquí se trata, se entenderá formalmente surtida la habilitación a que se refiere el artículo 10 de la presente ley.

La no inscripción en el registro acarrea las sanciones a que haya lugar.

PARÁGRAFO 1º. Todos los proveedores y titulares deberán inscribirse en el registro dentro de los noventa (90) días hábiles a partir de la vigencia de la reglamentación que sea expedida, sin perjuicio del cumplimiento de sus obligaciones en su calidad de proveedores y titulares, en particular del pago de contraprestaciones.

En todo caso los nuevos proveedores y titulares deberán inscribirse de forma previa al inicio de operaciones.

PARÁGRAFO 2º. El Ministerio de Tecnologías de la Información y las Comunicaciones, creará un sistema de información integral, con los datos, variables e indicadores relevantes, sobre el sector de las Tecnologías de la Información y las Comunicaciones, que facilite la fijación de metas, estrategias, programas y proyectos para su desarrollo.

La primera precisión es que la habitación general se entiende surtida con la incorporación que se hace por parte del proveedor de redes y servicios en el registro TIC. Por lo tanto, el particular no debe esperar una respuesta del Ministerio, sino informar simplemente la condición de ser proveedor de uno o varios servicios y acreditar los requisitos mínimos solicitados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones (MintTIC) en el Decreto Reglamentario.

Asimismo, la misma ley incorporó un sistema de transición con la finalidad que los operadores que se encontraban bajo el modelo de concesión pudieran mantener su régimen concesional, de licencias, permisos y autorizaciones por el término otorgado en cada uno de estos títulos, una vez finalizado el término quedarán sujetos al régimen previsto en la ley, esto es el de la Habilitación General. Adicionalmente, la ley permitía que los operadores que estuvieran bajo un título de concesión, de licencias, permisos y autorizaciones, y quisieran acogerse de manera anticipada al modelo estipulado en esta Ley, lo podrían hacer, renunciado a los términos previstos en cada uno de sus títulos. Nuevos agentes quedaban sujetos a lo previsto en la Ley y derivando una liquidación de

los contratos suscritos previamente.

Adicionalmente a la Ley, el concepto de proveedor de redes y servicios de comunicaciones, que se reglamenta a través del Decreto 4948 de 2009 (Ministro del Interior y de Justicia de la República de Colombia, 2009), donde el proveedor es: "la persona jurídica responsable de la operación de redes y/o de la provisión de servicios de telecomunicaciones a terceros. En consecuencia, todos aquellos proveedores habilitados bajo regímenes legales previos se consideran cobijados por la presente definición" (artículo 3).

De la definición dada se incluyen agentes que hacen parte de la cadena de valor de las telecomunicaciones, que pueden agruparse de la siguiente manera:

| Operadores de Red | Proveedores de servicios | Proveedores de contenido |
|---|--|--|
| Entendidos como aquellos que aportan la infraestructura de equipos y medios de transmisión para establecer las telecomunicaciones | Entendidos como aquellos encargados de la transmisión de información | Entendidos como los que aportan a la red la información producida o elaborada por ellos mismos o por terceros, donde encontramos contenidos tales como los de entretenimiento, información, documentación, comercio electrónico entre otros. |

Creación propia, basado en De La Rosa, 2010, p. 245.

El segundo aspecto que se incorpora a la Ley, es el Registro de Proveedores de Redes y Servicios, como un requisito indispensable para que el proveedor de redes y servicios puedan prestar o suministrar los servicios. Por consiguiente, para adquirir esta calidad la persona jurídica debe suministrar, tal como se precisaba en Título Único Convergente y el mismo modelo español, la información básica y necesaria para identificar a la persona inscrita y de esta manera tener identificada la tipología de redes en el territorio nacional.

La inscripción se entiende como un mecanismo formal de habilitación, que permite la adquisición plena y formal de la calidad de proveedor o servicios de telecomunicaciones y de esta manera iniciar la operación efectiva del servicio y de sus actividades complementarias, y asumir las obligaciones y cargas previstas en la ley.

Ahora bien, en supuestos que exista una inconsistencia de la información, será el Ministerio de Tecnologías de la Información y las Comunicaciones, la entidad que no realizará el registro en los siguientes supuestos: i) Cuando se encuentren inconsistencias entre los datos suministrados en la inscripción y los documentos soporte de la misma; ii) Cuando la vigencia de la persona jurídica, en el caso de la provisión de redes y/o servicios de telecomunicaciones, sea inferior a diez (10) años contados a partir de la fecha de la inscripción, y iii) Cuando en el objeto social de la persona jurídica no esté incluida la provisión de redes y/o servicios de telecomunicaciones.

Finalmente, hay dos temas adicionales asociados con la reforma al registro, modificaciones y reforma del registro.

En lo que respecta a las modificaciones y actualización del Registro, serán los proveedores de redes y/o servicios de telecomunicaciones y los titulares de permisos para el uso de recursos escasos, habilitaciones y autorizaciones, los encargados de informar al Ministerio de Tecnologías de la Información y las Comunicaciones, las modificaciones que se produzcan respecto de los datos consignados en el registro.

En cuanto las modificaciones en la provisión de redes y/o servicios, también será el proveedor de redes y/o servicios de telecomunicaciones, el encargado de notificar los cambios, esto es cuando vaya a proveer una nueva red y/o servicio de telecomunicaciones, o deje de proveerlos deberá notificar estos cambios al Ministerio de Tecnologías de la Información y las Comunicaciones. Cuando se vaya a proveer una nueva red y/o servicio de telecomunicaciones, solo se iniciarán sus operaciones el día siguiente al que se le comunique que su modificación ha sido exitosa.

En el caso que se deje de proveer una red y/o servicio de telecomunicaciones se entenderá que se han cesado operaciones el día en que lo informe al Ministerio de Tecnologías de la Información y las Comunicaciones.

Respecto al retiro del registro, el Ministerio de Tecnologías de la Información y las Comunicaciones, podrá retirar el registro al proveedor de redes y/o servicios de telecomunicaciones o al titular de permisos para el uso de recursos, habilitaciones y autorizaciones en los siguientes casos, atendiendo a los causales tradicionales y otros criterios objetivos previstos en el Decreto:

1. A solicitud de parte, sin perjuicio del cumplimiento de obligaciones legales.
2. Muerte de la persona natural o disolución de la persona jurídica.
3. Por liquidación obligatoria de la persona jurídica.
4. Por el cese definitivo de la provisión de la red y/o del servicio de telecomunicaciones.
5. Por el vencimiento de los permisos para el uso de frecuencias radioeléctricas de los titulares de red de telecomunicaciones que no se suministren al público.
6. Por sentencia judicial debidamente ejecutoriada.
7. Por no haber dado inicio a las operaciones del servicio o provisión de redes, al año siguiente de la incorporación en el registro de la información del respectivo servicio o provisión de red.

Es necesario precisar que la finalidad de la habilitación general como del registro, es la facilitar el acceso de una manera más sencilla la provisión de redes y servicios de telecomunicaciones, simplificando y eliminando los procedimientos establecidos en el régimen anterior, para, en su lugar, establecer una habilitación general.

La particularidad del modelo, es que el Estado nunca pierde la titularidad de la actividad, en razón a que los servicios de telecomunicaciones, continúan siendo servicios públicos, sujetos al control vigilancia control del Estado. Dicha habilitación deriva obligaciones y derechos, entre ellas el pago en su momento de una contribución al Fondo de Tecnologías de la Información y las Comunicaciones, como el pago por el uso del espectro radioeléctrico (Guerra de la Espriella & Oviedo Arango, 2011, pág. 43). El modelo previsto responde a la realidad dada en el contexto europeo y como una forma para garantizar los nuevos servicios en condiciones de calidad y eficiencia para los usuarios.

Un aspecto que incorporó la Ley 1341 de 2009, es el relacionado con los permisos para el acceso al uso del espectro radioeléctrico, atendiendo que hay servicios que requieren de uso y para lo cual se indicó que su uso requiere permiso, previo, expreso y otorgado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Para tal efecto, será el Ministerio el encargado de adelantar a través de mecanismos de selección objetiva, para el uso del espectro radioeléctrico, en aquellos supuestos donde exista una suficiencia del recurso y atendiendo al nivel de ocupación de la banda. Sumado a un conjunto de reglas asociadas con los plazos y la renovación de los permisos para el uso del espectro radioeléctrico. Vale la pena aclarar que la legislación del año 2009, indicaba que el plazo inicial era de 10 años, y en la reforma del año 2019, se ajustó este plazo a 20 años, con el fin de garantizar la inversión y un mayor aprovechamiento del recurso.

Adicionalmente, se consagra que el uso del recurso genera una contraprestación a favor del Ministerio de Tecnologías de la Información y las Comunicaciones.

En términos generales la modificación es que la concesión no sólo permitía la explotación del servicio y si no la utilización del espectro radioeléctrico. La Ley 1341 de 2009 reconoce al espectro como un recurso escaso (Fajardo Muriel, 2010), que debe ser aprovechado de manera óptima, con el fin de generar competencia, calidad y eficiencia en beneficio de los usuarios, de allí la incorporación de los mecanismos para su uso, su otorgamiento y futuras renovaciones, independiente del modelo de habilitación que se incorpora en la Ley.

3. HABILITACIÓN GENERAL. LEY 1978 DE 2019.

Ahora bien, conforme a la evolución normativa y la realidad del mercado y de las recomendaciones realizadas de la OCDE en el año 2004, donde se consideró conveniente revisar el modelo vigente y de crear un regulador convergente (Ortiz Laverde, 2017). La respuesta dada por parte del Legislador, producto de los estudios elaborados por parte del Departamento Nacional de Planeación (DNP), donde se analizó al sector audiovisual y las formas de ingreso al mercado, proveniente del modelo concesiones y licencias previstos en el régimen particular del servicio de televisión y las desventajas asociadas con la existencia de dos regímenes entre el sector de telecomunicaciones y el I sector audiovisual, se consideró necesario ampliar la Habilitación general para el sector audiovisual, incorporando un régimen de transición para los titulares de los contratos y licencias otorgadas, que se materializa las cuales se materializan con la expedición de la Ley 1978 de 2019 (Congreso de la República de Colombia, 2019), por la cual se crea el regulador convergente, se incorporan otras fórmulas orientadas a el cierre de la brecha digital y la generación un marco armónico de cara a la convergencia.

ARTÍCULO 10. HABILITACIÓN GENERAL. <Artículo modificado por el artículo 7 de la Ley 1978 de 2019. El nuevo texto es el siguiente:> A partir de la vigencia de la presente Ley, la provisión de redes y servicios de telecomunicaciones, que es un servicio público bajo la titularidad del Estado, se habilita de manera general, y causará una contraprestación periódica a favor del Fondo Único de Tecnologías de la Información y las Comunicaciones. Esta habilitación comprende, a su vez, la autorización para la instalación, ampliación, modificación, operación y explotación de redes para la prestación de los servicios de telecomunicaciones, se suministren o no al público. La habilitación general a que hace referencia el presente artículo no incluye el derecho al uso del espectro radioeléctrico.

PARÁGRAFO 1°. En materia de habilitación, el servicio de radiodifusión sonora continuará rigiéndose por las disposiciones específicas de la presente Ley.

PARÁGRAFO 2°. En materia de habilitación, el servicio de televisión abierta radiodifundida continuará rigiéndose por las normas especiales pertinentes, en particular la Ley 182 de 1995, la Ley 335 de 1996, la Ley 680 de 2001, y demás normas que las modifiquen, adicionen o sustituyan. No obstante, los

operadores del servicio de televisión abierta radiodifundida establecidos a la fecha de entrada en vigencia de la presente Ley podrán acogerse al régimen de habilitación general, de conformidad con el régimen de transición que la Ley disponga.

PARÁGRAFO 3°. En materia del pago de la contraprestación los operadores públicos del servicio de televisión mantendrán las exenciones y excepciones que les sean aplicables a la fecha de entrada en vigencia de la presente Ley.

Es así como se amplía la habilitación general y el registro único TIC previstos en la ley 1341 de 2009 al sector audiovisual, estableciendo un régimen de transición tal como se tenía en la ley precedente para que los operadores con títulos concesionales vigentes antes de la expedición de la Ley 1978 de 2019 y de esta manera se da una apertura total al sector audiovisual, estableciendo un marco general e igualitario para ambos sectores, con un conjunto obligaciones previstas como lo son la contraprestación periódica a favor del Fondo Único de Tecnologías de la Información y las Comunicaciones.

Ahora bien, con la inclusión de este sector se consideró oportuno revisar y ajustar la reglamentación prevista en materia del Registro Único TIC, conforme a los parámetros establecidos en la nueva ley.

4. LA CONVENIENCIA PARA EL MODELO PERUANO.

En lo que respecta al modelo vigente en la legislación peruana, la actividad de las telecomunicaciones, está sujeta, a la existencia de títulos administrativos que habilitan a la prestación de los servicios de telecomunicaciones, cuya finalidad principal es contribuir a mejorar los fines de las comunicaciones (Zegarra, 2005).

La particularidad por la que el modelo peruano se ha caracterizado, es que su proceso de privatización cumplió con los requisitos formales de la privatización, pero no los efectos plenos de la liberalización asociados con la des publificación de la actividad de las telecomunicaciones, garantizando la libertad entrada y de salida a los operadores privados.

La segunda particularidad, es que la legislación peruana no ha sufrido modificaciones, respecto al sistema de clasificación previsto en su ley general de telecomunicaciones, si en su régimen de ingreso al mercado previsto en el TÍTULO II CONDICIONES DE OPERACIÓN CAPÍTULO I CONCESIONES, AUTORIZACIONES, PERMISOS Y LICENCIAS, que en su artículo 47 modificado por el Artículo 1 de la Ley N° 28737, publicada el 18 mayo 2006.

Artículo 47.- Llámese concesión al acto jurídico mediante el cual el Estado concede a una persona natural o jurídica la facultad de prestar servicios públicos de telecomunicaciones. El Ministerio otorgará concesión única para la prestación de todos los servicios públicos de telecomunicaciones, independientemente de la denominación de éstos contenida en esta Ley o en su Reglamento, con excepción de la concesión para Operador Independiente.

La concesión se perfecciona mediante contrato escrito aprobado por resolución del Titular del Sector. Sin perjuicio de lo dispuesto en el párrafo anterior, las personas naturales o jurídicas, titulares de una concesión única, previamente deberán informar al Ministerio de Transportes y Comunicaciones los servicios públicos a brindar, sujetándose a los derechos y obligaciones correspondientes a cada uno de los servicios conforme a la clasificación general prevista en la

Ley, a lo dispuesto en el Reglamento, normas complementarias y al respectivo contrato de concesión. El Ministerio tendrá a su cargo el registro de los servicios que brinde cada concesionario, de acuerdo a las condiciones establecidas en el Reglamento.

Tal como precisa Zegarra (2018), en lo que respecta a la legislación peruana:

...la concesión es requerida para la prestación de los servicios públicos de telecomunicaciones y se perfecciona a través de la suscripción de un contrato de concesión única para la prestación de los servicios públicos de telecomunicaciones suscrito por el titular del MTC. Las concesiones son otorgadas a solicitud de parte o mediante concurso público de ofertas.

El concurso público se realiza en supuestos: a) cuando en una determinada localidad o área de servicio exista una restricción en la disponibilidad de frecuencias para la prestación del servicio, b) cuando lo señale el Plan Nacional de Asignación de Frecuencias o c) restrinja el número de concesionarios de un determinado servicio público debido a restricciones basadas en recursos escasos.

Bajo esta perspectiva, la legislación peruana tiene previstos: la concesión administrativa, la autorización administrativa y los registros administrativos.

En lo que respecta a la concesión administrativa, esta se consideró, antes de la reforma del año 2006, como un mecanismo de habilitación para la prestación de los servicios portadores finales y de difusión, que se realizaba por la máxima autoridad administrativa.

Si bien el régimen peruano, garantiza la libertad de ingreso a los operadores para la prestación de servicios de telecomunicaciones, se viene a precisar que a efectos de que el servicio se preste en condiciones óptimas, se puede condicionar el ingreso o bien por aspectos técnicos que están asociadas a los recursos necesarios para su prestación, como lo es el espectro radioeléctrico que pueden restringirse el número de concesionarios de un determinado servicio, lo que nos viene a indicar es que la concesión será otorgada conforme a un concurso público de ofertas, y en el supuesto de no existir estas limitaciones, el futuro concesionario podrá acceder al título concesional mediante una solicitud de parte y el cumplimiento de los requisitos para tal fin. En uno o ambos supuestos, debe existir un contrato de concesión y su contenido determina la validez del contrato y los derechos y deberes del concesionario.

El segundo título habilitante para la acceder a la prestación de los servicios de telecomunicaciones en el Perú, es la autorización administrativa, como una forma de habilitación para la prestación de los servicios de radiodifusión que tiene el carácter de servicios privados de interés público, donde se si bien son servicios privados, se consideró por parte del legislador, la participación del Estado para que este revisará y validará los requisitos, con el fin que los particulares no ejercieran un uso abusivo de este tipo de actividades.

La autorización administrativa, está vinculada al establecimiento, instalación, operación, explotación y el uso de espectro radioeléctrico, si el servicio lo requiere. Lo que requiere de una validación por parte del Estado del cumplimiento de los requisitos que se encuentran vinculados con la prestación de un servicio.

Y finalmente, los registros administrativos, donde la misma ley precisa que determinados servicios no requieren ni de concesión, ni de autorización, pero que de un registro de las personas ya sean naturales o jurídicas que prestan este tipo de servicios o actividades

vinculadas para su prestación.

La legislación vinculó el registro administrativo con los servicios de valor agregado o de valor añadido. Para tal efecto, deben inscribirse en registro correspondiente, luego de haber efectuado el inicio de la prestación de este servicio. La finalidad es que se pueda solicitar información, lo cual permite que se puedan desarrollar labores de inspección y verificación por parte de la administración.

Ahora bien, es conveniente analizar la Concesión única para la prestación de servicios públicos de telecomunicaciones prevista en la Ley 28737, entendida como un acto jurídico, mediante el cual el Estado concede a una persona natural o jurídica la facultad de prestar todos los servicios públicos de telecomunicaciones, la cual perfecciona mediante un contrato escrito aprobado por Resolución del Titular del Sector y se encuentra previsto en el Texto Único Ordenado de la Ley de Telecomunicaciones aprobado mediante Decreto Supremo N° 013-93-TCC y sus modificatorias, Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones (TUO del Reglamento), aprobado mediante Decreto Supremo N° 020-2007-MTC y sus modificatorias, Texto Único de Procedimientos Administrativos (TUPA) del Ministerio de Transportes y Comunicaciones, aprobado mediante Decreto Supremo N° 008-2002-MTC y sus modificaciones, Reglamento de Organización y Funciones del Ministerio de Transportes y Comunicaciones, aprobado por Decreto Supremo N° 021-2007-MTC. Texto Único Ordenado de la Ley N° 27444 – Ley del Procedimiento Administrativo.

La particularidad de este tipo de concesión, es la posibilidad de que se puedan prestar los servicios públicos, exceptuando los servicios de valor agregado o añadido. La finalidad de la concesión es que el solicitante, al menos deba cumplir con los requisitos exigidos para la prestación de al menos un servicio público de telecomunicaciones, desde el punto de vista jurídico, como desde el punto de vista técnico. Lo que nos permite concluir que una vez suscrito el contrato de concesión, el operador puede prestar otros servicios adicionales, solicitando el registro de estos nuevos servicios ante la autoridad competente, lo que puede entenderse como la primera aproximación a un modelo más amplio de títulos habilitantes que no está circunscrito al modelo de clasificación de servicios que se incorporan en la ley y que de alguna manera limita o restringe la inversión y la prestación de nuevos servicios atendiendo a la existencia de barreras de entrada atendiendo a la clasificación dada por el legislador peruano respecto a las formas de acceso al mercado como lo son la concesión la autorización y el permiso. (Zegarra, 2018, p. 83 y ss.).

Ahora bien, se debe partir de la premisa que, el artículo 121 del Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado por Decreto Supremo N° 020-2007-MTC, dispone que “Los servicios portadores, finales y de difusión de carácter público, se prestan bajo el régimen de concesión, la cual se otorga previo cumplimiento de los requisitos y trámites que establecen la Ley y el Reglamento, y se perfecciona por contrato escrito aprobado por el Titular del Ministerio”. El artículo 144 del mismo de la misma ley lista los requisitos necesarios que deben ser adjuntados a las solicitudes de otorgamiento de concesión; y que, el artículo 143 del Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, señala que “El otorgamiento de la concesión única confiere al solicitante la condición de concesionario para la prestación de los servicios públicos de telecomunicaciones establecidos en la legislación”.

Por lo anterior, se puede concluir que Perú no ha contemplado la posibilidad de incorporar nuevos modelos de ingreso al mercado, en el entendido que se sigue en presencia de un contrato suscrito con el Estado para la prestación de Servicios de Telecomunicaciones,

sujeto a un procedimiento reglado y previa presentación de un conjunto de requisitos que se precisan a continuación:

1. Hoja de datos personales y declaración jurada del representante legal y/o accionistas de ser el caso.
2. Perfil del proyecto técnico para la prestación del servicio solicitado, autorizado por un ingeniero colegiado hábil de la especialidad; asimismo, deberá adjuntar una Declaración Jurada del Ingeniero que autoriza dicho Perfil indicando que se encuentra habilitado.
3. Proyección de la inversión prevista para los primeros cinco (5) años y monto de la inversión inicial a ser ejecutada durante su primer año.
4. En caso de que la concesión involucre la provincia de Lima y/o la Provincia Constitucional del Callao, se deberá presentar:
 5. Carta Fianza (con vigencia de trece meses) equivalente al 15% de la inversión inicial de proyecto para asegurar el inicio de operaciones.
 6. Tratándose de teleservicios, el compromiso de atender, como mínimo, un distrito fuera de la Provincia de Lima y la Provincia Constitucional del Callao, asegurando la prestación del servicio en dicho distrito por el período que dure la concesión
 7. Pago por publicación de la resolución de concesión en el Diario Oficial El Peruano.
 8. Tratándose de personas jurídicas, deberá adjuntar una declaración jurada que acredite un capital social no menor a 10 UIT.
 9. En el caso de personas naturales y personas jurídicas sin fines de lucro deben acreditar ingresos anuales por el mismo monto, mediante Declaración Jurada del impuesto a la renta del ejercicio anterior a la presentación de la solicitud. Asimismo, deberán presentar el reporte del comportamiento de pago positivo emitido por una central de riesgo acreditada.

De los anteriores requisitos, se puede concluir que se sigue conservando la misma ritualidad o criterios previstos para la concesión tradicional, sin que medie una simplificación o mínima intervención de la Administración, como se evidencia en el procedimiento previsto en las leyes y decretos reglamentarios de la Ley peruana de telecomunicaciones, que se detallan a continuación:

1. Presentación de la solicitud con los requisitos formales.
2. Verificación del cumplimiento de los requisitos formales (evaluación legal), en caso de faltar algún requisito se otorga un plazo de diez (10) días hábiles para subsanar la omisión.
3. Habiendo subsanado lo requerido el Ministerio ordena al solicitante en un plazo de diez (10) días calendario la publicación de un extracto de la solicitud en el Diario Oficial El Peruano y en otro de circulación nacional, los cuales serán remitidos al Ministerio en un plazo no mayor a cinco (5) días hábiles.
4. Análisis integral de la solicitud (evaluación técnica), de ser necesaria

información adicional, el Ministerio la solicitará otorgando un plazo no mayor a cinco (5) días hábiles prorrogables.

5. El informe favorable de la DGCC y los actuados correspondientes se remiten a la Oficina General de Asesoría Jurídica para su verificación. Dicha Oficina General elevará los actuados al Despacho del Viceministro de Comunicaciones para que luego eleve los actuados al Ministro para la emisión de la Resolución Ministerial que otorga la concesión y aprueba el Contrato de Concesión.

Asimismo, es conveniente precisar que esta concesión tiene una vigencia de 20 años contados desde la suscripción del contrato y en lo que respecta a los servicios adicionales que se presten de manera adicional por parte del operador, estarán sujetos al mismo plazo otorgado en la concesión, teniendo como área para la prestación de los servicios el territorio de la República de Perú.

Si bien se habla de una concesión general para la prestación de los servicios de telecomunicaciones, denota que siguen vigentes ciertas restricciones a la competencia y no puede predicar un marco armónico de cara a la convergencia para la prestación de nuevos servicios.

La gran pregunta que surge ¿cuál es la diferencia que se puede dar entre este modelo de concesión única, respecto al régimen de títulos habilitantes previstos en la legislación peruana? y si este modelo previsto de autorizaciones, licencias y permisos, deben mantenerse, atendiendo a la experiencia de otros países, donde la liberación plena de los servicios y la inclusión de habilitaciones generales ha dinamizado el mercado. Es conveniente, en todo caso que se revise tal como se hizo en el contexto europeo, la existencia de un mercado de telecomunicaciones y va más allá de la clasificación de los servicios públicos comunicaciones, sino el reconocimiento de un mercado de comunicaciones.

Efectuada a una revisión de los diversos proyectos que han sido presentados para actualizar el Decreto Supremo N° 013-93-TCC de 28 de abril de 1993, teniendo como ejemplo el presentado por William Alfonso Monterola Abregú "Año de la Lucha Contra la Corrupción y la Impunidad" en el 2019, simplifican la clasificación existente resto a los servicios de telecomunicaciones, pero no hace alusión al mercado de las telecomunicaciones, atendiendo al reconocimiento de la convergencia como fenómeno técnico, económico y jurídico y de su incidencia en la transformación del sector de las telecomunicaciones al sector de las tecnologías de la información y las comunicaciones y que el modelo vigente debe dar paso a los nuevos modelos de habilitación para la prestación de los servicios que se demandan en la sociedad de la información y las comunicaciones, a pesar de que la contenga como un principio que inspira la Ley de Telecomunicaciones, que es la libre competencia.

A modo de conclusión, lo que se ha indicado y desarrollado a lo largo de este escrito, nos permite afirmar que pueden recurrirse a otro tipo de técnicas o instrumentos diferentes a la concesión para la prestación de los servicios de comunicaciones, donde se garantice no solo se garantice la esencia misma de servicio público, sino que se permita el ingreso de la inversión, de nuevos servicios y de esta manera la satisfacción de los derechos de los usuarios, sin que el Estado puedan verificar y monitorear de forma efectiva tanto los servicios como las redes que se desplieguen para su prestación (Zegarra, 2005).

CONCLUSIONES

A lo largo del documento académico se efectuó una revisión de la evolución y

transformación que desde el proceso de liberalización y que tiene una incidencia en la transformación de los títulos habilitantes y la forma como se accede al mercado. Es así como, en un principio se consideró conveniente atendiendo al modelo vigente de clasificación de los servicios y redes de telecomunicaciones, lo que configuraba que para poder prestar cada uno de estos servicios era necesario establecer un régimen de concesiones o licencias para la prestación del determinado servicio.

La introducción de la competencia y por consiguiente la construcción paulatina del mercado de las telecomunicaciones, trajo consigo una revisión del modelo vigente para garantizar la libertad de concurrencia y participación de nuevos agentes en el mercado, sumado al fenómeno de la convergencia que dinamizó el mercado desde el punto técnico, económico y jurídico, derivando en la respuesta desde el punto de vista regulatorio en la revisión del modelo de ingreso al mercado como una gran barrera por los costos asociados al mismo.

Es así como se efectuó una revisión del modelo diseñado en la Unión Europea y como este modelo no solo permeó las legislaciones como la colombiana, que desde el año 2007, empezó a gestar un modelo de legislación convergente y nuevas formas de ingreso al mercado, que se consolida con la expedición de la Ley 1341 de 2009 y con ella la incorporación de la Habilitación General y el Registro TIC, acompañado de un Régimen de Transición para que los proveedores de redes y servicios se acogieron al nuevo modelo, que finalmente bajo se amplió al sector audiovisual en la Ley 1978 de 2019.

Ahora bien, el nuevo modelo de habilitación general, no implica la pérdida de la titularidad del servicio o la desnaturalización del servicio de telecomunicaciones, sino que conforme a la liberalización el papel del Estado se transforma y se requiere del concurso de los operadores para la prestación de los servicios y el acceso de los servicios a zonas remotas y poco rentables para la satisfacción de las necesidades de la colectividad.

El título habilitante general, no exige del pago de los proveedores de redes y servicios de comunicaciones por los servicios que prestan, de allí que deban abonar mensualmente el pago de una contribución por las actividades que realizan, destinadas para el fomento de los planes y proyectos previstos para el desarrollo del sector.

En lo que respecta al modelo peruano, se conserva la figura de la concesión, entendida como una concesión general para los servicios de telecomunicaciones, donde se cuenta con una participación de la administración del Estado, atendiendo a que estamos en presencia de un contrato. De allí que se invite a revisar los modelos foráneos, a la incidencia de la convergencia y de las nuevas dinámicas del mercado con el fin de determinar si el modelo sigue siendo oportuno o se debe acoger un modelo de Habilitación general, con todos los beneficios que puede derivar para el mercado y la transformación que se requiere en un entorno digital.

REFERENCIAS BIBLIOGRÁFICAS

Comunidades Europeas. (3 de marzo de 2002). Directiva 2002/20/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a la autorización de redes y servicios de comunicaciones electrónicas (Directiva autorización). Directiva de Autorización. Bruselas, Bélgica.

Congreso de la República de Colombia. (30 de julio de 2009). Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–,

se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Bogotá, Colombia.

Congreso de la República de Colombia. (25 de julio de 2019). Ley 1978 de 2019. *Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones*. Bogotá, Colombia.

De La Quadra-Salcedo, T. (2010). Reflexiones sobre el nuevo marco normativo de las tecnologías de la información y las comunicaciones en Colombia. En E. González López, L. Herrera Zapata, & S. Ortiz Laverde, *Comentarios a la Ley de Tecnologías de la Información y las Comunicaciones -TIC (Ley 1341 de 2009)* (pp. 23-61). Bogotá: Universidad Externado de Colombia.

De La Rosa, S. (2010). Habilitación Genera. Titularidad estatal y registro de proveedores para provisión de redes y servicios de telecomunicaciones. En E. G. (Director), L. M. Coordinadoras Herrera Zapata, & S. M. Ortiz Laverde, *Comentarios a la Ley de Tecnologías de la Información y las Comunicaciones - TIC (Ley 1341 de 2009)* (pp. 231-251). Bogotá: Universidad Externado de Colombia.

Departamento Nacional de Planeación. (2016). *El futuro del sector audiovisual en Colombia: necesidad de política pública y reformas normativas en el marco de la convergencia tecnológica y las tendencias del mercado, informe final*. Bogotá.

Fajardo Muriel, A. (2010). El espectro radioeléctrico en la Ley 1341 de 2009. En E. González López, L. M. Herrera Zapata, & S. M. Ortiz Laverde, *Comentarios a la Ley de la Información y las Comunicaciones- TIC (Ley 1341 de 2009)* (pp. 405-440). Bogotá: Universidad Externado de Colombia.

Guerra De la Espriella, M. d. (2010). La Ley de Tecnologías de la Información y las Comunicaciones (Ley 1341 de 2009). En E. González López, L. Herrera Zapata, & S. M. Ortiz Laverde. Bogotá: Universidad Externado de Colombia.

Guerra de la Espriella, M. d., & Oviedo Arango, J. D. (abril de 2011). *De las telecomunicaciones a las TIC: Ley de TIC de Colombia (L1341/09)*. CEPAL - Serie Estudios y perspectivas - Colombia - N° 22. Bogotá, Colombia: Cepal.

Jefatura de Estado. (24 de abril de 1998). Ley 11/1998, General de Telecomunicaciones. Madrid, Madrid, España.

Jefatura del Estado. (3 de noviembre de 2003). Ley 32/2003, General de Telecomunicaciones. Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Madrid, Madrid, España.

Intven, H., & Tétrault, M. (2000). *MANUAL DE REGLAMENTACIÓN DE LAS TELECOMUNICACIONES*. Módulo 2. Licencias de servicios de telecomunicaciones. Washington: infoDEV.

Laguna De Paz, J. C. (2010). *Telecomunicaciones: Regulación y Mercado*. Tercera edición ampliada, reformada y actualizada. Cizur Menor (Navarra): Thomson Reuters.

Lavilla Rubira, J. (2004). Artículo 5. Principios aplicables. En T. De la Quadra-Salcedo, & E. García de Enterría, *Comentarios a la Ley de Telecomunicaciones Ley 31/2003, De 3 de noviembre* (pp. 81-86). Bogotá: Thomson- Civitas.

Lavilla Rubira, J. (2004). Artículo 6. Requisitos exigibles para la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas. En E. García de Enterría, & T. De la Quadra-Salcedo, *Comentarios a la Ley General de Telecomunicaciones Ley 32/2003, de 3 de Noviembre* (pp. 86-104). Bogotá: Thomson-Civitas.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). Exposición de motivos "Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones - TIC, se distribuyen competencias, se suprime la Autoridad Nacional de Televisión, y se dictan otras disposiciones". Bogotá.

Ministro del Interior y de Justicia de la República de Colombia. (18 de diciembre de 2009). DECRETO 4948 DE 2009. Por el cual se reglamenta la habilitación general para la provisión de redes y servicios de telecomunicaciones y el registro de TIC. Bogotá, Colombia.

Montaña Plata, A. (2010). Tecnologías de la información y las comunicaciones y servicios públicos. Fundamentación de la intervención del Estado en el sector. En E. González López, L. M. Herrera Zapata, & S. M. Ortiz Laverde, *Comentarios a la Ley de Tecnologías de la Información y las Comunicaciones - TIC (Ley 1341 de 2009)* (pp. 173-195). Bogotá: Universidad Externado de Colombia.

Montero Pascual, J. (2007). *Derecho de las Telecomunicaciones*. Valencia: Tirant lo Blanch.

Ortiz Laverde, S. M. (2017). El regulador convergente. Ventajas y desventajas. La revisión de la experiencia del modelo del Reino Unido, México y Argentina de cara al nuevo regulador. En E. González López, L. Herrera Zapata, J. Murgueitio Cabrera, & S. M. Ortiz Laverde, *El Ecosistema Digital y las Autoridades de Regulación de los Sectores Audiovisual y TIC* (pp. 637-687). Bogotá: Universidad Externado de Colombia.

Parlamento y Consejo Europeo. (10 de abril de 1997). Directiva 97/13/ce del Parlamento Europeo y del Consejo de 10 de abril de 1997 relativa a un marco común en materia de autorizaciones generales y licencias individuales en el ámbito de los servicios de telecomunicaciones. *Directiva 97/13/ce del Parlamento Europeo y del Consejo*. Bruselas, Bélgica.

Parlamento Europeo y Consejo Europeo. (11 de diciembre de 2018). Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo de 11 de diciembre de 2018. *Por la que se establece el Código Europeo de las Comunicaciones Electrónicas*. Bruselas, Bélgica.

Presidencia de la República de Colombia. (31 de julio de 2007). Decreto 2870 de 2007. *Por medio del cual se adoptan medidas para facilitar la Convergencia de los servicios y redes en materia de Telecomunicaciones*. Bogotá, Colombia.

Saura Fructuoso, C. (2015). Análisis general de las técnicas de intervención del Estado en la economía. *Revista Digital de Derecho Administrativo* (14), 27-43.

Zegarra Valdivia, D. (2005). *Servicio Público y Regulación Marco Institucional de las Telecomunicaciones en el Perú*. Lima: Palestra.

Zegarra Valdivia, D. (2018). *Introducción al derecho de las Telecomunicaciones*. Lima: Pontificia Universidad Católica del Perú. Fondo Editorial.



REGULACIÓN PARA LA COMPETENCIA EN EL MERCADO DE LAS TELECOMUNICACIONES EN COSTA RICA. UN CAMBIO DE PARADIGMA.

REGULATION FOR COMPETITION IN THE TELECOMMUNICATIONS MARKET IN COSTA RICA. A CHANGE OF PARADIGM.

LUIS A. ORTIZ ZAMORA¹
GLORIANA ALVARADO LEÓN²

RESUMEN

En el marco del décimo aniversario de la apertura del mercado de telecomunicaciones en Costa Rica, se hace relevante mirar hacia atrás y valorar el camino recorrido hasta ahora. Esta apertura ha presentado, desde luego, una serie de desafíos; empero, también ha confirmado la importancia que tienen las potestades atribuidas a la Superintendencia de Telecomunicaciones (SUTEL) para promover la competencia. Con todo, aún nos encontramos en un proceso de transición que no ha culminado, pues sólo ciertos servicios han sido declarados en competencia efectiva, lo cual representa un enorme reto ante el despliegue de nuevas tecnologías.

PALABRAS CLAVE

Apertura del mercado de las telecomunicaciones | Convergencia y neutralidad tecnológica | Regulación para la competencia | Mercado de las telecomunicaciones | Concentración de mercado.

ABSTRACT

Within the scope of the tenth anniversary since the telecommunications market opened in Costa Rica, it is relevant to look back and assess the path traveled until now. Certainly, this process has presented many challenges; however, it has also confirmed the significance of the powers conferred to the Superintendency of Telecommunications (SUTEL) to promote competition. Nonetheless, to date, there is a transition process that has not yet been completed. This poses an enormous challenge regarding the deployment of new technologies considering that only some services have been declared in effective competition.

KEYWORDS

Telecommunications market opening | Convergence and technology neutrality | Regulation for competition | Telecommunications market | Market concentration.

-
- 1 Presidente de la Asociación Iberoamericana de Estudios de Regulación (ASIER). Profesor de la Universidad Escuela Libre de Derecho (Costa Rica), así como de los Cursos de Regulación y Competencia de la Universidad de Valladolid (España) y del Programa Regional de Especialización en Regulación Económica Aplicada, Instituto Centroamericano de Administración Pública. Presidente del Jurado de las Pruebas de Grado de la Maestría en Derecho Público de la Universidad Autónoma de Centroamérica. Reconocido por el Directorio Legal Who's Who Legal como uno de los cuatro expertos más reconocidos en Derecho Administrativo de América Central y por el Directorio Chambers and Partners como abogado recomendado en las áreas de Derecho Público, Telecomunicaciones e Infraestructura. Experto de la Comisión Regional de Interconexión Eléctrica (CRIEE). Árbitro del Centro Iberoamericano de Arbitraje (CIAR).
- 2 Abogada. Máster en Derecho de las Telecomunicaciones y Tecnologías de la Información y Comunicación por la Universidad Carlos III de Madrid. Máster en Derecho Público, Universidad Carlos III de Madrid. Miembro de la Asociación Iberoamericana de Estudios de Regulación (ASIER).

CONTENIDO

I. Introducción; II. La Apertura Del Mercado De Las Telecomunicaciones; III. Convergencia y Neutralidad Tecnológica; IV. El Papel Del Regulador; A. Funciones Del Regulador Para Promover La Competencia; B. Gestión De Recursos Escasos: El Espectro Radioeléctrico; C. Tarifas y Precios; D. Control Preventivo de las Concentraciones; V. El Servicio Universal; VI. Régimen de Acceso e interconexión; VII. Conclusión; VIII. Referencias.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 3 de junio de 2021 y aprobado para su publicación el 16 de agosto de 2021.

I. INTRODUCCIÓN

Alguna vez le preguntaron al famoso economista inglés John Hicks: ¿Qué es el monopolio? A lo que el Premio Nobel contestó: La vida tranquila (Hicks, 1935).

En cambio, la competencia, como dijera en su momento el famoso juez americano Learned Hand: es un constante estrés; la falta de competencia actúa como un narcótico, mientras que la rivalidad es el estimulante del progreso económico [Estados Unidos c. Aluminium Co. of America, 148 F.2d 416, 427 (2d Cir. 1945)].

Es así, precisamente gracias a esa preocupación por no perder sus clientes, que el empresario se esfuerza en hacer todo lo posible para reducir sus costos, ofrecer precios más bajos, mejorar la calidad del servicio y el trato al cliente, todo lo cual genera dos beneficios: el primero en la producción y el otro en la distribución de lo producido; es decir, el primero en el pastel y el segundo en el que se lo come (Ordóñez, 2000).

Pues bien, hace no mucho tiempo en Costa Rica había listas de espera para adquirir una línea celular y tocaba esperar varios meses por una conexión de Internet para la casa u oficina. Sin embargo, con la apertura del mercado de las telecomunicaciones, a partir del año 2011, todo esto cambió. No es cliché ni hipérbole, tampoco es mera retórica ni hipótesis falaz, es la realidad que los hechos puros y duros demuestran en nuestro mercado de las telecomunicaciones, finalmente abierto a la competencia.

Ahora, como con acierto ha señalado Zegarra (2005), la introducción de la competencia plantea el reto de que las empresas que son dominantes en los mercados liberalizados o en aquellos en los que se ha introducido competencia, sin haberse desprendido el Estado de ellas, abusen de su posición de dominio y conviertan en monopolio de hecho lo que antes era un monopolio de derecho. Y, en efecto, algo similar a lo que plantea el Profesor Zegarra sucede en Costa Rica, donde el otrora monopolista, Instituto Costarricense de Electricidad (ICE), empresa estatal, en algunas ocasiones ha abusado de su posición dominante.

Viene a bien repasar, por tanto, cuál ha sido la fórmula jurídica que ha implementado Costa Rica para pasar de un monopolio legal vigente por más de 60 años a un mercado en competencia, así como también para, transcurridos 10 años desde la apertura del mercado de telecomunicaciones, hacer balance y dejar al descubierto sus virtudes, pero también sus errores (Ariño, Cuétara, & Noriega, 2005).

Para tales efectos, pasaremos revista de cómo se dio el proceso de apertura, así como también analizaremos cuáles han sido las piedras angulares del cambio de paradigma de monopolio a mercado en competencia, a saber: la convergencia y la neutralidad tecnológica, el papel del regulador, el servicio universal y el régimen de acceso e

interconexión. Finalmente, haremos un balance de los 10 años transcurridos desde el cambio de paradigma operado.

II. LA APERTURA DEL MERCADO DE LAS TELECOMUNICACIONES

Históricamente, el servicio de las telecomunicaciones en Costa Rica lo prestaba el Estado en un régimen de monopolio legal. En su artículo 121, inciso 14, la Constitución Política de la República de Costa Rica enumera un listado de los bienes que no pueden salir definitivamente del dominio del Estado, entre los cuales está el espectro radioeléctrico y las posibles modalidades para su explotación. Así, para explotar el espectro radioeléctrico es necesario contar con una concesión otorgada directamente por la Asamblea Legislativa, o bien por el Poder Ejecutivo de conformidad con una ley marco que lo habilite para tal efecto, concesión que sólo el Instituto Costarricense de Electricidad (ICE) y Radiográfica Costarricense (RACSA) ostentaron durante más de 60 años.

Para el año 2006, tan solo un año antes de que el país tomara la decisión de llevar adelante la apertura del mercado de las telecomunicaciones, de acuerdo con datos del Instituto Nacional de Estadísticas y Censos (INEC), cerca de la quinta parte de los hogares del país (aproximadamente 220.000) no tenían teléfono y el 35% no tenía ningún teléfono celular. En cuanto a los servicios de Internet, menos de una tercera parte de los hogares tenía computadora y sólo el 10% tenía conexión a Internet en la casa.

A mayor abundamiento, según un estudio de la Comisión Asesora en Alta Tecnología (Hewitt, 2006), entre la población más pobre del país la brecha digital era mucho más profunda. Así, mientras que en el quintil de los hogares más ricos del país, un 86% tenía teléfono fijo y un 83% al menos un teléfono celular; en el quintil más pobre, esos porcentajes eran de 42% y 17%, respectivamente, a la vez que, solo un 6% tenía computadora en la casa y un 1% conexión a Internet.

En general, de acuerdo con datos de la Unión Internacional de las Telecomunicaciones (UIT) del 2005, la densidad telefónica en Costa Rica apenas si alcanzaba el promedio mundial, mientras que su densidad de telefonía celular era significativamente menor al promedio mundial. Si nos comparábamos con otros 35 países de América, nuestro país se encontraba entre los que tenían densidades telefónicas más bajas (posición 13 entre 36 países), así como también entre los que menor ritmo de crecimiento de la telefonía celular tuvieron durante la primera mitad de la década del 2000 (posición 18 entre 36 países) (Autoridad Reguladora de los Servicios Públicos, 2007).

Ahora bien, fue el Tratado de Libre Comercio entre República Dominicana, Centroamérica y Estados Unidos (TLC), aprobado por Costa Rica mediante un referendo celebrado el 7 de octubre del 2007, el que propulsó y formalizó el compromiso del país hacia una apertura selectiva del mercado de las telecomunicaciones, específicamente en telefonía móvil, Internet y servicios empresariales de banda ancha.

A fin de implementar el TLC, se aprobó un paquete normativo que estableció el marco jurídico necesario para cumplir con los compromisos adquiridos, a saber: Ley N°8642, Ley General de Telecomunicaciones (LGT) y Ley N° 8860, Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector de las Telecomunicaciones (LFMEPST). Posteriormente, en el año 2011, se cumplió esa primera fase de apertura con la entrada de 2 nuevos operadores al mercado costarricense, adjudicatarios de un concurso público promovido por el gobierno de Costa Rica.

Así, pues, el mercado de las telecomunicaciones en Costa Rica se rige por la LGT, cuyo principio esencial es la prestación del servicio en un régimen de competencia efectiva

y no discriminación. De esta forma, se han creado mecanismos adecuados para que compitan en condiciones iguales, operadores y proveedores, así como también el principio del trato menos favorable a cualquier operador, proveedor o usuario público o privado. Por tanto, ya no se trata del modelo tradicional de regulación que ha presidido los grandes servicios públicos, en que el regulador sustituía al mercado y se hacía cargo de la mayoría de las decisiones, sino de un modelo que promueve la competencia y al mismo tiempo protege los intereses de los usuarios (Ubico, 2008).

Complementa a este cuerpo normativo la LFMEPST, que creó formalmente el Sector Telecomunicaciones y separó los tres roles que le corresponden al Estado: rector, regulador y operador del mercado. El incumbente (ICE) –antiguo monopolista- fue fortalecido por medio de esta normativa, a la vez que se le otorgaron mayores facultades y libertades para su desarrollo como un operador más en un mercado de competencia, por lo que debe cumplir, al igual que los demás operadores, con las disposiciones legales vigentes.

Se creó, además, un tercero imparcial –Superintendencia de Telecomunicaciones (SUTEL)-, como agencia reguladora independiente del Gobierno, para vigilar la competencia en el mercado, regular la actividad de los operadores, vigilar el correcto funcionamiento y prestación del servicio, así como sancionar en caso de faltas que pongan en riesgo la competencia del mercado.

Finalmente, se creó el Viceministerio de Telecomunicaciones del Ministerio de Ciencia y Tecnología que, en su carácter de rector y en conjunto con la SUTEL, debe promover la competencia efectiva en el mercado e incentivar la inversión.

III. CONVERGENCIA Y NEUTRALIDAD TECNOLÓGICA

La LGT fue más allá del compromiso original de Costa Rica conforme al Anexo 13 del TLC. En efecto, además de instaurar la apertura en cuanto a telefonía móvil, Internet y servicios empresariales de banda ancha, se incluyó dentro de su texto la noción de convergencia, a partir de la cual se entiende comprendida la oferta múltiple de redes y servicios; esto es, la posibilidad de ofrecer, a través de una misma red, múltiples servicios, lo que permite que la información sea interactiva e interoperable con cualquier tipo de red.

Una de las características más importantes de la regulación en convergencia es la eliminación de la clasificación de los servicios de telecomunicaciones. Por ello, en este contexto no tiene sentido restringir los títulos habilitantes para el funcionamiento de los operadores a determinados tipos de servicios de telecomunicaciones, pues lo propio es que cada día surjan nuevos servicios y varíen los que ya existían, de ahí que, los servicios no pueden sujetarse a una descripción legal ni a un tipo de tecnología.

Tampoco tiene sentido restringir los títulos habilitantes a la oferta de un único servicio, toda vez que las tecnologías actuales permiten que, a través de la misma red y equipo terminal, se puedan ofrecer múltiples servicios. Es por ello que, la LGT prevé que los operadores de redes públicas y proveedores de servicios pueden ampliar la oferta de servicios que prestan con tan solo informar previamente a la SUTEL. Con ello, la LGT adopta el principio de neutralidad tecnológica, mismo que resulta vital para la regulación de las telecomunicaciones en un contexto de convergencia. En este sentido, la LGT establece la posibilidad que tienen los operadores de redes y proveedores de servicios de telecomunicaciones para escoger las tecnologías por utilizar, siempre que estas dispongan de estándares comunes y garantizados, cumplan los requerimientos necesarios para satisfacer las metas y los objetivos de política sectorial y se garanticen,

en forma adecuada, las condiciones de calidad y precio.

Siguiendo esta filosofía, la LGT clasifica a los títulos habilitantes en tres categorías:

Concesiones: para el uso y explotación de frecuencias del espectro radioeléctrico.

Autorizaciones: para operar y explotar las redes públicas y privadas de telecomunicaciones que no requieran del uso del espectro radioeléctrico, para prestar servicios de telecomunicaciones disponibles al público por medio de redes públicas de telecomunicaciones que no se encuentren bajo su operación, y para operar redes privadas de telecomunicaciones que no requieran uso del espectro radioeléctrico.

Permisos: para el uso de las bandas de frecuencias para operaciones de carácter temporal, experimental, científico, servicios de radiocomunicación privada, banda ciudadana, de radioaficionados o redes de telemetría de instituciones públicas, y para seguridad, socorro y emergencia.

IV. EL PAPEL DE REGULADOR

SUTEL es el órgano del Estado costarricense al que principalmente le corresponde promover la competencia efectiva en el mercado de las telecomunicaciones, pues debe procurar que ningún operador de redes o proveedor de servicios de telecomunicaciones manipule el mercado de manera tal que pueda modificar a su favor y en perjuicio de los demás, las condiciones de mercado, restringiendo el funcionamiento eficiente de este, con daño a los usuarios. Ahora bien, una vez que el mercado es declarado en competencia efectiva, su función pasa a ser ex post. En este sentido, en la recientemente aprobada Ley N° 9736, Ley de Fortalecimiento de las Autoridades de Competencia de Costa Rica (LFACCR), se ratifica lo que la LGT ya había establecido de previo, sea que, en el caso específico del sector telecomunicaciones, es a la SUTEL a la que le corresponde la defensa y promoción de la competencia y libre concurrencia en el mercado de las telecomunicaciones, otorgándosele, de esta manera, la competencia exclusiva y excluyente en el sector.

De conformidad con ello, le corresponde a la SUTEL aplicar los mecanismos necesarios para garantizar la igualdad de condiciones de los operadores del mercado a través de todas las facultades que la legislación establece. Para ese fin, debe aplicar el principio constitucional de igualdad –artículo 33 de la Constitución Política de Costa Rica-, pues es este precisamente el que permite que vía regulatoria se impongan o supriman facultades a los operadores del mercado que cuenten con mayores o menores beneficios, en un tratamiento desigual con el uso de medidas preventivas, según lo amerite (regulación asimétrica).

De esta forma, el ordenamiento jurídico de las telecomunicaciones, a la luz del principio constitucional de igualdad, fue ideado para permitir y promover una regulación asimétrica hasta tanto no se esté en presencia de un mercado estable y maduro que no requiera la discriminación positiva, pues no basta con permitir la libertad de entrada de los operadores, así como el acceso a las redes e infraestructuras, si no se cuenta con los mecanismos legales que les permitan a los entrantes desenvolverse en un mercado que garantice condiciones óptimas de igualdad y estabilidad. Como bien ha señalado la doctrina:

...el principio de libre competencia no exige sólo que cualesquiera interesados puedan acceder a la condición de operador en un mercado determinado. Además es necesario que, una vez que aquéllos han accedido al mismo, y como condición

para la libertad y efectividad de la competencia entre los partícipes, todos ellos se hallen situados en una posición de igualdad. Pues bien, la LGTT trata de satisfacer asimismo esta exigencia, sometiendo con carácter general, a todos los operadores a las mismas condiciones, lo cual se asegura mediante el carácter normativo de las mismas y la consiguiente imposibilidad de que, en principio –y al contrario de los que ocurriría en la regulación anterior en el caso de las licencias individuales, la Administración pueda imponer condiciones particulares a determinados operadores. Ello no obstante, la efectividad del principio de igualdad –condición imprescindible para que la competencia pueda calificarse como libre- exige tratar desigualmente a los desiguales. Por ello, y asumiendo la realidad de que el punto de partida no es siempre el mismo, la LGTT permite la imposición de condiciones y obligaciones específicas a determinados operadores, pero siempre con la finalidad de asegurar la no distorsión de la libre competencia. (..) La imposición de obligaciones específicas a los operadores con poder significativo en el mercado, que se condiciona a la existencia de un entorno de competencia efectiva en éste, de forma que aquellas han de suprimirse cuando se constate de la existencia de tal entorno. (Quadra, 2004).

Valga señalar que, en el mercado costarricense, sólo unos cuantos servicios han sido declarados en competencia efectiva por parte de la SUTEL, pero existe actualmente un proceso de transición que no ha culminado, pues el incumbente concentra más del 50% del espectro radioeléctrico disponible en el país, situación que obliga a la existencia de una regulación asimétrica para evitar la existencia de prácticas monopolísticas o abusos de posición de dominio.

A. FUNCIONES DEL REGULADOR PARA PROMOVER LA COMPETENCIA

Como ya dijimos, le corresponde a la SUTEL fomentar la competencia en el mercado de las telecomunicaciones, tanto con acciones afirmativas como con la imposición de obligaciones a los operadores con la finalidad de prevenir, evitar o suprimir una situación que conlleve como resultado la distorsión en el mercado y la afectación al servicio esencial que se presta, así como también por medio del ejercicio de su potestad sancionatoria (Chloe, Stewart, Sunstein, Vermule, & Herz, 2011).

Específicamente, le corresponde el ejercicio de las siguientes funciones: i) Promover los principios de competencia en el mercado nacional de telecomunicaciones; ii) Analizar el grado de competencia efectiva en los mercados, iii) Determinar cuándo las operaciones o los actos que se ejecuten o celebren fuera del país, por parte de los operadores o proveedores, pueden afectar la competencia efectiva en el mercado nacional, iv) Garantizar el acceso de los operadores y proveedores al mercado de telecomunicaciones en condiciones razonables y no discriminatorias, v) Garantizar el acceso a las instalaciones esenciales en condiciones equitativas y no discriminatorias, vi) Evitar los abusos y las prácticas monopolísticas por parte de operadores o proveedores en el mercado, vii) Conocer de oficio o por denuncia, así como corregir o sancionar, cuando proceda, las prácticas monopolísticas cometidas por los operadores o proveedores que tengan por objeto o efecto limitar, disminuir o eliminar la competencia en el mercado de las telecomunicaciones.

Le concierne, además, el ejercicio de otras funciones que de manera directa o indirecta tienen incidencia en la regulación para la competencia, como lo son, por ejemplo: la función normativa, la función sancionatoria, la fijación de tarifas máximas, el otorgamiento de títulos habilitantes cuando corresponda, y el control preventivo de concentraciones, entre otras.

La SUTEL también se encuentra habilitada para solicitar la información que considere pertinente a los operadores, quienes a su vez están obligados a proporcionarla, cuando considere que existe o puede existir una práctica monopolística que se debe corregir o prevenir, o bien, que se deben resguardar los derechos de los usuarios. De manera posterior a la solicitud de información, la SUTEL debe analizar y pronunciarse sobre los elementos obtenidos y valorar si existen o no prácticas monopolísticas absolutas o relativas a la luz de la LGT.

De igual forma, le corresponde analizar el grado de competencia efectiva en los mercados de telecomunicaciones. Para ello, debe analizar y clasificar los mercados existentes y establecer, con base en la normativa de telecomunicaciones, la existencia o no de un mercado en competencia, pues a partir de ello puede seleccionar - previa motivación - a los operadores que tienen un poder significativo de mercado y señalar aquellos mercados que requieren de mayor o menor regulación porque su estabilidad está o dejó de estar en riesgo.

Una vez analizados los mercados de referencia y seleccionado el operador con poder significativo de mercado - siempre y cuando el mercado no haya sido declarado en competencia efectiva - corresponde entonces la imposición de las obligaciones a ese operador, con la finalidad de garantizar una competencia en el mercado y evitar la distorsión del mismo, dentro de las cuales, según el artículo 75 del Reglamento a la LGT, pueden citarse las siguientes: i) abstenerse de realizar prácticas monopolísticas; ii) dar libre acceso a las redes y a los servicios que por medio de éstas se prestan, en condiciones razonables y de manera oportuna.

Específicamente, el Consejo de la SUTEL definió por primera vez los mercados relevantes y los operadores importantes a través de su resolución No. RCS-307-2009, de 9 de diciembre de 2009, definiendo 18 mercados relevantes y un único operador dominante en todos ellos, el ICE y sus empresas (Grupo ICE), pues para ese momento, era el único operador presente en el mercado.

A pesar de lo anterior, y previendo que la apertura del mercado de las telecomunicaciones estaba próxima a ocurrir, se le impusieron algunas medidas y obligaciones tales como: hacer pública cierta información que la SUTEL le solicitará; mantener la contabilidad de costes por separado; someter el esquema de regulación y determinación de cargos de acceso e interconexión orientados a costos; comunicar previamente los precios y condiciones aplicables a los servicios ofrecidos; dar libre acceso a sus redes en forma oportuna y en condiciones razonables y no discriminatorias a otros operadores, proveedores y usuarios de servicios de telecomunicaciones, así como a los operadores y proveedores de servicios de información; facilitar el acceso oportuno a sus instalaciones esenciales y poner a disposición de los operadores y proveedores la información técnica relevante en relación con estas instalaciones; cumplir las obligaciones propias del régimen de acceso e interconexión; entre otros.

Como era de esperarse, con la apertura a la competencia, la situación de mercado varió, y por ello, precisamente, mediante la resolución RCS-245-SUTEL-2012, de 16 de agosto de 2012, se aprobaron los Lineamientos para la definición de mercados relevantes y operadores con poder significativo de mercado, los cuales deben incorporarse al respectivo estudio que se lleve a cabo en cada uno de los procesos que se utilizan para definir y analizar los mercados relevantes y operadores con poder significativo de mercado. Estos lineamientos constituyen criterios y técnicas internacionalmente reconocidas y, por tanto, deben considerarse incorporadas al ordenamiento jurídico costarricense, en adición y complemento a los parámetros legales y reglamentarios.

Dichos Lineamientos atienden, por supuesto, a la determinación de características o indicadores que a su vez permitan determinar un grado de competencia en el mercado, como lo son, por ejemplo, los criterios relacionados con la sustituibilidad de la demanda y de la oferta, así como establecimiento y determinación del área geográfica.

De esta manera, para determinar si un operador cuenta con poder significativo de mercado, debe analizarse la cuota de mercado, participaciones de mercado y sus tendencias, control de infraestructura y facilidades esenciales para el período en estudio, ventajas tecnológicas que no sean factiblemente adquiribles y proyectos de inversión de los operadores, así como control de canales de distribución, poder de negociación y compra, economía de escalas, entre otros.

B. GESTIÓN DE RECURSOS ESCASOS: EL ESPECTRO RADIOELÉCTRICO

El espectro radioeléctrico es el bien demanial esencial en la prestación del servicio de telecomunicaciones, protegido constitucional y legalmente mediante el artículo 121 inciso 14 de la Constitución Política, y el artículo 7 de la LGT, por lo que los servicios inalámbricos no pueden salir del dominio del Estado y para su explotación se debe contar con una concesión.

En este sentido, la Sala Constitucional, en su resolución número 4329 de 30 de marzo de 2011, sostuvo que el espectro radioeléctrico es un bien de dominio público, al indicar que las ondas etéreas forman parte del espectro que es un bien demanial perteneciente a la Nación; y, además, el Estado tiene el derecho y el deber de velar por la conservación del dominio público.

Asimismo, de acuerdo con el artículo 2, inciso g) de la LGT dicho bien es escaso, por lo cual, solamente una determinada cantidad de frecuencias pueden ser aprovechadas y explotadas, siendo así que su correcto uso se define a través del Plan Nacional de Atribución de Frecuencias (PNAF), mediante el cual se designan los usos de las bandas del espectro radioeléctrico.

Debido a que este es el bien que permite la prestación de los servicios de telecomunicaciones, su correcta explotación y distribución resulta de fundamental importancia, pues de ello va a depender de manera directa, el comportamiento del mercado y la correcta prestación del servicio. En razón de ello, le corresponde a la SUTEL la comprobación técnica de las emisiones radioeléctricas, así como la inspección, detección, identificación y eliminación de las interferencias perjudiciales. Asimismo, la SUTEL debe sancionar las conductas que puedan afectar la correcta gestión o explotación del espectro radioeléctrico y realizar los análisis correspondientes que le solicite el Poder Ejecutivo en relación con la distribución del espectro radioeléctrico, pudiendo denunciar situaciones de concentración, subutilización y mal uso de este.

Asimismo, no puede bajo ningún supuesto dejarse su gestión a discreción de las Administraciones públicas, sino que, por el contrario, los organismos administrativos que intervengan en su gestión deben valorar siempre, salvo excepción legal, la opinión del regulador, pues es éste el que tiene los conocimientos técnicos y puede, además, interpretar los parámetros legales con los que Costa Rica debe cumplir. Por tanto, toda la regulación que gire alrededor del espectro radioeléctrico debe ser tendiente a una correcta distribución por ser un bien escaso y esencial para la prestación de los servicios de telecomunicaciones, y además a la concreción de un mercado en competencia.

Ahora bien, en Costa Rica las funciones relacionadas con la correcta distribución del espectro radioeléctrico se ejercen de manera conjunta por la SUTEL y el Viceministerio

de Telecomunicaciones. De conformidad con el artículo 10 de la LGT, le corresponde: a) al Poder Ejecutivo dictar el PNAF, previa consideración de las recomendaciones de la Unión Internacional de Telecomunicaciones (UIT) y de la Comisión Interamericana de Telecomunicaciones (CITEL); así como la asignación, reasignación, o rescate de las frecuencias, de acuerdo con lo establecido en el PNAF, de manera objetiva, oportuna y no discriminatoria; b) a la SUTEL, por su parte, le corresponde la comprobación técnica de las emisiones radioeléctricas, así como la inspección, detección, identificación y eliminación de las interferencias perjudiciales.

En ambos casos, la SUTEL y el Poder Ejecutivo deben tener en cuenta los principios inspiradores del mercado de las telecomunicaciones, pues solo así se garantiza un correcto uso y una distribución equitativa del mismo. Con todo ello se busca, sin duda, según lo establece el artículo 8 de la LGT, optimizar su uso de acuerdo con las necesidades y las posibilidades que ofrezca la tecnología, garantizar una asignación justa, equitativa, independiente, transparente y no discriminatoria, así como también asegurar que la explotación de las frecuencias se realice de manera eficiente y sin perturbaciones producidas por interferencias perjudiciales.

En virtud de lo que viene señalado, queda claro entonces que una mala regulación del espectro radioeléctrico, o su mal aprovechamiento, puede tener incidencia y llegar a afectar de manera directa el comportamiento de los operadores y el mercado, toda vez que puede generar o permitir la creación de barreras de entrada o permitir abusos de poder dominante, entre otros.

En relación con la explotación del espectro radioeléctrico propiamente, resulta menester señalar que, según lo dispone el artículo 11 de la LGT, se debe contar con una concesión que habilite su uso, para lo cual se debe celebrar un procedimiento concursal instruido por la SUTEL que culmine con un acto de adjudicación a favor de algún operador. De conformidad con el artículo 12 del mismo cuerpo legal, le corresponde a la SUTEL, además, realizar los estudios de precios necesarios para determinar la necesidad y factibilidad del otorgamiento de las concesiones de conformidad con el Plan Nacional de Desarrollo de las Telecomunicaciones y las Políticas Sectoriales (PNDTPS).

Del mismo modo, le compete a la SUTEL llevar la información en el Registro de Telecomunicaciones, así como permitir o no la ampliación de servicios que prestan los operadores, pues si lo considera pertinente, ante la comunicación previa del operador interesado, de conformidad con el artículo 27 de la LGT, puede requerir información adicional o aclaraciones, dentro de los 15 días hábiles siguientes a la presentación, así como los ajustes que considere necesarios, a fin de que la prestación de los nuevos servicios se ajuste a lo previsto en esa Ley, a la concesión o autorización otorgada y al PNDTPS. El incumplimiento de la obligación de informar a la SUTEL implicará una sanción administrativa, de conformidad con lo dispuesto en los artículos 65 y 70 de la LGT.

Resulta entonces fundamental la participación de la SUTEL en relación con la gestión del espectro radioeléctrico, pues además de realizar las mediciones y vigilar su correcta explotación tiene un papel fundamental en su disposición al público, ya que le corresponde realizar los estudios de factibilidad y con ello debe tener presente la utilización de las bandas, analizar la situación de las frecuencias y el correcto uso de este bien, y promover de manera indirecta, con su gestión, la competencia en el mercado y la prestación efectiva del servicio de telecomunicaciones en estricto apego a los principios de universalidad y solidaridad.

En uso de esas facultades, la SUTEL, de previo a la licitación pública que permitió el ingreso de nuevos operadores móviles a Costa Rica, emitió su informe No. 251-SUTEL-2009 mediante el cual concluyó que, en aras de garantizar la competencia efectiva en el mercado de las telecomunicaciones y evitar una subutilización del bien, debía desconcentrarse el espectro para permitir el acceso de nuevos operadores y proveedores. Bajo esa premisa, pues, le recomendó al Poder Ejecutivo recuperar algunas de las bandas (pues todas estaban en manos del incumbente), para realizar una adecuada asignación, y permitir con ello el ingreso de nuevos operadores.

No obstante, actualmente, la concentración de espectro radioeléctrico advertida por la SUTEL desde el año 2009 se mantiene. En este sentido, como lo ha advertido Rivera (2000):

Entonces, lo primero que debemos entender, es que avanzar hacia el 5G es necesario para habilitar la revolución digital y la conectividad de las cosas y de sectores productivos, no tanto para mejorar en sí la conexión de las personas. Por ello, cuando pensemos en reducir la brecha digital o abarcar áreas rurales que requieren mejorar su cobertura no significa que es necesario ir al 5G sino más bien hay que fortalecer las redes actuales de 4G y la capilaridad de las redes fijas.

Entendido ese punto, ¿Cómo avanzamos hacia 5G en Costa Rica? Hay tres elementos centrales para trazar una hoja de ruta (que no la hay o por lo menos, no se ha dado a conocer abiertamente): el espectro radioeléctrico, la infraestructura pasiva o de soporte y la red de transmisión, es decir, el despliegue de fibra óptica a lo largo del país. Por la necesidad de extensión de cada punto, concentrémonos en el primero.

Contrario a las generaciones de tecnología móviles anteriores, el desarrollo pleno de 5G pasa por combinar diferentes frecuencias del espectro radioeléctrico: las bajas (por debajo de 1Ghz), las medias (de 1Ghz hasta 6Ghz) y las altas (arriba de 6Ghz). Los diferentes desarrollos de 5G van a requerir que las redes de telecomunicaciones combinen estas diversas bandas para optimizar las diferentes aplicaciones: aquellas que puedan requerir conectar grandes áreas como aplicaciones agrícolas o agro-alimentarias, otras que permitan asegurar en sitios críticos la ultra velocidad y la quasi eliminación de la latencia y otras que masifiquen la tecnología en las ciudades y poblados. Sin espectro no habrá 5G. En bandas altas, el MICITT está haciendo correctamente su tarea, y muestra de ello, la reciente propuesta de reforma al Plan Nacional de Atribución de Frecuencias.

No obstante, en Costa Rica, algunas de las bandas denominadas centrales para el desarrollo de 5G se encuentran concentradas en el Grupo ICE. Esto sucede con la banda de 3.5Ghz, banda que por internacionalmente se ha identificado como pívot en la estrategia de despliegue de 5G. Esto implica que desde ya, los dispositivos tanto para personas, celulares, tablets y wearables (dispositivos "vestibles") así como las "cosas" propiamente, se están produciendo para funcionar en esta banda.

Permítanme ser claro: si el Gobierno -el MICITT- no asume con determinación el recuperar esta banda para ponerla a disposición del mercado, bajo los mecanismos establecidos por la Ley General de Telecomunicaciones, solo podemos tener dos escenarios posibles de 5G en el país: o un desarrollo

en monopolio del 5G o un desarrollo forzosamente compartido sobre la base de un único operador mayorista. Es nuestro criterio que ninguna de estas opciones asegura que el país adopte de forma competitiva y oportuna la tecnología en beneficio de la sociedad, los consumidores y los sectores productivos.

Similar situación se vivió en el año 2013 con el desarrollo de la 4G, específicamente en relación con la banda 2600 -banda por excelencia para el despliegue de la red 4G-. Lamentablemente, enfrentado con el caso de acaparamiento de la banda idónea del espectro radioeléctrico por parte del operador incumbente (ICE), el Tribunal Contencioso Administrativo y Civil de Hacienda, en su Res. N°2343-2013 de las nueve horas y cincuenta minutos del treinta de octubre del dos mil trece, consideró que, si bien el caso presentado por el operador entrante gozaba de apariencia de buen derecho y efectivamente se había demostrado la existencia de un daño potencial o eventual que se le podría causar por la desventaja competitiva en que quedaba con relación al incumbente, la balanza debía inclinarse en favor del interés público, pues en la palestra de los intereses en juego se encontraba la entidad pública estatal (incumbente) (Ortiz, 2021).

Como se puede comprobar, el Tribunal asimiló el interés público con el interés de la Administración Pública, aún y cuando están claramente delimitados en el artículo 113 de nuestra Ley General de la Administración Pública que dice:

- Artículo 113.- 1. El servidor público deberá desempeñar sus funciones de modo que satisfagan primordialmente el interés público, el cual será considerado como la expresión de los intereses individuales coincidentes de los administrados.
2. El interés público prevalecerá sobre el interés de la Administración Pública cuando pueda estar en conflicto.
3. En la apreciación del interés público se tendrá en cuenta, en primer lugar, los valores de seguridad jurídica y justicia para la comunidad y el individuo, a los que no puede en ningún caso anteponerse la mera conveniencia.

Y es que, cuando el país adoptó la decisión de liberalizar el mercado de las telecomunicaciones se inclinó por un modelo que busca promover la competencia efectiva como medio para aumentar la disponibilidad de los servicios, mejorar su calidad y asegurar precios asequibles. Consecuentemente, el fin de la apertura consistió en beneficiar a los usuarios, quienes tienen derecho a obtener servicios de telecomunicaciones de calidad, con más y mejor cobertura, más alternativas -donde su poder de elección de operador debe privar y ser respetado-, en forma continua, no discriminatoria, eficiente y a un precio que corresponda al precio de mercado.

Por tanto, es claro que el interés público prevalente en el mercado de las telecomunicaciones es la correcta prestación del servicio en aras de garantizar el acceso universal, mas no la protección del operador estatal tan solo porque administra fondos públicos, pues las empresas privadas, al igual que el incumbente, coadyuvan con la prestación del servicio y no son el enemigo a vencer (Ariño, 2004).

C. TARIFAS Y PRECIOS

Con ocasión del análisis de mercado que le corresponde realizar, SUTEL debe determinar si existe competencia efectiva, para con ello definir la procedencia o no de la fijación de las tarifas. En concreto, en caso de la existencia de competencia efectiva, debe dejar los precios al mercado; pero, en caso contrario, cuando determina que no existen las

condiciones suficientes para asegurar una competencia efectiva, debe intervenir fijando la tarifa mediante el sistema de tope o price cap.

En un principio, mediante su resolución RCS-615-2009, la SUTEL definió como tarifas máximas las emitidas por la Autoridad Reguladora de los Servicios Públicos (ARESEP), permitiendo con ello un avance en el proceso de la transición a la competencia efectiva, puesto que con ello se permitió la incursión de nuevos operadores al mercado y se evitó la creación de barreras de entrada de este tipo. En lo que interesa, la resolución citada acordó definir como tarifas máximas las que fueron aprobadas en su momento por la ARESEP, aclarar que esas tarifas regirían para todos los operadores y proveedores que contaran con el respectivo título habilitante para la prestación del servicio, así como establecer que de forma temporal las condiciones y tarifas máximas aprobadas y vigentes para el sistema de telefonía fija convencional, regirían como tarifas máximas para los servicios de telefonía IP, independientemente de la modalidad de pago (pre o post pago), y establecer como tarifas aplicables a los servicios de canales punto a punto y a los puntos multipunto, así como para los servicios de internet y envío de mensajes.

Sin embargo, andando el tiempo y un poco más maduro el mercado, mediante RCS-248-2017, la SUTEL declaró que el mercado relevante del servicio minorista de telecomunicaciones móviles se encuentra en competencia efectiva, tomando en consideración para tal conclusión que, efectivamente se verifica en este mercado específico, la condición de que ningún operador de redes o proveedor de servicios de telecomunicaciones, o grupo de cualquiera de estos, puede fijar los precios o las condiciones de mercado unilateralmente, restringiendo el funcionamiento eficiente de este, en perjuicio de los usuarios. En consecuencia, a partir de la publicación de la citada resolución, los precios del servicio de acceso a la red pública de telecomunicaciones, el servicio de llamadas con origen en una ubicación móvil y destino nacional, el servicio de mensajería corta con origen en una ubicación móvil y con destino nacional y el servicio de transferencia de datos a través de redes móviles dejaron de ser fijados por la SUTEL y son ahora definidos por el mercado.

D. CONTROL PREVENTIVO DE LAS CONCENTRACIONES

El criterio de atribución de la competencia en el control de concentraciones es de tipo subjetivo, es decir, recae sobre determinados actores y no sobre ciertas actividades. Al respecto, el artículo 56 de la LGT somete al conocimiento de la SUTEL aquellas concentraciones realizadas entre operadores de redes y proveedores de servicios de telecomunicaciones, así como aquellas en las que cualquier persona adquiera el control de dos o más operadores o proveedores de telecomunicaciones independientes entre sí.

Se entiende por concentración, en los términos del artículo 56 de la LGT y el numeral 23 del Reglamento de la Competencia, la fusión, la adquisición del control accionario, o cualquier otro acto en virtud del cual se concentren las sociedades, las asociaciones, las acciones, el capital social, los fideicomisos o los activos en general, que se realicen entre operadores de redes y proveedores de servicios de telecomunicaciones que han sido independientes entre sí.

Al ser la concentración una fusión de activos, funciones, sociedades o asociaciones que presten servicios de telecomunicaciones, debe tenerse presente que su fusión puede representar, sin duda alguna, una afectación sustancial al mercado, tanto a largo plazo como a corto plazo; y es precisamente por este motivo que se requiere de una autorización, sujeta, en la mayoría de los casos, a condiciones y obligaciones esenciales que permite garantizar una competencia efectiva en el mercado.

La SUTEL, según el numeral 28 del Reglamento de la Competencia, puede imponer condiciones con el fin de superar aquellos obstáculos que se presenten con la fusión que puedan afectar la competencia de manera sustancial. Incluso, debe valorar si de la concentración resulta una situación de poder sustancial o incremento de la posibilidad de ejercer poder en el mercado relevante, según los términos establecidos en la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor (LPCDEC). Para ello, deben considerarse los presupuestos que establece el artículo 15 de la LPCDEC para determinar el poder sustancial del mercado, pues solo puede considerarse su existencia cuando la participación del operador en ese mercado le permita fijar precios de manera unilateral, o bien, restringir el abastecimiento en el mercado de referencia, sin que los demás agentes puedan contrarrestar ese poder; existencia de barreras de entrada al mercado y los elementos que previsiblemente puedan tanto esas barreras como la oferta de los competidores; la existencia y el poder de sus competidores; restricción del acceso a los agentes económicos y sus competidores; su comportamiento reciente, y demás conductas que puedan afectar la competencia.

De lo anterior, debe quedar claro entonces que la SUTEL cuenta con las facultades y condiciones legales –así como con la discrecionalidad correspondiente-, para autorizar las concentraciones e imponer o suprimir obligaciones a cargo de uno o varios operadores con la finalidad de resguardar de la mejor manera posible la competencia en el mercado de las telecomunicaciones, considerando siempre, las particularidades que cada mercado representa.

A pesar de las amplias facultades que le asisten a la SUTEL en relación con la imposición de obligaciones, es importante recordar que su función está sujeta al principio de legalidad y, por ende, no puede imponer obligaciones que sean competencia de otras instituciones involucradas en el mercado de las telecomunicaciones. En efecto, está impedida, por ejemplo, para solicitar la renuncia de una concesión o la devolución de frecuencias, pues éstas son competencia exclusiva y excluyente del Poder Ejecutivo.

En el mismo orden de ideas, el procedimiento a seguir para aprobar la concentración es el siguiente:

Los operadores de redes y los proveedores de servicio solicitan la autorización respectiva a la SUTEL, y aportan en ese mismo momento, toda la información que se requiere para ello.

La SUTEL tiene un plazo de 30 días hábiles, a partir de la solicitud (completa, junto con la información adicional), para resolver. Solamente en casos de especial complejidad puede ampliar ese plazo por una sola vez, hasta por quince días hábiles adicionales.

De previo a emitir su resolución, debía la SUTEL -pues hoy en día esta competencia le corresponde en exclusiva en virtud de la reciente reforma ya apuntada- solicitar el criterio técnico a la Comisión de la Competencia. Este criterio no le era vinculante, pero para apartarse del mismo debía hacerlo mediante resolución motivada.

Una vez que autoriza o deniega la concentración, deberá hacerlo de manera motivada, indicando las medidas que se deben adoptar y el plazo para su implementación. Las medidas deberán aplicarse por el plazo máximo otorgado al operador o proveedor en la concesión o autorización.

Las medidas que se pueden imponer a los operadores para autorizar la concentración de sus operaciones, a la luz del numeral 57 de la LGT, así como el numeral 103 de la LFACCR, son las siguientes: i) cesión, el traspaso o la venta de uno o más de sus

activos, derechos, acciones, sistemas de distribución o servicios a un tercero autorizado, ii) la limitación o la restricción de prestar servicios determinados o vender determinados bienes, o la delimitación del ámbito geográfico en que estos pueden ser prestados o al tipo de clientes al que pueden ser ofrecidos, iii) Obligación de suplir determinados productos o prestar determinados servicios en términos y condiciones no discriminatorias a clientes específicos o a otros operadores, iv) introducción, eliminación o modificación de cláusulas contenidas en los contratos escritos o verbales que rigen sus relaciones comerciales con clientes o proveedores, v) separación o escisión de agente económico, vi) limitación o restricción para adquirir nuevas concesiones o autorizaciones, vii) cualquier otra condición estructural o de conducta que sea necesaria para impedir, disminuir o contrarrestar los efectos anticompetitivos de la concentración.

Aunado a lo anterior, la SUTEL, de conformidad con los artículos artículo 58 de la LGT y 119 incisos a), b) y f) de la LFACCR, puede imponer a los operadores, sin perjuicio de la sanción que corresponda, medidas correctivas cuando realicen concentraciones no autorizadas en la ley, como lo son la suspensión, la corrección o la supresión de la práctica de que se trate, y la desconcentración, parcial o total, de lo que se haya concentrado indebidamente.

Resulta de interés comentar a continuación, dos casos de concentraciones que se han presentado en el mercado de las telecomunicaciones de Costa Rica desde su apertura.

1. Concentración de Grupo ICE con CABLEVISION:

En primer término, valga la pena mencionar que el Instituto Costarricense de Electricidad (ICE, en lo sucesivo), antiguo monopolista, hoy operador del mercado de las telecomunicaciones, solicitó a la SUTEL, autorización para la concentración con la empresa Cable Visión de Costa Rica, y pretendía con ello, adquirir el 100% de sus acciones.

La SUTEL realizó el análisis del mercado y, en lo que interesa, solicitó criterio técnico a la Comisión para Promover la Competencia, y además, realizó un análisis del mercado de referencia (televisión), y aprobó la concentración con la imposición de medidas, en aras de garantizar la competencia efectiva en el sector y evitar el abuso de la posición de dominio que podría eventualmente llegar a tener el Grupo ICE, disponiendo en lo que interesa que se autorizaba la concentración sujeta al cumplimiento de varios requisitos, como lo son la abstención de ventas atadas entre los distintos servicios que ofrecen, entre ellos televisión. De la misma manera dispuso que no podrían ofertar en forma conjunta los servicios que aceptación la oferta por parte de los consumidores sea totalmente libre y voluntaria, entre otros.

Obsérvese cómo el regulador costarricense procuró a través de la resolución de cita, permitir una concentración en el mercado, pero sin que ello implicara por sí mismo, una afectación sustancial a este; en el tanto, es claro que las medidas impuestas fueron todas tendientes a evitar los abusos por parte del Grupo ICE, pero además, garantizar el acceso de nuevos competidores al mercado, sin permitir la creación de barreras de entrada, o la adopción de prácticas monopolísticas que beneficien a los consumidores, a los operadores actuales y a los futuros.

Debe resaltarse, además, que de manera razonada consideró que el Grupo ICE debía garantizar el acceso a la infraestructura a los demás operadores, proteger el derecho de elección de sus consumidores, como beneficiarios últimos del mercado, y, además, de manera acertada, se le obligó a que sometiera sus promociones y servicios empaquetados a aprobación previa de la SUTEL. Llama la atención esta última medida porque si bien

se está en presencia únicamente del mercado de televisión por cable, lo cierto es que el empaquetamiento de servicios que puede brindar ahora el Grupo ICE (televisión, internet y telefonía fija), sin duda podría llegar a afectar otros mercados asociados e incluso, crear un monopolio de hecho, mismo que la Constitución Política, según se apuntó al inicio del presente apartado, es prohibido. Lo anterior permite evidenciar la función que cumple el regulador frente a las concentraciones en el mercado, en aras de garantizar ex-ante, la existencia de un mercado óptimo y en igualdad de condiciones, aplicando la ya analizada regulación asimétrica frente a estas situaciones donde existe un operador cuya posición de privilegio podría distorsionar o afectar la competencia efectiva.

2. Concentración de Radiográfica de Costa Rica para la adquisición de la Base de activos y clientes de Virtualis, S.A.

Mediante el acuerdo del Consejo de la SUTEL, No. 002-005-2014, de 24 de enero de 2014, se aprobó en Resolución No. RCS-017-2014, la solicitud de autorización de concentración presentada por Radiográfica Costarricense, para la adquisición de la Base de activos y clientes de Virtualis (operador móvil virtual). Dicha solicitud fue aprobada, previo criterio técnico de la Comisión para la Competencia.

Resulta de interés para los efectos de esta investigación mencionar que la SUTEL -debido a la ausencia de pronunciamiento de RACSA- debió determinar por su parte, el mercado relevante del que se trata; siendo entonces que analizó que RACSA –sin considerar que forma parte del Grupo ICE-, prestaba los servicios de transferencia de datos y servicios mayoristas de acceso, y por su parte, Virtualis solamente prestaba servicios de telefonía móvil; por lo que dispuso que el mercado relevante para los efectos del presente caso era el mercado de telefonía móvil (acceso a internet, llamadas internacionales, terminación de llamadas).

Asimismo, y a pesar de que RACSA y el Instituto Costarricense de Electricidad forman parte del mismo Grupo de Interés Económico –Grupo ICE-, sostuvo que dentro de los operadores que competían en el mercado de las telecomunicaciones, al que pretendía ingresar RACSA, presta servicios como un operador del mismo, el Instituto Costarricense de Electricidad. Aunado a ello, realizó la SUTEL un análisis de las cuotas del mercado; mediante el cual se obtuvo como resultado que el Grupo ICE contaba para ese momento con un 65% de participación en el mercado de telefonía móvil (mucho más del 25% que solicita el Reglamento de interconexión para considerar a un operador con peso significativo de mercado, lo que permite concluir que es un operador con poder sustancial en el mercado, en los términos del artículo 54 de la LGT).

No obstante lo anterior, y ante la evidente situación de posible afectación del mercado, la SUTEL utilizó como referencia para valorar los efectos de esta concentración los parámetros o medidas empleadas por el Departamento de Justicia y la Comisión Federal de los Estados Unidos de América (Commission, 2010), mediante los cuales se diseñan diferentes rangos y se le atribuye distinto valor a cada uno para determinar la afectación de un mercado relevante como consecuencia de una concentración (Mota, 2004).

Queda entonces la duda de si ¿realmente convenía implementar el uso de técnicas de un mercado con condiciones disímiles a las existentes en Costa Rica, o bien, si por el contrario realmente esta es una medida que permite la concreción de un mercado en competencia en el caso costarricense a escasos 3 años de su apertura material? No existe aún una respuesta concreta, pero solamente puede quedar plasmada, con ello, una duda sobre la función del regulador y su potestad para variar los criterios de aplicación, de un caso a otro según su “discreción”, y además, una incertidumbre sobre la justificación que

permitió utilizar esta metodología, si analizado anteriormente, correspondiente a la fusión de Grupo ICE con Cablevisión, aplicó la metodología europea y no la estadounidense como se hizo en este supuesto; normativa que valga la pena mencionar resulta de mejor aplicación al mercado costarricense debido a que Costa Rica tiene una fuerte influencia europea en el proceso de liberalización de las telecomunicaciones, y en su legislación se recogen básicamente los mismos principios, pero además, muchos de los mercados europeos tuvieron una apertura gradual como el nuestro, pues pasaron de un monopolio a una apertura del mercado de las telecomunicaciones y posteriormente, a diferencia del nuestro, a la privatización del antiguo monopolista. Por tanto, ¿qué ocurrió para que el regulador optara esta vez por utilizar una metodología distinta? Su justificación, se echa de menos en la resolución de marras; pues además de ser inexistente, no da motivos o indicios que permitan concluir la importancia y relevancia de su utilización.

Ahora bien, llama poderosamente la atención, asimismo, el análisis que realizó la SUTEL sobre la incidencia que podría tener esta decisión en el mercado de las telecomunicaciones, al considerar que no se producía un cambio significativo en el mercado relevante de telefonía móvil, por cuanto se permite presumir, del análisis realizado con base en la metodología utilizada en Estados Unidos, que no tendrá un efecto anticompetitivo en el mercado.

Sostuvo, además, que los competidores del ICE –Claro y Telefónica-, ofrecen servicios similares y ofrecen servicios, paquetes y promociones similares, por lo que pueden competir de manera efectiva con el ICE. Sin embargo, no se puede compartir esta postura, sobre todo porque el ICE, según el análisis que realizó la SUTEL en la misma resolución, contaba para ese momento con una cuota de mercado del 65%, por lo que su posición de operador con poder significativo de mercado era innegable, porcentaje que valga resaltar, es superior al establecido como mínimo por parte del propio regulador en la resolución citada anteriormente. Ante ello, la SUTEL solamente refirió de manera breve y además justificó su existencia por considerar que es el operador incumbente, y que, por ende, no afectaría la competencia de manera significativa, en el tanto, el ICE desde antes ya percibía ingresos porque Virtualis prestaba los servicios a través de su red. Se le olvidó para este punto a la SUTEL que los ingresos que obtendría el ICE son mayores que los que obtenía en el pasado por el alquiler de la red a Virtuales, pues percibiría además los ingresos correspondientes a la prestación del servicio al usuario final.

Finalmente, la SUTEL autorizó la concentración sin ninguna condición a la operación de concentración solicitada por Radiográfica de Costa Rica, para la adquisición de base de clientes y activos de VIRTUALIS.

V. EL SERVICIO UNIVERSAL

Las telecomunicaciones incluyen una pluralidad de servicios esenciales, que la sensibilidad político – social actual considera ineludibles para desarrollar una vida humana en condiciones adecuadas. La prestación de estos servicios –en aceptables condiciones de calidad y precio- debe, pues, ser garantizada a todos los ciudadanos, con independencia de su situación geográfica o de su rentabilidad. Esto es algo que antes buscaba asegurar el régimen del servicio público y que ahora deben garantizar las obligaciones de servicio público (López, 2001). Lo anterior se refleja en el concepto de "servicio universal", entendido como un conjunto definido de servicios cuya prestación se garantiza a todos los usuarios finales, con independencia de su localización geográfica, con una calidad determinada y a un precio asequible (Arroyo, 2010). Se trata, por tanto, de una oferta de servicios en condiciones dignas y adecuadas.

Ejemplo de esto es la normativa comunitaria europea (Ruiz, 2007), la cual contempla dos alternativas generales para su fijación, a saber:

- i) Las autoridades nacionales podrán introducir un mecanismo de compensación con cargo a los fondos públicos; o bien,
- ii) Repartir el coste neto de las obligaciones de servicio universal entre los proveedores de servicios y redes de comunicaciones electrónicas. Así, cabe que el fondo sea sufragado por todos los operadores del sector, o bien que se alimente por una tasa parafiscal o impuesto especial, que se cobra a todos los usuarios de servicios de telecomunicaciones (Paz, 2007).

En lo que respecta al ordenamiento jurídico costarricense –siguiendo la línea de la mayor parte de los países europeos y de los Estados Unidos de Norteamérica-, el financiamiento del servicio universal corresponde a los operadores del sector. Ello, como es bien conocido, surge a partir de la apertura comercial en el mercado de las telecomunicaciones, con ocasión de la suscripción del TLC, mediante el cual se establecieron las bases de la “nueva” normativa referente al tema.

A partir de tales bases la LGT creó el Fondo Nacional de Telecomunicaciones (FONATEL) como instrumento de administración –por parte de la SUTEL- de los recursos destinados a financiar el cumplimiento de los objetivos fundamentales del régimen de acceso universal, servicio universal y solidaridad establecidos en la misma Ley, así como las metas y prioridades definidas en el PNDT. La contribución especial parafiscal al Fondo representa un aporte que recae sobre los ingresos brutos obtenidos directamente por la operación de redes públicas de telecomunicaciones o bien por proveer dichos servicios disponibles al público.

Los mencionados objetivos se encuentran regulados en los ordinales 31 al 33 del Título II – “Régimen de Garantías Fundamentales”-, Capítulo I – “Acceso Universal, Servicio Universal y Solidaridad de las Telecomunicaciones”- de la LGT; mientras que los aspectos relativos a la administración del FONATEL, las formas de asignación de los recursos, la ejecución de los fondos, las fuentes de financiamiento y los mecanismos de rendición de cuentas en relación con el mismo, están reguladas a partir del artículo 34 y hasta el numeral 40 del citado capítulo.

A la luz de tales lineamientos, con el fin de alcanzar sus objetivos, el FONATEL mantiene un fideicomiso de gestión de sus proyectos y programas, cuyo patrimonio es producto de las diferentes fuentes de financiamiento del Fondo (artículo 38 de la LGT), siendo su principal ingreso recurrente, la mencionada contribución especial parafiscal. En lo que interesa, el numeral 38 dispone que los recursos del FONATEL no podrán ser utilizados para otro fin que no sea el establecido en el PNDT, en cumplimiento de los objetivos anteriormente citados, y que éstos deberán asignarse íntegramente cada año. No obstante, los costos de administración del FONATEL serán cubiertos con los recursos del mismo Fondo, para lo cual no se podrá destinar una suma mayor a un uno por ciento (1%) del total de los recursos. La administración de tales recursos está sometida a la fiscalización de la Contraloría General de la República y de la Dirección General de Tributación del Ministerio de Hacienda.

De conformidad con el artículo 39 de la LGT, esta contribución parafiscal se justifica en el beneficio individualizable que para los operadores y proveedores señalados representa la maximización del uso de las redes de telecomunicaciones y el incremento de los usuarios de servicios de comunicaciones impulsados por la ejecución de los proyectos de acceso,

servicio universal y solidaridad.

En lo que respecta a su procedimiento de pago, este es determinado por el mismo contribuyente por medio de una declaración jurada que corresponde a un período fiscal año calendario, distribuyéndose el monto resultante en cuatro tráctos equivalentes, pagaderos al día quince de los meses de marzo, junio, setiembre y diciembre del año posterior del período fiscal que corresponda.

La tarifa de dicha contribución debe ser calculada y fijada por la SUTEL a más tardar el 30 de noviembre del período fiscal respectivo. Esta se fija dentro de una banda con un mínimo de un uno coma cinco por ciento (1,5%) y un máximo de un tres por ciento (3%), debiendo basarse dicha fijación en las metas estimadas de los costos de los proyectos por ser ejecutados para el siguiente ejercicio presupuestario y en las metas de ingresos estimados para dicho ejercicio. En el evento de que la Superintendencia no fije la tarifa al vencimiento del plazo señalado, se aplicará la ejecutada en el período fiscal inmediato anterior.

VI. RÉGIMEN DE ACCESO E INTERCONEXIÓN

La implantación de la competencia requiere abrir las redes existentes, para permitir con ello el ingreso de nuevos operadores al mercado. El acceso y la interconexión entonces son inherentes el proceso de liberalización e implementación de la competencia en el mercado de telecomunicaciones, pues en caso contrario, se crearía una barrera de entrada que no permitiría a los operadores construir todas sus redes en poco tiempo, de manera tal que tampoco lograrían contar con las mismas características del operador histórico que tenía más de 60 años de desplegarlas.

Al no poderse replicar la red existente se debe permitir a los nuevos operadores de servicios de telecomunicaciones, el uso de las redes preexistentes, y por ello es que se le imponen obligaciones específicas en relación con el acceso e interconexión de redes. Solamente de esta manera se logra que los nuevos operadores puedan empezar a desenvolverse en un mercado en condiciones de competencia efectiva, pues este acceso debe propiciarse de manera transparente y no discriminatoria.

Como bien lo establece el artículo 59 de la LGT, el acceso y la interconexión tienen como fin procurar la eficiencia, la competencia efectiva, la optimización del uso de los recursos escasos y un mayor beneficio para los usuarios. La SUTEL debe asegurar, por tanto, que el acceso e interconexión sean provistos en forma oportuna y en términos y condiciones no discriminatorias, razonables, transparentes, proporcionadas al uso pretendido y que no impliquen más que lo necesario para la buena operación del servicio previsto.

Le compete a la SUTEL, de conformidad con el citado numeral 59, la imposición de obligaciones de acceso e interconexión, de manera tal que se permita con ello, la buena operación del servicio que se presta. Debe tenerse en cuenta que los acuerdos de acceso e interconexión son negociados de manera libre por los operadores de telecomunicaciones, previa aprobación, o intervención cuando corresponda, de la SUTEL. En efecto, los operadores deben notificar a SUTEL: a) una vez que inicien las negociaciones para el acceso y la interconexión; y b) los acuerdos de interconexión que hayan suscrito.

Cuando se notifique a la SUTEL el acuerdo, ésta lo revisará y como lo expresa el numeral 60 del mismo cuerpo legal, podrá adicionar, eliminar o modificar todas aquellas cláusulas que en su criterio requieran ser ajustadas de acuerdo con lo normativa de telecomunicaciones, para garantizar a su vez, una competencia efectiva en el mercado.

Caso contrario, si los operadores no llegaren a un acuerdo, o bien, si alguno de ellos no desea suscribir un contrato de interconexión, dentro de los tres meses siguientes a la notificación, la SUTEL puede, de oficio o a petición de parte, determinar la forma, los términos y las condiciones bajo las cuales se materializará el acuerdo. En caso de urgencia, tiene competencia para fijar las condiciones de manera provisional y hasta tanto no se resuelva de manera definitiva la situación.

Estas especiales características de los contratos de acceso e interconexión plantean la duda acerca de su naturaleza jurídica. ¿Son realmente contratos? A esta pregunta la doctrina ha replicado, básicamente con dos tesis: la que pregonó que se trata de un contrato de Derecho privado y la que postula su naturaleza jurídica como de Derecho público (Farfán, 2005).

Con todo, desde nuestra perspectiva, las normas aplicables al acceso e interconexión evidentemente no son las del Derecho privado, sino las normas de carácter sectorial, o sea, el marco regulatorio del mercado de las telecomunicaciones, toda vez que la obligación no surge como resultado directo de la voluntad libremente manifestada por las partes. Antes bien, los elementos fundamentales del contrato están previamente establecidos por la ley e inclusive en aquellos aspectos secundarios, el Regulador puede intervenir con la finalidad de modificar, complementar o incluso anular y sustituir la declaración de voluntad de las partes por la suya propia. En consecuencia, no puede decirse que su naturaleza sea contractual, sino que, lo que se verifica es una intervención administrativa-regulatoria, de suerte que, la relación jurídica de acceso e interconexión que surge como consecuencia de un contrato o acuerdo de acceso e interconexión es de Derecho público.

Ahora bien, le corresponde al Instituto Costarricense de Electricidad, como operador incumbente y dueño de la red, de conformidad con el artículo 59 del Reglamento de Acceso e Interconexión, publicar su Oferta de Interconexión de Referencia, mediante la cual expresa las condiciones técnicas y económicas que regirán el acceso y la interconexión que pretende ofrecer a los demás operadores. Esta oferta debe ser siempre aprobada por la SUTEL y, además, puede ser modificada por ella misma.

Aunado a ello, le compete además al organismo regulador del sector de telecomunicaciones a la luz de lo analizado en el presente trabajo, aprobar los precios de acceso e interconexión de redes para garantizar con ello, el acceso en condiciones de igualdad, sin otorgar ventajas a algunos operadores. Al respecto, el numeral 61 de la Ley General de Telecomunicaciones consagra que los precios de interconexión deberán estar orientados a costos, conforme al inciso 13) del artículo 6 de esta Ley y serán negociados libremente por los operadores entre sí, con base en la metodología que establezca la SUTEL. Esta metodología deberá garantizar transparencia, objetividad, no discriminación, factibilidad financiera y desagregación de costos.

El regulador debe, asimismo, velar por el cumplimiento de los acuerdos de acceso e interconexión, así como sancionar cuando corresponda, por la violación o incumplimiento del referido contrato, pues esa conducta, a la luz de la normativa del sector de las telecomunicaciones, corresponde a una falta grave.

VII. CONCLUSIÓN

Si partimos del hecho que el servicio de las telecomunicaciones en Costa Rica fue prestado por el Estado en un régimen de monopolio legal durante más de 60 años y había listas de espera para adquirir una línea celular o una conexión de Internet, el nuevo modelo propulsado por el Tratado de Libre Comercio entre República Dominicana, Centroamérica

y Estados Unidos y consumado mediante la Ley General de Telecomunicaciones y la Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector de las Telecomunicaciones ha supuesto un verdadero cambio de paradigma (Kuhn, 1970).

En este sentido, como se comprueba fácilmente a partir del estudio del estatuto del Regulador, la gran mayoría de sus funciones, de una u otra manera tienen una incidencia en la concreción de los mercados en competencia. Asimismo, los mecanismos jurídicos instaurados, principalmente por la LGT y sus reglamentos, tienen por objeto crear un mercado de telecomunicaciones en competencia, pero sin olvidar el fin social que le asiste; de ahí que se previera toda una regulación para el servicio universal, que se satisface principalmente por medio del Fondo Nacional de Telecomunicaciones (FONATEL).

Con todo, es claro que el periodo de transición del monopolio a la competencia es un proceso lento y requiere de un enorme esfuerzo de todos los actores, sobre todo porque, en nuestro mercado de telecomunicaciones, el incumbente es una empresa estatal que sigue ostentando un innegable peso significativo de mercado, de suerte que, la regulación para la competencia debe ser profunda, incisiva y constante para evitar – parafraseando a (Taruffo, 2006)-, seguir viviendo en un sistema creyendo estar en otro.

VIII. REFERENCIAS

- Ariño, G. (2004). Principios de Derecho Público Económico. Marcial Pons.
- Ariño, G., Cuétara, J. M., & Noriega, y. R. (2005). Banda Ancha. Nuevo papel del Estado en sectores regulados. Deusto.
- Arroyo, G. S.-A. (2010). El Régimen Legal del Servicio Universal en Telecomunicaciones. Adrus.
- Autoridad Reguladora de los Servicios Públicos. (2007). Hacia un nuevo marco regulatorio en el sector de telecomunicaciones en Costa Rica: opciones y riesgos a considerar. Centro de Estudios de Regulación.
- Chloe, N. a., Stewart, W. H., Sunstein, C. R., Vermule, A., & Herz, a. M. (2011). Administrative Law and Regulatory Policy. Wolters Kluwer.
- Commission, U. D. (2010). Horizontal Merger Guidelines. USA.
- Farfán, M. H. (2005). Naturaleza Jurídica del Acuerdo o Contrato de Interconexión en el Sector Telecomunicaciones. Pontificia Universidad Católica del Perú.
- Hewitt, R. M.-J. (2006). Los costarricenses en la economía basada en el conocimiento: Infraestructura, destrezas, uso y acceso. Jessfrank.
- Hicks, J. R. (1935). Anual Survey of Economic Theory: The Theory of Monopoly. Econometrica, 8.
- Kuhn, T. (1970). The Structure of Scientific Revolutions. University of Chicago Press.
- López, G. A.-L. (2001). Derecho de la Competencia en Sectores Regulados. Comares.
- Mota, M. (2004). Competition Policy: Theory and Practice. Cambridge University Press.
- Ordóñez, M. A. (2000). La competencia. Alianza.
- Ortiz, L. (2021). El factor ideológico en la enseñanza del Derecho administrativo. En J.

- R. Arana-Muñoz, Reflexiones iberoamericanas sobre la enseñanza del Derecho Administrativo (pp. 2019-251). Tirant lo Blanch.
- Paz, J. C. (2007). Telecomunicaciones: Regulación y Mercado. Aranzadi.
- Quadra, E. G. (2004). Comentarios a la Ley General de Telecomunicaciones. Ley 32/2003, de 3 de noviembre. Civitas.
- Rivera, J. P. (13 de noviembre de 2020). Costa Rica ya está tarde para la era del 5G. Delfino.
- Ruiz, M. C. (2007). El Servicio Universal de Telecomunicaciones. Aranzadi.
- Sala Constitucional, Voto 5445-99 (Sala Constitucional de la Corte Suprema de Justicia 1999).
- Sojo, C. (2010). Igualiticos: la construcción social de la desigualdad en Costa Rica. Master Litho, PNUD
- Taruffo, M. (2006) El vértice ambiguo. Ensayos sobre la Casación civil. Palestra.
- Ubico, C. (2008). Telecomunicaciones: Aprendiendo a liberalizar correctamente. En L. Ortiz, Derecho Público Económico (pp. 207-253). Continental.
- UNCTAD. (2010). Model Law on Competition - Chapter VII. United Nations Conference on Trade and Development.
- Zegarra, D. (2005). Servicio Público y Regulación. Marco Institucional de las Telecomunicaciones en el Perú. Palestra.



DE LOS SANDBOX REGULATORIOS Y OTROS MEDIOS (DEMONIOS) DE CRECER EL ACCESO A INTERNET EN PERÚ

REGULATORY SANDBOX AND OTHER MEANS (DEMONS) TO FOSTER INTERNET ACCESS IN PERU

VIRGINIA NAKAGAWA MORALES¹
JOSÉ AGUILAR REÁTEGUI²

RESUMEN

Dada la nueva realidad, que tiene como eje la conectividad digital, la pregunta a responder es: ¿Cómo hacemos para, literalmente, “quemar etapas” y cerrar la brecha digital actual y la que se nos va a formar “a la vuelta de la esquina” con el 5G?

Este documento propone ideas que consideramos indispensables aplicar, para generar un crecimiento exponencial “post pandemia” de las redes de telecomunicaciones en todo el territorio nacional, especialmente en zonas rurales y de preferente interés social, y que servirán para dar conectividad digital (internet de alta velocidad) sobre una base de inclusión digital (no discriminatoria e incluyente).

En ese sentido, no sólo es necesaria la innovación tecnológica, sino que es indispensable revisar integralmente el marco normativo vigente del sector (ya sea la normativa emitida por el Ministerio de Transportes y Comunicaciones o la emitida por el Organismo Supervisor de Inversión Privada en Telecomunicaciones) para (i) eliminar barreras de entrada, sobrecostos regulatorios, así como, normativa que no genera valor y que esté desfasada por la evolución tecnológica,

ABSTRACT

Given the new reality, which has digital connectivity at its core, the question to answer is: How do we literally “burn stages” and close the current digital divide and the one that will form “just around the corner” with 5G?

This document proposes ideas that we consider essential to apply in order to generate an exponential “post pandemic” growth of telecommunications networks throughout the national territory, especially in rural areas and areas of preferential social interest, and that will serve to provide digital connectivity (high speed internet) on a basis of digital inclusion (non-discriminatory and inclusive).

In this sense, not only is technological innovation necessary, but it is also essential to review the sector's current regulatory framework (whether the regulations issued by the Ministry of Transport and Communications or those issued by the Supervisory Body for Private Investment in Telecommunications) to (i) eliminate barriers to entry, regulatory cost overruns, regulations that do not generate value and that are outdated by technological evolution and therefore no longer pass a brief cost & benefit assessment) and (ii) generate incentives for the expansion of networks

-
- 1 Abogada. Consultora Senior Experta en regulación de servicios públicos y transformación digital. Con más de 30 años de experiencia en la actividad pública y privada, en materia regulatoria y despliegue de infraestructura.
 - 2 Economista. Experto en regulación de servicios públicos y de políticas de Estado. Orientado a impulsar nuevas tecnologías y servicios con regulación e incentivos adecuados. Con más de 15 años de experiencia en temas regulatorios y financieros.

con lo cual ya no superan una somera evaluación costo & beneficio; y, (ii) generar incentivos para la expansión de redes y la generación de mayores servicios innovativos, que producen valor positivo a los consumidores, y en especial, a los "no conectados". Por ello, nuestra recomendación consiste en implementar "**Sandbox Regulatorios**", para que los mismos agentes que están en el mercado u otros, puedan plantear innovaciones y ofrecer nuevos servicios, bajo una burbuja regulatoria, que genere predictibilidad y permita presentar casos de negocio, en un marco de confianza y colaboración público-privado.

Pero no solo eso: consideramos que los "**Sandbox Regulatorios**", deben dar paso a una siguiente generación que denominamos "**Plan Flexibilizar para Conectar**", que permita que los diversos agentes puedan presentar propuestas innovadoras que cumplan con los siguientes objetivos: i) impulsar la conectividad en zonas de baja o nula conectividad; ii) incentivar el uso de tecnologías nuevas y/o disruptivas; iii) que beneficien a los usuarios; y iv) que genere mayor competencia.

Al igual que en el mercado, se hablaba de 2G, luego 3G, para pasar al 4G y hoy ya estamos en 5G e incluso, ya hay literatura especializada que habla de 6G.... en normativa de avanzada, Perú ya debería estar desarrollando "**Sandbox Regulatorios**" así como "**Plan Flexibilizar para Conectar**". No hay tiempo que perder.

PALABRAS CLAVES

Flexibilidad regulatoria | Internet | Inclusión digital | Telecomunicaciones | Transformación digital

CONTENIDO

1. El reto a afrontar; **2.** De los Sandbox regulatorios; **2.1** ¿Qué es un Sandbox Regulatorio (SR)?, **2.1.1.** Corea del Sur, **2.1.2** Reino Unido, **2.1.3** Colombia; **2.2.** ¿Qué hacemos en el Perú con las zonas donde no hay conectividad? Mecanismos tradicionales; **3.** ¿Qué hacemos en el Perú con las zonas donde no hay conectividad? Pensemos fuera de la caja; **3.1** Plan "Flexibilizar para Conectar"; **3.2** Análisis de Impacto Regulatorio; **3.3** ¿Es suficiente

and the generation of more innovative services, that produce positive value for consumers, especially the "unconnected". Therefore, our recommendation is to implement "**Regulatory Sandboxes**", so that the same agents that are in the market or others can propose innovations and offer new services, under a regulatory bubble that generates predictability and allows business cases to be presented, in a framework of trust and public-private collaboration.

But not only that: we believe that the "**Regulatory Sandboxes**" should give way to the next generation, which we call the "**Flexibilize to Connect Plan**", which will allow the various agents to present innovative proposals that meet the following objectives: i) promote connectivity in areas with low or no connectivity; ii) encourage the use of new and/or disruptive technologies; iii) benefit users; and iv) generate greater competition.

As in the market, there was talk of 2G, then 3G, to move on to 4G and today we are already in 5G and there is even specialized literature that talks about 6G.... in advanced regulations, Peru should already be developing "**Regulatory Sandbox**" as well as "**Flexibilize to Connect Plan**". There is no time to lose.

KEYWORDS

Regulatory sandbox | Internet | Digital inclusion | Telecommunications | Digital transformation

un Sandbox Regulatorio para mejorar la conectividad?; **4. Conclusiones; Bibliografía.**

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 3 de mayo de 2021 y aprobado para su publicación el 17 de agosto de 2021.

1. EL RETO A AFRONTAR

En los últimos años, muchos ciudadanos han podido disfrutar de los beneficios de la conectividad. Desde el inicio de la privatización de las empresas nacionales de telecomunicaciones en el Perú, empezó un crecimiento en los indicadores de diversos servicios: mayor cantidad de líneas fijas, la disruptión de la telefonía móvil (servicio con mayor alcance en los usuarios y con mayor despliegue de red a nivel nacional), el surgimiento del internet, así como la aparición de diversas tecnologías: internet por cable coaxial, fibra óptica al hogar, internet inalámbrico, 2G, Wimax, 3G, 4G y recientemente el 5G en varias zonas urbanas de Lima, ciudad capital.

El sector telecomunicaciones es uno de los sectores dinamizadores de la economía peruana. En los últimos doce años, el Producto Bruto Interno (PBI) sectorial ha crecido un poco más de tres (3) veces de lo que creció el PBI nacional. Así mismo, es un sector que invierte cerca de mil millones de dólares cada año. Es un sector, donde existen cuatro (4) operadores importantes, en una dinámica competitiva que ha permitido que los precios al usuario se reduzcan en 95% por Mbps³. En el servicio de internet fijo, si bien en algunas regiones aún predomina el operador incumbente, en otras existe una mayor oferta comercial que brinda variadas alternativas a los usuarios. Todos estos son indicadores alentadores del crecimiento y de la importancia del sector.

Sin embargo, con la pandemia global del COVID-19, la forma de interactuar cambió, tal como lo evidencia Savona (2020)⁴. Ya no existen reuniones presenciales y fueron reemplazadas por reuniones virtuales mediante el uso de diversas plataformas, muchas personas están en trabajo remoto, los niños y jóvenes estudian mediante educación a distancia, así como hubo un incremento del comercio electrónico, entre otros.

El acceso a internet, la banda ancha (internet de alta velocidad), o la denominación que queramos acuñar, es un servicio público, esencial, y de primerísima necesidad, lo que ha quedado más que demostrado en esta Pandemia, en que el mundo se volcó en cuarentenas y la única vía para poder seguir trabajando, estudiando, y en general, poder tomar contacto con el exterior fue el internet. Esta nueva realidad está basada en conectividad. Sin embargo, a la par que quedó clara su importancia, se evidenció en las zonas más alejadas o en las personas con menor capacidad adquisitiva, la falta de este servicio, la ausencia de infraestructura y conectividad digital, la carencia de las competencias y habilidades digitales y la asequibilidad del servicio en sí y el equipamiento asociado a éste: en suma, la falta de todo lo que compone, la transformación digital.

Por eso durante este 2021, diversos países han implementado una serie de medidas como los que detallamos a continuación: Todos Conectados en Perú, *Emergency Broadband*

3 <https://www.osiptel.gob.pe/portal-del-usuario/noticias/osiptel-usuarios-pagan-hasta-68-menos-por-velocidades-mas-altas-de-internet-fijo/>

4 Savona, M. (2020). ¿La “nueva normalidad” como “nueva esencialidad”? COVID-19, transformaciones digitales y estructuras laborales. *Revista de la Cepal* No 132. Diciembre. CEPAL. Disponible en https://repositorio.cepal.org/bitstream/handle/11362/46831/RVE132_Savona.pdf?sequence=1&isAllowed=y

Benefit en Estados Unidos, el Plan de Recuperación, Transformación y Resiliencia en España, el Proyecto Gigabit en el Reino Unido y el Plan Governo Eletrônico - Serviço de Atendimento ao Cidadão en Brasil, entre otros. Todos estos planes enfocados no solo en expandir la infraestructura en las zonas alejadas de cada país, sino también en financiar equipos y subsidiar el consumo de internet de banda ancha.

Así las cosas, resulta impresionante la evidencia que se ha generado, en el sentido que:

...la infraestructura digital es un componente fundamental en el mantenimiento de la resiliencia económica. La capacidad de las redes para acomodar las necesidades de comunicación resultantes de COVID-19 solamente puede ser garantizada mediante la acción conjunta de operadores, reguladores, y plataformas de internet.⁵ (CAF, 2020, p. 17).

Y es en este punto que se observa que todos los indicadores generales mencionados anteriormente no eran suficientes y es necesario profundizar el análisis. En el Perú, contamos con aproximadamente cien mil centros poblados (CCPP) y según información del Organismo Supervisor de la Inversión en Telecomunicaciones (OSIPTEL), sólo el 44% de los CCPP tienen cobertura de telefonía móvil y representan cerca de 91% de la población⁶ y aproximadamente 76,2% de los hogares cuenta con internet (fijo o móvil), según la Encuesta Residencial de Servicios de Telecomunicaciones (EREESTEL, 2020)⁷. La pregunta, entonces que nos debemos hacer es: ¿qué sucede con el resto de la ciudadanía y de hogares que no tiene acceso a los servicios de telecomunicaciones?

La mayor conectividad no sólo es importante por los efectos en el bienestar de las personas (una mejora en los ingresos mensuales de hogares rurales en aproximadamente S/ 390)⁸ y en el crecimiento del PBI (un incremento de 10 puntos porcentuales en los hogares conectados con internet, impactaría en 2% en el PBI)⁹, como lo demuestran los estudios

5 Ver: CAF (2020). El estado de la digitalización de América Latina frente a la pandemia del COVID-19. Abril. Caracas: CAF. Retrieved from: <https://scioteca.caf.com/handle/123456789/1540>

Resultan interesantes los resultados de este estudio de la CAF, quienes estimaron con base a evidencia empírica, la importancia de la digitalización como factor mitigante de la disrupción de la pandemia. Entre sus principales conclusiones, resaltamos tres: (i) El análisis econométrico del impacto económico del virus SARS-CoV indica que aquellos países con una infraestructura de conectividad desarrollada pudieron mitigar un 75% de las perdidas económicas asociadas con la epidemia del SARS y el impacto de las medidas sanitarias tomadas para contrarrestarlo (cuarentena, distanciamiento social, interrupción de tráfico aéreo, uso de mascarillas, etc.); (ii) La resiliencia del aparato productivo también indica falencias no en términos de adopción tecnológica sino en la asimilación de tecnología en procesos productivos, en particular en las cadenas de aprovisionamiento. Esto resulta en una debilidad importante para afrontar las disrupciones ocasionadas por la pandemia; y, (iii) COVID-19 implica una disrupción adicional en el mercado laboral ocasionada por la proporción de la fuerza de trabajo que puede transicionar al teletrabajo.

6 Ver OSIPTEL (2018). Consulta Pública sobre el Proyecto "Mecanismos supervisados de compartición y acceso en la industria de servicios móviles". Informe 242-GPRC/2018. Lima.

7 <https://www.gob.pe/institucion/osiptel/noticias/305041-osiptel-el-acceso-a-internet-de-los-hogares-peruanos-se-incremento-mas-de-283-de-2012-a-2019>

8 Aguilar, J.; Gil Malca, C.; Aparco, E.; Acosta, D.; Cajavilca, A.; Rusbel, A.; Asencios, L.; Roque, E. y Robles, F. (2020). Impacto económico del acceso a internet en los hogares peruanos. Documento de trabajo N° 01. Lima: MTC.

9 Aguilar, J.; Gil Malca, C.; Aparco, E.; Acosta, D.; Asencios, L.y Robles, F. (2021). Impacto del acceso a internet en el crecimiento económico del Perú: Un enfoque ARDL. Documento de

realizados por Aguilar et al (2020) y Aguilar et al (2021). Sino que adicionalmente a estos impactos positivos económicos, con la nueva realidad, la conectividad es la única forma en que ciudadanos de zonas más alejadas y de menor densidad poblacional puedan estar “en línea” con la educación, el acceso a las prestaciones de salud, seguridad y para reunirse con la familia.

Y a la actual brecha digital, muy pronto habrá que sumarle, el incremento que se va a generar entre las personas que tengan servicios 5G y las personas que no tengan servicios 5G. Como es de conocimiento público, los usuarios que cuenten con servicios 5G podrán gozar con un servicio de internet 10 o más veces más rápido que el actual 4G, lo que equivale a un internet de altísima velocidad, y tendrán un ecosistema en que se podrán desarrollar las Tecnologías de la Información y Comunicación (TIC), apareciendo el IoT (internet de las cosas), las Ciudades Inteligentes, aplicaciones para la Agricultura, Educación a Distancia, Tele salud, Transporte público inteligente, entre otros. Es decir, un sin fin de oportunidades tecnológicas que van a generar mayor bienestar a la población y un impacto positivo al PBI. Entonces, la pregunta es: ¿Cómo le hacemos para, literalmente, “quemar etapas” y cerrar la brecha digital actual y la que se nos va a formar “a la vuelta de la esquina” con el 5G?

Un aspecto a tener en consideración es que hoy tenemos un nuevo “usuario digital”. En efecto, este nuevo usuario digital (post pandemia) es un usuario mucho más consciente del ámbito de la calidad, ya que de ello depende que pueda trabajar en forma remota o recibir clases virtuales, sin que haya interrupciones de servicio. Por tanto, si ya existe la brecha digital entre los que tienen servicios de telecomunicaciones y los que no tienen servicios de telecomunicaciones, ésta brecha se hace más grande ya que se requiere una buena calidad¹⁰.

Dicho lo anterior, nos enfocaremos en las ideas o propuestas que consideramos indispensables evaluar su aplicación en nuestra realidad peruana, no sin antes dejar de mencionar que estas propuestas parten del uso necesario que se debe efectuar de las redes de fibra óptica implementadas o en construcción bajo el Régimen de Banda Ancha, y nos referimos tanto a la Red Dorsal Nacional de Fibra Óptica (RDNFO) así como a las redes de transporte regional y las redes de acceso regional financiadas con el fondo de acceso universal (FTEL) que implican un crecimiento importante de redes de fibra óptica en todo el territorio nacional, especialmente en zonas rurales y de preferente interés social, y que sirven para dar conectividad digital (internet de alta velocidad) sobre una base de inclusión digital.

En ese sentido, no sólo es necesario innovar para poder brindar alternativas para mejorar la conectividad en esas localidades que no cuentan con el servicio de telecomunicaciones. Es necesario innovar en forma creativa, para generar ecosistemas digitales, es decir, entornos digitales que permitan la sostenibilidad de los servicios en el tiempo, lo que nos lleva a revisar el marco normativo vigente del sector para que permita solucionar esa problemática.

trabajo N° 02. Lima: MTC.

- 10 La necesidad de contar con una mejor calidad del servicio de internet, ha generado en el Perú, la reciente aprobación de la Ley 31207 por el cual se ha modificado el Art. 5 de la Ley 29904, estableciendo que tanto en zonas urbanas como en zonas rurales, los prestadores de servicios de internet deberán garantizar el 70% de la velocidad mínima ofrecida en los contratos con los consumidores o usuarios y establecidas en sus planes (postpago, prepago y otros) publicitados en los diferentes medios de comunicación. Esta normativa se aplicará tanto en el servicio provisto por medios fijos o por medios inalámbricos.

Recientemente en otros países, se han enfrentado a estos problemas similares. Su solución fue implementar Sandbox Regulatorios, de forma que permita a los mismos agentes que estaban en el mercado, innovar y ofrecer nuevos servicios, bajo una burbuja regulatoria. Para ello, es el propio Estado -léase el Ministerio de Transportes y Comunicaciones (MTC) y OSIPTEL—quien deben abrir estos espacios de propuestas, que van más allá de un mero *wish list*, en la medida que son los agentes del mercado quienes conociendo su entorno y con mayor acceso a información que las entidades del Estado, proponen y se comprometen a llevar dichos proyectos, haciendo de la colaboración público-privado, un real laboratorio de innovación tecnológica y regulatoria como pasaremos a explicar.

2. DE LOS SANDBOX REGULATORIOS

2.1. ¿Qué es un Sandbox Regulatorio (SR)?

Con el auge del internet y la evolución de nuevas tecnologías, se han desarrollado una serie de nuevos modelos de negocio para brindar una gama de productos y servicios digitales a una cantidad cada vez más importante de clientes. De acuerdo con la CEABAD (2020)¹¹, esto trajo como consecuencia que los Reguladores actúen de forma reactiva (*ex post*) para determinar las condiciones que permitan garantizar los deberes y derechos de los usuarios, y que incluso, en casos extremos, afecten la posibilidad de aparición de nuevos servicios.

En ese sentido, en vez de actuar de forma posterior y reactiva, algunos Reguladores han optado por adoptar un enfoque proactivo. De esa manera, surgen los Sandbox Regulatorios, que implican un banco de pruebas para nuevos modelos de negocios, de forma que la regulación no sea estática, sino que sea dinámica y se adapte de forma ágil a las innovaciones que se presenten en el tiempo.

De la revisión bibliográfica realizada, se han encontrado varias definiciones, de las cuales destacamos dos. La primera de la *Financial Conduct Authority* del Reino Unido, que ha sido una de las primeras en implementar los Sandbox Regulatorios de forma exitosa. Para la mencionada entidad, esta regulación proactiva está definida como un lugar para que las empresas prueben nuevas ideas, cumpliendo con la regulación exigida y permite acelerar el desarrollo y pruebas de nuevos productos en beneficio de los usuarios. La segunda definición pertenece a Corea del Sur, y de acuerdo con la modificación de la Ley de Convergencia de Información y la Comunicación, se define como un sistema en que las regulaciones no se aplican bajo ciertas condiciones, lo que facilita que las nuevas tecnologías y servicios innovadores puedan entrar de forma rápida al mercado.

No hay que olvidar, que los Sandbox Regulatorios se aplicaron inicialmente a los servicios financieros y que gracias a las nuevas tecnologías existe una cantidad amplia de campos de aplicación. Para cumplir con su objetivo, los Sandbox Regulatorios deben tener muy claro la problemática y la normativa que afecta su aplicación. Adicionalmente, es importante que los nuevos modelos de negocios sean propuestas que representen una innovación, no definida solamente por el uso de una nueva tecnología, sino también orientada a la definición de nuevos procesos que permitan prestar nuevos servicios mediante reducción de costos para impactar de forma positiva a los clientes.

De la revisión efectuada, y que se desarrollarán a continuación, las principales

11 Ver Centro de Estudios Avanzados en Banda Ancha para el Desarrollo (CEABAD). 2021. Modulo 1. Sandbox Regulatorios. Managua.

características de los Sandbox Regulatorios son:

1. Experimentales
2. Tienen un plazo limitado de vigencia
3. Se evalúan y ofrecen soluciones para cada caso.
4. Son excepcionales

Respecto al primer punto, los Sandbox Regulatorios se han implementado para innovar y contar con información del comportamiento del mercado ante nuevos modelos de negocios que no cumplan con la normativa vigente, que puede estar desactualizada o que genere dudas sobre su aplicabilidad. Esta etapa de innovación se ha establecido para probar nuevos modelos de negocios, pero también para verificar si la normativa aplicable o vigente es muy rigurosa respecto a ciertas condiciones específicas. En este sentido, las condiciones requeridas a los solicitantes se han flexibilizado para promover la inclusión de nuevas empresas y generar competencia. Estas menores exigencias permiten incluso la participación de empresas que no cuenten con las autorizaciones correspondientes para brindar el servicio, aunque una vez finalizada la duración del Sandbox Regulatorio, se deban contar con todos los requisitos solicitados.

Con relación al segundo punto, la temporalidad de los Sandbox Regulatorios es un detalle sumamente importante, dado que permite dar predictibilidad a las empresas y usuarios, por lo que siempre será necesario establecer un plazo máximo de duración de las propuestas innovadoras dentro del ambiente regulatorio especial, definido en el Sandbox Regulatorio.

El punto 3, también resulta determinante. Dado que las innovaciones que se pueden dar, son diversas y pueden aplicar soluciones distintas a varios problemas, las condiciones regulatorias especiales que se aplicarán a cada propuesta deben ser *ad-hoc* para cada caso, es decir, para problemas distintos, soluciones y regulaciones específicas. Si se cuenta con un esquema o propuesta general, esto le puede quitar eficiencia a los modelos de Sandbox Regulatorio.

Como se observará luego al analizar diversas prácticas internacionales, cuando se diseña un Sandbox Regulatorio, como las que proponen en la Guía de Promoción de la Innovación Financiera y Regulatoria (2018)¹² puede ser de mucha utilidad, formular las siguientes interrogantes:

- ¿La empresa busca ofrecer innovación que sea un negocio regulado o backup de otros negocios?
- ¿Es un negocio regulado?
- ¿Es la innovación pionera o constituye una oferta significativamente diferente en el mercado?
- ¿Existe algún beneficio para el consumidor?

12 Garvey, Kieran and Li, Wenwei and Shenglin, Ben and Zhang, Bryan Zheng and Rowan, Philip and Rauchs, Michel and Rau, P. Raghavendra and Ziegler, Tania and Rui, Hao. (2018). Guide to Promoting Financial & Regulatory Innovation: Insights from the UK. Disponible en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701847/UK_financial__regulatory_innovation.pdf

- ¿Se necesita un Sandbox Regulatorio?
- ¿Está la empresa lista para realizar pruebas? ¿Está la empresa lista para probar su innovación en un entorno en vivo?

El poder responder a estas preguntas será de mucha utilidad para diseñar un esquema específico para cada propuesta, dado que, de esta manera, se tiene definido claramente la problemática, el objetivo, cómo la innovación resuelve el problema y, los impactos en los usuarios. De esta forma, se podrá analizar de forma objetiva el éxito o fracaso de la propuesta.

Finalmente, está la excepción regulatoria. En este punto se entiende que el Sandbox Regulatorio no es permanente, sino que una alternativa temporal a la normativa vigente. Generalmente, los diversos participantes con frecuencia comentan que algunas soluciones no son posibles debido a la regulación existente. Con el Sandbox Regulatorio, los reguladores pueden probar la eficacia de este esquema y probar temporalmente en el mercado y usuarios, la aplicación de algunas medidas regulatorias.

En resumen, se puede concluir que los principales objetivos de un Sandbox Regulatorio son:

- Impulsar el desarrollo del mercado de un sector.
- Promover la competencia en algunos sectores mediante la innovación de productos, servicios y nuevos modelos de negocios.
- Reducir los costos y el tiempo de implementación de nuevas ideas que beneficien a los usuarios.
- Retirar barreras regulatorias que frenen la innovación.
- Garantizar una adecuada protección a los usuarios en tanto se implementen los nuevos productos o servicios.

2.1.1. Corea del Sur

Corea del Sur ha utilizado los Sandbox Regulatorios en el mercado financiero, especialmente para promover los servicios Fintech y su uso con las TIC. Como se comentó líneas arriba, el servicio de internet ha permitido el crecimiento de una serie de servicios, entre ellos, varias aplicaciones a los mercados financieros.

Dado que el sector Fintech es muy relevante para la implementación de políticas públicas a nivel mundial, el rápido crecimiento de ese sector y la poca competencia, el gobierno coreano gestionó durante el 2018, la propuesta de la Ley Especial de Apoyo a la Innovación Financiera para la introducción de un Sandbox Regulatorio financiero. Dicha norma fue aprobada en diciembre de ese año.

De acuerdo, a la información disponible en la página web del Fintech Center Korea (FCK)¹³, a la fecha se han aprobado cerca de 142 innovaciones en servicios financieros, desde la introducción de los Sandbox Regulatorios en mercados financieros en abril 2019.

13 Financial Regulatory Sandbox (2021). Financial Regulatory Sandbox Programs. Corea. <https://sandbox.fintech.or.kr/>

Los principales objetivos del Fintech Center Korea, son:

- Protección de valores públicos, mediante una búsqueda equilibrada entre el desarrollo de nuevas tecnologías, desarrollo de nuevas industrias y la protección, seguridad de las personas y del medio ambiente.
- Innovación regulatoria para acelerar el lanzamiento de nuevos productos y servicios.
- Procedimientos seguros, lo que implica supervisiones regulares para proteger a los consumidores frente a los riesgos de información que implica el uso de la tecnología.

En el caso de Corea, sólo aquellas empresas con presencia física en ese país pueden ser beneficiados del esquema de Sandbox Regulatorio. Para que una propuesta de innovación pueda aplicar al esquema de Sandbox Regulatorio, debe realizar un procedimiento de cinco (5) etapas (aplicación, revisión, decisión, supervisión y mejora regulatoria). Así pues, para que una propuesta pueda ser considerada, se evalúan los siguientes criterios:

- Región beneficiada. El servicio financiero debe ser brindado principalmente en el país.
- Servicio innovador respecto a los existentes.
- Que sea beneficioso a los consumidores.
- Excepción regulatoria inevitable. El servicio propuesto no puede ser brindado con la normativa regulatoria vigente.
- Califica adecuadamente para brindar el servicio propuesto.
- Medidas de gestión de riesgos y de protección al consumidor.

Como resultados se pueden observar casos de servicios de préstamos de contratos de seguros mediante el uso de inteligencia artificial o servicios de verificación sin utilizar la verificación facial en tiempo real, mediante verificación de otras credenciales autorizadas y validadas.

2.1.2. Reino Unido¹⁴

Como lo menciona Bijkerk (2021)¹⁵, el nombre Sandbox Regulatorio fue adoptado por la *Financial Conduct Authority* (FCA) de Reino Unido en 2015 dentro del *project innovate* que tiene como objetivo canalizar y apoyar los distintos productos o servicios ofrecidos a los clientes mediante innovación disruptiva. La FCA utiliza este enfoque para coordinar de forma constructiva con empresas innovadoras y eliminar regulaciones innecesarias que puedan frenar la innovación.

Como se aprecia en FCA (2021), esta entidad apoya a las empresas con propuestas de negocio innovadoras que promueven la innovación en beneficio de los consumidores.

La FCA está comprometida a favorecer propuestas innovadoras en servicios financieros y

14 Financial Conduct Authority. (2021). FCA Innovation – fintech, regtech and innovative businesses. [Https://www.fca.org.uk/firms/innovation](https://www.fca.org.uk/firms/innovation)

15 Bijkerk, W. 2021. Sandboxes regulatorios, hubs de innovación y más innovaciones regulatorias en América Latina y el Caribe. Washington, D.C.: BID.

dado el contexto actual de pandemia, la entidad cree que la innovación juega un rol muy importante frente a los desafíos resultantes de la pandemia ocasionada por el COVID-19. Además, están convencidos de apoyar a las firmas con propuestas innovadoras que tengan un impacto positivo en los usuarios y deseen probar sus proyectos en un mercado real.

De forma similar al modelo coreano, este modelo de Sandbox Regulatorio está enfocado en los mercados de servicios financieros, pero con un enfoque de combatir los efectos de la pandemia actual. En ese sentido, la FCA apoyará el desarrollo de nuevos negocios, productos o servicios que busquen:

- Detectar y prevenir fraudes y estafas.
- Apoyar la resiliencia financiera de usuarios vulnerables.
- Mejorar el acceso financiero a las pequeñas y medianas empresas.

Para que una propuesta pueda ser considerada, se requieren algunos requisitos. En el caso de la FCA, la empresa solicitante debe contar con un partner (por ejemplo, ser un proveedor tecnológico de una empresa regulada), a su vez, la empresa debe contar con una oficina principal en el Reino Unido, así como una cuenta bancaria en dicho país. En forma similar al modelo coreano, se consideran algunos de los siguientes criterios:

- Que busque innovar en un negocio regulado.
- Que la propuesta de innovación sea nueva o significativamente diferente de alguna que ya exista en el mercado.
- Que la propuesta de innovación ofrezca un beneficio directo a los usuarios.
- Que la empresa esté lista para realizar la propuesta innovadora en el mercado con usuarios reales.

Según la información de la FCA, a la fecha se han realizado siete convocatorias. Al momento de la redacción de este artículo, están en evaluación los resultados de la última. Durante el 2019, se presentaron 686 propuestas, de las cuales se aprobaron 101. En el Cohort 6 (etapa de presentación de propuestas, realizada durante el 2020), se presentaron 68 postulaciones y se aceptaron 22 propuestas de negocios para emplear el Sandbox Regulatorio y experimentar sus productos y servicios innovadores.

Varias de las propuestas presentadas estaban enfocadas en corregir la problemática de acceso y exclusión de los servicios financieros a la población vulnerable. La decisión de la FCA estuvo centrada en aquellas propuestas que el regulador estimó que podrían incrementar la demanda de servicios digitales como consecuencia del COVID-19.

Entre las propuestas aceptadas, se pueden destacar plataformas de educación financiera, custodia y transacciones de activos digitales utilizando tecnología de contabilidad distribuida y plataformas financieras de inversión sostenibles, que permitan la movilidad de capitales hacia proyectos verdes. Estos proyectos son beneficiados del SR para implementarse en el corto plazo y en un ámbito pequeño de aplicación.

2.1.3. Colombia¹⁶

¹⁶ Comisión de Regulación de Comunicaciones (2021a). Sandbox Regulatorio. Una zona segura de libertades creativas. <https://www.crc.com.gov.co/es/pagina/sandbox-regulatorio>

En la región latinoamericana, el primer Regulador que ha desarrollado una normativa para aplicar Sandbox Regulatorio al sector de telecomunicaciones ha sido la Comisión de Regulación de Comunicaciones (CRC, 2021a). De acuerdo al regulador colombiano, un Sandbox Regulatorio es “un mecanismo que otorga exenciones regulatorias a una empresa para que esta pueda probar nuevos productos, servicios o modelos de negocio, bajo la supervisión del regulador”.

El Sandbox Regulatorio en Colombia, tiene como objetivo “adaptar la regulación para impulsar la innovación en la provisión de redes y servicios de comunicaciones, priorizar el acceso y uso de las TIC especialmente en zonas de baja conectividad, incentivar la competencia y generar respuestas oportunas a los cambios de la industria”.

El caso colombiano es muy interesante dado que a diferencia de los casos revisados de Corea y del Reino Unido que estaban centrados en la industria Fintech, este modelo está enfocado en el sector de comunicaciones.

De acuerdo con la normativa de la CRC, el ámbito de aplicación del Sandbox Regulatorio son las empresas y proveedores de telecomunicaciones y servicios postales que están bajo el ámbito de competencia del regulador, así como proveedores de contenidos. En ese sentido, buscan soluciones innovadoras en cualquier aspecto de la provisión de redes y servicios de comunicaciones, lo que es un aspecto muy interesante ya que propicia la creatividad y modelos disruptivos.

Recién en abril del 2021 se ha abierto la convocatoria para la presentación de propuestas. Esta ventana fue ampliada hasta el 12 de mayo del 2021. De forma similar al modelo de la FCA, pudieron participar agentes no regulados bajo el ámbito de la CRC, pero conjuntamente con entidades reguladas, así como presentarse proyectos en asociación.

Siguiendo las buenas prácticas de Corea y del Reino Unido, las propuestas presentadas a la CRC debieron cumplir los siguientes criterios de selección:

- Innovación. Es decir, que la propuesta utiliza tecnologías de última generación, nuevas formas de utilizar la tecnología disponible o que no existen ofertas comerciales similares en el mercado.
- Beneficio a los ciudadanos. Este criterio consiste en que la propuesta de innovación puede brindar conectividad en zonas rurales o apartadas, incentiva la competencia en el sector de comunicaciones o puede tener un impacto positivo en la calidad del servicio o en las tarifas pagadas por usuarios.
- Necesidad demostrada, es decir, que no se puede aplicar bajo la normatividad vigente o que adaptar la propuesta al marco regulatorio actual implicaría una cantidad importante de inversión que haría inviable el mismo o anularía un posible impacto en términos económicos a los usuarios.
- Experiencia del proponente. Dicho criterio consiste en que el proponente hubiera realizado proyectos similares, así como demostrar que cuenta con los recursos para implementar la propuesta presentada al regulador.

Siguiendo el modelo de otros países, las autorizaciones concediendo la flexibilización necesaria se realizan caso por caso, lo que permite evaluar mejor cada propuesta y el marco regulatorio necesario. Una vez que empieza la fase de experimentación, ésta dura doce meses que se pueden prorrogar una sola vez y por el mismo plazo.

Una vez finalizado el periodo de aplicaciones, en Colombia se presentaron un total de

veinte y tres (23) proyectos. De ellos, veinte (20) son a nivel de usuarios en general, cinco (05) son a nivel nacional y dieciocho (18) están enfocados en zonas urbanas.

La CRC realizó una serie de comentarios a los proyectos presentados¹⁷ (2021b) y ha presentado un informe preliminar donde se explica, de forma sucinta, el alcance de los proyectos. Es de resaltar que se presentaron varios proyectos que buscan desplegar fibra óptica en zonas alejadas, formas alternativas de televisión (IPTV y televisión digital terrestre, TDT) y mecanismos menos costosos y de fácil compartición de antenas de telecomunicaciones (*Open Ran*). También existe un proyecto de redes comunitarias, así como un par de proyectos para mejorar la seguridad en los envíos del servicio postal. Se observan algunos proyectos muy interesantes también que son un contrato convergente para servicios móviles y fijos, infraestructura *fintech* para ciudades inteligentes, la creación de un registro único para IoT y un mecanismo para fomentar el comercio electrónico en zonas fronterizas.

La CRC remitió sus comentarios y las propuestas contaban con un plazo que venció el 21 de junio de este mismo 2021, para verificar la información proporcionada y empezar a analizar las propuestas al Sandbox Regulatorio.

Finalmente, la CRC publicó la lista de los proyectos aprobados para la segunda fase¹⁸. Estos proyectos ahora serán evaluados para verificar el impacto que pueden tener. En esta etapa hay diez (10) proyectos: Tres (03) se enfocan en desplegar fibra óptica, otros dos (02) se enfocan en adoptar mediciones de calidad de servicio; otros tres (03) buscan implementar o mejorar los servicios de telecomunicaciones para zonas rurales, una propuesta incluye redes comunitarias, o periurbanas con el uso de *Open Ran*. Los otros dos (02), tratan de flexibilizar condiciones vinculadas con la televisión digital abierta, y otro a generar un nuevo modelo de contrato convergente.

Como producto de esta segunda etapa de evaluación se espera que los resultados sean definidos y se publiquen para fines del mes de julio del 2021. Es interesante observar que en este proceso participan algunas de las principales empresas del sector, así como pequeños prestadores de telecomunicaciones.

En resumen, de la revisión de la literatura internacional, se puede concluir que el éxito de los Sandbox Regulatorios consiste en que: i) se desarrolle un marco de Sandbox Regulatorio para un sector determinado; ii) se brinde la flexibilidad regulatoria cuando la iniciativa no se puede desarrollar con la normativa vigente; iii) que la propuesta esté enfocada en promover la innovación beneficiando siempre a los usuarios; iv) deben ser temporales; v) participan los agentes regulados, en forma asociada con empresas no reguladas; y vi) deben servir para que el Regulador pueda realizar los ajustes necesarios, dado los resultados positivos de los proyectos propuestos.

2.2. ¿Qué hacemos en el Perú con las zonas donde no hay conectividad? Mecanismos tradicionales

La pandemia se ha constituido como el mayor acelerador digital y no cabe la menor

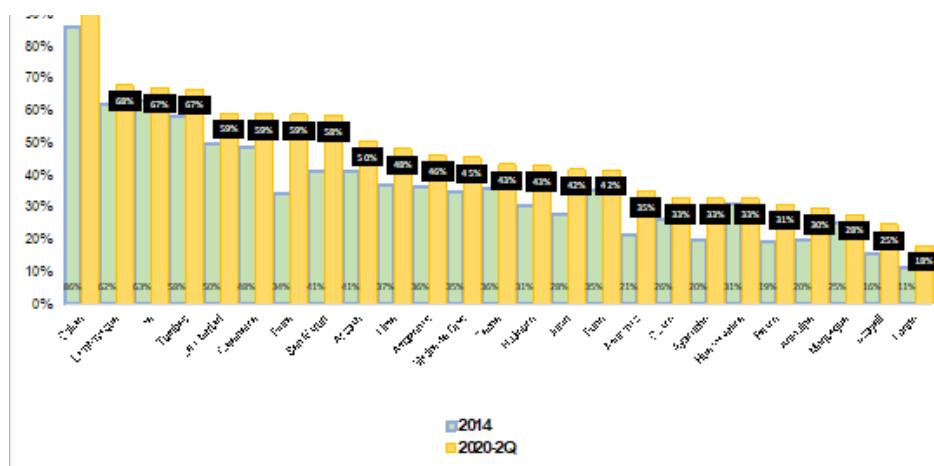
17 Comisión de Regulación de Comunicaciones (2021b). Informe preliminar de proponentes habilitados. https://www.crc.com.co/uploads/images/files/INFORME_PRELIMINAR_SANDBOX_REGULATORIO_CRC.pdf

18 Comisión de Regulación de Comunicaciones (2021c). Informe final de evaluación. Disponible en <https://www.crc.com.co/uploads/images/files/INFORME%20FINAL%20DE%20EVALUACION%20DE%20REQUISITOS%20HABILITANTES%20%20DE%20LA%20FASE%20DE%20APLICACI%C3%93N.pdf>

duda que se requiere de mecanismos expeditivos que permitan el despliegue de redes de telecomunicaciones tanto en fibra óptica como en infraestructura inalámbrica (lo que requerirá de incentivos tanto del lado de la oferta como de la demanda, en su oportunidad).

De acuerdo a la información estadística que publica OSIPTEL en el ERESTEL, el 76.2% de los hogares peruanos tiene acceso a Internet. Respecto al internet móvil, el 86.3% cuenta con dicho servicio, mientras el 30.25% de los hogares cuenta con internet fijo. Como se puede observar del siguiente cuadro, la necesidad de mayor cobertura es evidente a nivel nacional:

Gráfico 1. Porcentaje de Centros Poblados con Cobertura Móvil, 2014 y 2020



Fuente: Ministerio de Transportes y Comunicaciones (2020)¹⁹.

En vista a la evidente necesidad de incentivar el despliegue de redes móviles como fijas (fibra óptica), no sólo de redes de transporte, sino principalmente de escenarios de redes de fibra óptica que llegan hasta los clientes finales (FTTH), es decir, última milla²⁰, se considera más eficiente, explorar mecanismos que funcionan en la actualidad, incluso en nuestro propio país.

Un ejemplo de un mecanismo a utilizar es el Decreto Supremo N° 043-2006-MTC modificado por Decreto Supremo N° 003-2018-MTC, por el cual se aprobó una modificación al Reglamento del canon por el uso de espectro radioeléctrico para servicios públicos móviles de telecomunicaciones, el cual permite desplegar infraestructura como parte del cumplimiento de las obligaciones a cargo de las empresas operadoras móviles de telecomunicaciones, constituyendo un régimen especial aplicable únicamente a dichas empresas interesadas en acogerse al mismo. Esta normativa permite al Estado financiar, con cargo a los pagos que las empresas móviles deben efectuar por el uso del espectro

19 Ministerio de Transportes y Comunicaciones. (2020). Propuesta de asignación de bandas de frecuencia 3.5 GHz, y 26 GHz e Identificación de la banda de frecuencia de 6 GHz para el desarrollo de servicios y tecnologías digitales 5G. Versión 2. Disponible en <https://www.gob.pe/institucion/mtc/normas-legales/1322679-0796-2020-mtc-01-03>

20 Debido a que a través de ese medio de enlace se garantiza banda ancha fija (internet de alta velocidad).

radioeléctrico, las nuevas radiobases celulares de las empresas móviles que se acogen al régimen, siendo obligación de éstas, prestar servicios en dichas zonas, suscribiendo previamente los documentos contractuales correspondientes, y sujeto a la supervisión del MTC.

Dado el potencial de este mecanismo, mediante Decreto Supremo 004-2021-MTC, se amplió el porcentaje del Canon que puede ser solicitado por la empresa móvil hasta un equivalente al 40% de la recaudación estimada del canon anual para cada empresa. Dicho porcentaje puede modificarse a través de una Resolución Ministerial. Es de precisar que se consignan una lista de criterios a través de los cuales, el MTC publica en el Diario Oficial El Peruano, la Resolución Directoral que aprueba los dos listados de localidades, según corresponda: i) listado de localidades sin cobertura y/o ii) listado de localidades con infraestructura 2G únicamente. De dichos listados las empresas operadoras de servicios públicos móviles eligen en cuáles instalan infraestructura y/o mejoran la tecnología de la infraestructura para el año siguiente, las que se denominan localidades beneficiarias. Según información divulgada por el MTC²¹, este mecanismo beneficiará a 136 localidades durante el 2021, o lo equivalente a aproximadamente el 25% de un total de 40% que permite la normativa vigente.

A tenor de este antecedente, consideramos que el mecanismo debe ser transparentado y ampliado sus beneficios, con motivo de la coyuntura de emergencia sanitaria, dado que el Canon (que son recursos del Estado) está financiando únicamente el despliegue de infraestructura de redes móviles, cuando también podría financiar, el despliegue de redes fijas (fibra óptica) en zonas rurales y de preferente interés social, por parte de empresas concesionarias de servicios portadores o servicios fijos. Obviamente, ello implicaría elaborar una metodología *ad-hoc* aplicable a este nuevo escenario, lo cual es factible.

Finalmente, hay que destacar otros esfuerzos del ente rector del sector. A fines de abril de 2021, se emitió la Resolución Ministerial 373-2021-MTC/01, con la que se modificó el Plan Nacional de Atribución de Frecuencias (PNAF) para identificar espectro radioeléctrico para nuevas tecnologías como son los Espacios en Blanco de Televisión (TVWS por sus siglas en inglés), plataformas de gran altitud (HAPS) y WiFi6 que mejorará el uso de internet dentro de los hogares.

3. ¿QUÉ HACEMOS EN EL PERÚ CON LAS ZONAS DONDE NO HAY CONECTIVIDAD? PENSEMOS FUERA DE LA CAJA

En el caso peruano, el OSIPTEL cuenta con las facultades legales necesarias para poder formular normativa relacionada a los Sandbox Regulatorios, respecto de la normativa aprobada por este organismo. En efecto, con base en lo establecido en la Ley 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, OSIPTEL es un organismo público descentralizado adscrito a la Presidencia de Consejo de Ministros (PCM), con personería de derecho público interno, y con autonomía administrativa, funcional técnica, económica y financiera. Dentro de sus funciones principalísimas, se encuentra la Función normativa.

Artículo 3. Funciones

3.1, c) Función normativa: comprende la facultad de dictar en el ámbito y materias de su respectiva competencia, los reglamentos, normas que regulen los procedimientos a su cargo, otras de carácter general y mandatos u otras

21 <https://elperuano.pe/noticia/120369-canon-movil-favorecera-a-136-localidades-rurales>

normas de carácter particular referidas a intereses, obligaciones o derechos de las entidades u actividades supervisadas o de usuarios.²² (Ley 27332, 2000).

A su vez, el Reglamento General del OSIPTEL, aprobado por Decreto Supremo 008-2001-PCM, contiene principios que validan plenamente cualquier decisión del OSIPTEL que nos conduzca a los Sandbox Regulatorios, como son:

Art. 6. Principio de actuación basado en el Análisis Costo-beneficio

Los beneficios y costos de las acciones periódicas y programadas emprendidas por el OSIPTEL, serán evaluados antes de su realización y deberán ser adecuadamente sustentados en estudios y evaluaciones técnicas que acrediten su racionalidad y eficacia. Esta evaluación tomará en cuenta tanto las proyecciones de corto como de largo plazo, así como los costos y beneficios directos o indirectos, monetarios o no monetarios. (DS 008-2001-PCM, 2000).

Por otro lado, este Reglamento establece los criterios que las decisiones funcionales de OSIPTEL deberán tener en cuenta, y que nos parece sumamente pertinente para el presente análisis:

Art.13 Principio de Análisis de Decisiones Funcionales

El análisis de las decisiones funcionales del OSIPTEL tendrá en cuenta sus efectos en los aspectos de fijación de tarifas, calidad, incentivos para la innovación, condiciones contractuales y todo otro aspecto relevante para el desarrollo de los mercados y la satisfacción de los intereses de los usuarios. En tal sentido, deberá evaluarse el impacto que cada uno de estos aspectos tiene en las demás materias involucradas. (DS 008-2001-PCM, 2000).

De acuerdo a lo anterior, OSIPTEL cuenta con las facultades legales suficientes para conducir en el Perú, Sandbox Regulatorios respecto a la normativa aprobada por este organismo, lo cual nos parece sumamente necesario a efectos de poder incrementar conectividad, servicios, habilidades y competencias digitales, en suma, coadyuvar decididamente en la transformación digital que resulta indispensable, más ahora en esta nueva normalidad post pandemia. Por eso, debemos tener presente que, entre los objetivos específicos del Regulador, se encuentran dos objetivos potentes, que se consideran en el Art. 19 del Reglamento General de OSIPTEL, a saber, (i) literal b) garantizar el acceso universal a los servicios públicos de telecomunicaciones y (ii) literal g) facilitar el desarrollo, modernización y explotación eficiente de los servicios de telecomunicaciones.

22 OSIPTEL cuenta con función normativa y función reguladora. El Reglamento General de OSIPTEL (DS 008-2001-PCM), establece lo siguiente:

“Artículo 23.– Definición de Función Normativa

La función normativa permite al OSIPTEL dictar de manera exclusiva y dentro del ámbito de su competencia, reglamentos y normas de carácter general, aplicables a todos los administrados que se encuentren en las mismas condiciones. Estos reglamentos podrán definir los derechos y obligaciones entre las empresas operadoras y de éstas con los usuarios.

Asimismo, comprende la facultad de dictar mandatos y normas de carácter particular; referidas a intereses, obligaciones o derechos de las entidades o actividades bajo su competencia, o de sus usuarios.”

“Artículo 28.– Función Reguladora.

Es la facultad que tiene OSIPTEL de fijar tarifas de los servicios públicos de telecomunicaciones.”

Por su lado, el Ministerio de Transportes y Comunicaciones (MTC) se encuentra también facultado para aprobar normativa relativa a los Sandbox Regulatorios en materias de su competencia. En efecto, como ente rector y bajo lo establecido en el Texto Único Ordenado de la Ley de Telecomunicaciones (aprobado con Decreto Supremo 013-93-TCC), el MTC —a través de decretos supremos sectoriales— podría exonerar del cumplimiento de metas de uso, asignar temporalmente espectro, exonerar de pagos por concepto de Canon, exoneración de las mediciones de los Límites Máximos Permisibles -LMP por cada instalación de antenas de telecomunicaciones, entre otros.

Artículo 75.- Además de las atribuciones señaladas en su propia Ley Orgánica, son funciones del Ministerio de Transportes, Comunicaciones, Vivienda y Construcción en materia de telecomunicaciones, las siguientes:

1.- Fijar la política de telecomunicaciones a seguir y controlar sus resultados.

(...)

8.- Incentivar el desarrollo de las industrias de telecomunicaciones y de servicios informáticos sustentados en base a servicios de telecomunicaciones en orden al desarrollo tecnológico del país.

(...)

Es de precisar que el Reglamento General de la Ley de Telecomunicaciones, aprobado con Decreto Supremo 020-2007-MTC, establece lo siguiente:

Artículo 12.- Proyectos de telecomunicaciones

El Ministerio promoverá y desarrollará proyectos de telecomunicaciones incluyendo proyectos piloto, especialmente aquellos dirigidos a cumplir con los fines del acceso universal y que tengan como finalidad, impulsar el acceso a las Tecnologías de la Información y Comunicación (TICs) y el desarrollo de la Sociedad Global de la Información y el Conocimiento. (DS 020-2007-MTC, 2007).

Por lo expuesto, tanto el MTC como OSIPTEL, pueden dictar normativa en materias de sus competencias, que posibiliten la realización de Sandbox Regulatorios. Estas facultades no son menores, ya que permiten llevar a cabo estos Laboratorios de Prueba dentro del sector, sin depender de otros sectores u entidades, que a veces conlleva a demoras, y porqué no decirlo, a barreras para implementar ideas creativas dentro del propio Estado.

3.1. Plan “Flexibilizar para Conectar”

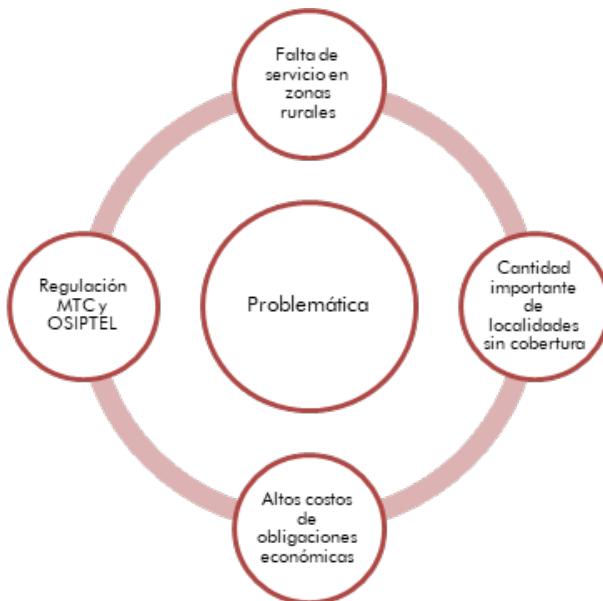
Como se ha expresado a lo largo del presente documento, hoy mas que nunca se evidencia la gran necesidad de contar con infraestructura de telecomunicaciones en todo el País, lo que se logra a través de una decidida colaboración público-privado, que conjuge a todos los actores del ecosistema digital.

La infraestructura de telecomunicaciones es crítica para soportar el accionar económico y social de hoy en día. Es una infraestructura robusta, innovadora y cambiante. El acceso a ella, al internet, a los servicios de telecomunicaciones y las tecnologías de la información es un derecho humano que permite habilitar el ejercicio de otros derechos fundamentales como la salud, la educación, la cultura, la seguridad, la libertad de expresión y la movilidad entre otros. Esta infraestructura es estratégica, porque en situaciones críticas como la que se enfrenta al COVID-19, preserva el ejercicio de estos derechos y es el mejor

aliado de los gobiernos y la sociedad para mantener la economía.²³ (Agudelo et al., 2020, p. 3).

Como se comentó en la primera sección, existe una gran cantidad de centros poblados y de ciudadanos que aun no cuentan con las bondades y beneficios de la conectividad. Dada la nueva normalidad, es sumamente importante, brindar los mecanismos regulatorios que permitan reducir no solo la brecha digital, sino también el tiempo de implementación de las nuevas tecnologías al interior del país.

Gráfico 2. Problemática del sector telecomunicaciones



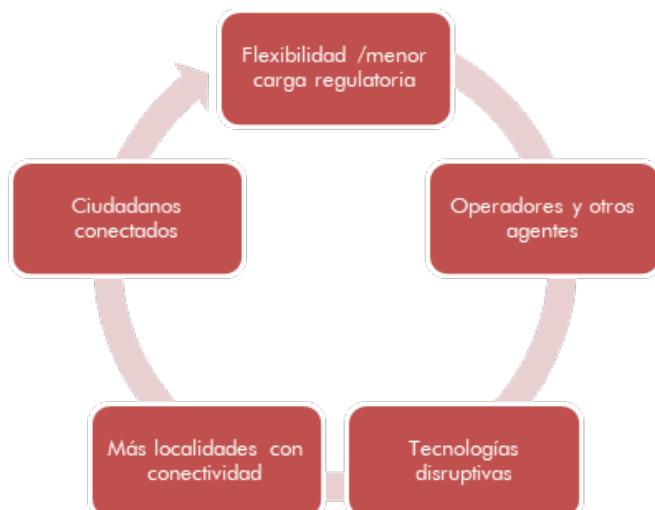
En ese sentido, nuestra propuesta no sólo consiste en llevar a cabo, Sandbox Regulatorios en materia de telecomunicaciones en el Perú, sino ir más allá y llevar a cabo lo que hemos denominado como "**Plan Flexibilizar para Conectar**", que permita que los diversos agentes puedan presentar propuestas innovadoras que cumplan con los siguientes objetivos:

- i) Impulsar la conectividad en zonas de baja o nula conectividad.
- ii) Incentivar el uso de tecnologías nuevas y/o disruptivas.
- iii) Que dichas propuestas beneficien a los usuarios y generen mayor competencia.

Con estos objetivos, se espera lograr un círculo virtuoso de conectividad que se puede graficar de la siguiente manera:

23 Agudelo M, Chomali E, Suniaga J, Nuñez G, Jordán V, Rojas F, et al. (2020). Las oportunidades de la digitalización en América Latina frente al Covid-19. Santiago de Chile: CEPAL.

Gráfico 3. Círculo virtuoso de conectividad en zonas con limitada o nula conectividad



Elaboración propia.

Como hemos indicado líneas arriba, de acuerdo con la revisión de casos internacionales, el Sandbox Regulatorio flexibiliza la normativa regulatoria. Sin embargo, la normativa que debiera ser materia de evaluación y en su caso, de ingresar al Sandbox Regulatorio, debiera considerar dos fuentes: la normativa aprobada por el Regulador, esto es, OSIPTEL, y la normativa aprobada por el MTC, cada uno en materias de su competencia.

Por ello, el **Plan Flexibilizar para Conectar** que proponemos, involucra a la normativa de ambas entidades, lo que implica un nivel colaborativo importante entre el ente rector (MTC) y el regulador (OSIPTEL). Así, luego de conversar con diversos actores del sector y analizar diversas experiencias internacionales, entre las principales consideraciones y flexibilidades regulatorias y/o normativas que se aplicarían, de acuerdo con las necesidades de las distintas iniciativas que se puedan presentar, se podrían enumerar las siguientes:

- Participantes. Podrían participar empresas bajo el ámbito de regulación del MTC, así como empresas no reguladas, siempre que cuenten con un socio regulado por el Ministerio.
- Ámbito de aplicación. La flexibilidad regulatoria y/o normativa sólo se aplicaría en las localidades aprobadas para el desarrollo de las propuestas y en zonas de limitada o nula conectividad.
- Temporalidad de la flexibilidad normativa. Sería un plazo de tres años, ampliable por dos años adicionales, para generar los incentivos necesarios para atraer proyectos y un plazo adecuado para generar la predictibilidad para la recuperación de las inversiones.
- Incentivar la competencia. Las iniciativas aprobadas deben brindar facilidades de acceso a cualquiera que requiera utilizar sus servicios.
- Asignación temporal de espectro, siempre que exista disponibilidad y no

genere interferencias, para poder emplear tecnologías disruptivas, con el fin de poder brindar alternativas de conectividad.

- Exoneración de pago de canon (móvil, satelital)²⁴, así como la no aplicación de los indicadores de metas de uso aprobadas por el MTC en las zonas o localidades donde se desarrollen las propuestas aprobadas.
- Exoneración de la medición de Límites Máximos Permisibles para la nueva infraestructura de telefonía móvil que se despliegue en las zonas beneficiadas. Las empresas, al final de cada año, realizarán la medición a una muestra del total de antenas instaladas en las localidades de los proyectos.
- Normativa de calidad. Dado que en las localidades donde se aplicarán las iniciativas, la conectividad es limitada o nula, se propone la inaplicabilidad de la normativa de cobertura establecida por el OSIPTEL, con el objetivo de incentivar a las empresas a conectar localidades.
- Obligaciones. Sin perjuicio de algunos indicadores que se puedan establecer para cada iniciativa aprobada, hay dos que siempre se exigirán: i) que las empresas incluyan esas localidades como zonas con cobertura; ii) contar con una oferta comercial adecuada al ámbito de influencia de la iniciativa.

3.2. Análisis de Impacto Regulatorio

En las secciones anteriores, se explicó qué es un Sandbox Regulatorio, así como el plan Flexibilizar para Conectar como una propuesta de menor regulación que busca incentivar la conectividad mediante la innovación tecnológica. En esta sección se realizará un análisis cualitativo respecto a las bondades del Plan Flexibilizar para Conectar.

Alternativa 1: No intervenir y mantener el status quo

| | Estado | Usuario | Empresas |
|-------------|---|---|--|
| Ventajas | No se implementan cambios regulatorios | Mantiene situación actual | Enfocan inversiones en zonas urbanas o de mayor densidad poblacional |
| Desventajas | Uso ineficiente de los recursos como el espectro radioeléctrico Indicadores bajos de conectividad Menor impacto en el crecimiento económico | Sin conectividad Mala calidad del servicio | Mala calidad del servicio. Riesgo de multas por incumplimiento de normativa MTC u OSIPTEL |

24 En general, desplegar infraestructura en zonas alejadas, no es un caso de negocio para los operadores. Por eso, una idea, sería exonerar del pago de obligaciones económicas para generar incentivos a las empresas.

Alternativa 2: Intervención regulatoria con implementación del Plan Flexibilizar para Conectar

| | Estado | Usuario | Empresas |
|-------------|---|--|--|
| Ventajas | <p>Mayor impacto en el PBI, dado el incremento de conectividad</p> <p>Uso eficiente de los recursos escasos como el espectro radioeléctrico</p> | <p>Tiene conectividad</p> <p>Mejora la calidad del servicio</p> <p>Oferta comercial especial</p> <p>Mejora en los ingresos mensuales, como consecuencia de contar con internet</p> | <p>Mejora la calidad del servicio (impacto reputacional)</p> <p>Sin riesgo de multas por incumplimiento de normativa flexibilizada</p> <p>Plazo adecuado para generar inversiones con retorno económico y social</p> |
| Desventajas | <p>Elaboración normativa</p> <p>Análisis de las propuestas que aplican al SR</p> <p>Revisión de normativa de forma excepcional</p> | | Mayores inversiones |

Se observa que los beneficios cualitativos del esquema propuesto son mayores a los costos de implementación, así como de mantener el *status quo*. De acuerdo con los documentos de trabajo publicados por el MTC, se pueden resumir los beneficios de la conectividad en dos aspectos principales:

- Los hogares rurales que tuvieron acceso a internet fijo han visto una mejora en sus ingresos mensuales de S/ 390.
- El resultado del incremento de diez (10) puntos porcentuales de hogares conectados impactaría en 2% el PBI. Si medimos con el PBI del 2019, ese monto equivale a casi once mil millones de soles.

Es muy importante, contar con indicadores de cobertura y de hogares nuevos conectados, dado que así se podrá analizar la evolución de los despliegues, así como su impacto. El Sandbox Regulatorio propuesto, en forma conjunta con otras medidas propuestas, deben permitir conectar a una mayor cantidad de hogares. A modo de ejercicio, se hizo el siguiente análisis:

- Existen aproximadamente 10 millones de hogares en el Perú.
- Según el ERESTEL, el 76,2% de los hogares cuentan con internet.
- La brecha de hogares sin internet es de 2,4 millones.
- Conectar a 10% de los 2,4 millones de hogares, en zonas rurales.

Los resultados de este ejercicio se obtuvieron considerando los resultados de los estudios realizados por el equipo técnico del MTC, y los compartimos a continuación.



Si bien son estimaciones gruesas, el esfuerzo por realizar estas medidas, son recompensadas por un mayor ingreso de los hogares impactados, así como un impacto de 0,48% en la economía. Medidas de esta naturaleza, sobretodo en el contexto actual, en el que se necesita seguir reactivando la economía luego del Covid-19, y sobretodo permitir conectar a nuevos hogares, son imprescindibles.

3.3. ¿Es suficiente un Sandbox Regulatorio para mejorar la conectividad?

Es muy importante detenernos y puntualizar lo siguiente: El Sandbox Regulatorio daría la flexibilidad regulatoria temporal, respecto a normas emitidas por el ente rector y el Regulador y sujeto a que dicha decisión pueda ser modificada, en cualquier momento. Por ello, para incentivar un clima de inversiones predecible, sería pertinente que la propia normativa establezca el plazo mínimo en que dicho marco estará vigente, para que las empresas puedan realizar su evaluación económica-financiera en el tiempo, y fluya un escenario *win to win*. O dicho en otra manera, el Sandbox Regulatorio daría el periodo de prueba y el perfil de un nuevo producto o servicio, que en la siguiente etapa ya de “producción”, requeriría de un nuevo marco regulatorio con vocación de permanencia. De esta manera, estos mecanismos ayudarían a incrementar un entorno digital que promueve la conectividad y el acceso de más peruanos a los servicios de telecomunicaciones, es decir, el acceso universal.

Sin embargo, no hay que olvidar que existe normativa no sectorial que sería indispensable que acompañara estos esfuerzos para conectar a los no conectados. Para lograr ese objetivo, el MTC requeriría de una Base Legal que le facultara para ello; por tanto, recomendamos una Ley o Decreto Legislativo por el cual, se habilitara al MTC a efectos que vía Decreto Supremo –con el refrendo de PCM-, identifique regiones carentes de infraestructura y de acceso a internet, disponiendo la suspensión total o parcial, de la normativa relacionada a los permisos para el despliegue de redes de telecomunicaciones a efectos de promover la expansión de infraestructura y de conectividad digital, por un plazo mínimo de tres (3) años, renovable (previa verificación del crecimiento de conectividad) hasta por un máximo de diez (10) años.

En forma adicional, permitir que el monto de las multas impuestas por el incumplimiento de la normativa del MTC u OSIPTEL, siempre que no se judicialicen, no sea entregado al Fondo FITEL sino que las empresas puedan utilizar esos recursos para desplegar redes de fibra óptica en zonas (periurbanas o rurales) donde no llegan con la mencionada

tecnología. Esto debido a que, en la actualidad, dicho fondo ya tiene la totalidad de sus recursos comprometidos en el financiamiento de los proyectos regionales de fibra óptica.

A su vez, que se habilite al MTC con la finalidad de que pueda destinar un monto a determinar del canon móvil que se recauda por el uso de frecuencias en dichas regiones, para financiar la infraestructura de las empresas móviles que desplieguen red en dichas zonas, siempre que (i) exista el compromiso de seguir prestando los servicios, bajo el principio de continuidad; (ii) que presten una tarifa social que únicamente cubra los costos, bajo supervisión del Regulador y iii) la obligación de brindar el roaming nacional en esas localidades.

En este orden de ideas, resulta interesante la experiencia de Ecuador, en que se viene implementando la política de ECUADOR DIGITAL, que tiene el eje de ECUADOR CONECTADO, el cual tiene por objetivo conectar al 98% de las parroquias (localidades) existentes a escala nacional, a través de la dotación de servicios de voz o datos.

En efecto, a través del Ministerio de Telecomunicaciones y de la Sociedad de la Información – MINTEL y la Corporación Nacional de Telecomunicaciones - CNT E.P. (²⁵), mediante acuerdos, están implementando el proyecto “Conectando Comunidades”, que implica que el MINTEL, a través de la CNT, gestiona la instalación de cientos de puntos WiFi a escala nacional, en colaboración con los Gobiernos Autónomos Descentralizados (GAD, que en Perú serían los Gobiernos Regionales). Los puntos de conectividad funcionan bajo la plataforma Express WiFi de Facebook. La CNT provee el servicio de conectividad e instalación; y, el GAD se encarga de la definición de sitios y de la forma de gestionar los mismos²⁶.

-
- 25 CNT es la empresa estatal que presta servicios de telecomunicaciones. Téngase presente que, en Ecuador, las telecomunicaciones son calificadas como “Sector Estratégico”, y en forma excepcional, se permite la actividad de las empresas privadas. A saber, la Constitución Ecuatoriana establece lo siguiente:

“Capítulo quinto Sectores estratégicos, servicios y empresas públicas

Art. 313.- El Estado se reserva el derecho de administrar, regular, controlar y gestionar los sectores estratégicos, de conformidad con los principios de sostenibilidad ambiental, precaución, prevención y eficiencia. Los sectores estratégicos, de decisión y control exclusivo del Estado, son aquellos que por su trascendencia y magnitud tienen decisiva influencia económica, social, política o ambiental, y deberán orientarse al pleno desarrollo de los derechos y al interés social. Se consideran sectores estratégicos la energía en todas sus formas, las telecomunicaciones, los recursos naturales no renovables, el transporte y la refinación de hidrocarburos, la biodiversidad y el patrimonio genético, el espectro radioeléctrico, el agua, y los demás que determine la ley.” (el resaltado es nuestro)

“Art. 316.- El Estado podrá delegar la participación en los sectores estratégicos y servicios públicos a empresas mixtas en las cuales tenga mayoría accionaria. La delegación se sujetará al interés nacional y respetará los plazos y límites fijados en la ley para cada sector estratégico.

El Estado podrá, de forma excepcional, delegar a la iniciativa privada y a la economía popular y solidaria, el ejercicio de estas actividades, en los casos que establezca la ley”.

- 26 Esta iniciativa permite la unión de los esfuerzos del Gobierno Central con los GAD (Gobiernos Regionales) para llevar conectividad a las zonas sin servicio. Así pues, con el **Plan de Conectividad Social “Conectando Comunidades”**, se propone mediante trabajo mancomunado, enlazar al Gobierno Central y los GAD para brindar conectividad de calidad, impulsar la economía, generar inclusión social y financiera de comunidades más alejadas, así como iniciar un proceso de adopción tecnológica que presente como resultado el uso de comercio electrónico, así como, trámites en línea. De acuerdo a las noticias en la página web del MINTEL, se observa que el MINTEL brinda asesoría técnica, elabora portafolio de

En otro escenario, en Ecuador están implementando conexiones de redes de fibra óptica en áreas rurales financiadas por empresas privadas (tales como mineras, por ejemplo). Estas redes de última milla, financiadas voluntariamente por la empresa privada que así lo deseé, pasan a formar parte de la red de CNT, a título gratuito. A su vez, CNT, quien incorpora esos activos a la empresa, presta el servicio de acceso a internet en dichas zonas, a través de una tarifa social. Este escenario nos resulta interesante ya que es un ejemplo de colaboración público-privado con muchas posibilidades.

De acuerdo a lo anterior, y en vista a la inexistencia en el Perú de un brazo operativo como es la CNT²⁷, consideramos eficiente, que se establezca un espacio colaborativo (a) MTC, (b) Empresa Concesionaria, (c) Empresa que financia red, y (d) Localidades a conectar, por el cual, se viabilice que empresas privadas ubicadas en zonas rurales o de preferente interés social –de así quererlo-- financien a su costo, la instalación de redes de fibra óptica en las localidades de su interés y que carezcan de conectividad. La Empresa Concesionaria plantea su proforma técnica– económica, siguiendo los lineamientos técnicos del MTC, y de ser aceptada, se suscriben los documentos contractuales correspondientes por los cuales, se aprueba el Proyecto, y se incorpora como obligación contractual de la concesionaria, la continuidad del servicio y los paquetes o planes sociales que se ofrecerán a dichas localidades, sujeto a la supervisión del Regulador. Consideramos que la presencia técnica del MTC y el carácter vinculante que se puede brindar al Proyecto en si, es importante para que empresas privadas puedan ofrecer este tipo de financiamiento para el acceso a internet en las áreas en que realizan actividades económicas, por ejemplo.

Por último, es muy importante identificar un umbral (poblacional, geográfico, de ingresos), de forma tal que, por encima de ese umbral, es posible utilizar el Sandbox Regulatorio; caso contrario, se necesita intervención directa del Estado para poder conectar esas localidades. Aquí se pueden destacar algunas iniciativas de países como Estados Unidos, Reino Unido o Colombia, que impulsan la reducción de la brecha de conectividad impulsando proyectos de subsidio a la demanda.

4. CONCLUSIONES

1. Los esquemas de Sandbox Regulatorios son una alternativa que permitirán conectar a más hogares, sobre todo en zonas con menor densidad poblacional o de difícil acceso, a través del incremento de una economía digital. La implementación de escenarios de prueba que requieren la suspensión temporal de normativa que impide u obstaculiza su desarrollo, permitirá que las autoridades hagan una evaluación de sus resultados en campo, y de generar valor positivo, plantear y modificar la normativa en búsqueda de que dicho valor positivo sea sostenible en el tiempo, de así considerarlo.
2. Los Sandbox Regulatorios permiten que se constituya un laboratorio regulatorio para trabajos en campo, sin que dicha intervención pueda generar efectos permanentes negativos. Las decisiones regulatorias siempre buscan no generar

soluciones y efectúa la gestión con los prestadores del servicio. A su vez, los GAD detectan las necesidades, facilitan los permisos de despliegue e instalación, socializan el proyecto y sus beneficios, y lo financian, de ser necesario. Las soluciones que se plantean son (i) Puntos WIFI fijos, (ii) Puntos WIFI satelitales y (iii) WIFI Comunitario. Resultará interesante evaluar los resultados de este Plan de cara a incentivar el involucramiento de los Gobiernos Regionales en materia de conectividad en nuestro País.

27 La existencia de empresas estatales en el sector de las comunicaciones en el Perú tuvo en la CPT S.A. y ENTEL S.A., su más negativa experiencia.

externalidades negativas o distorsionar el mercado, por lo que la posibilidad de incentivar la creatividad y la prueba y error, potencian los resultados a favor de una economía digital sólida y, por ende, vuelve atractivo las zonas impactadas con el Sandbox Regulatorio para la implementación de la infraestructura necesaria para la conectividad.

3. La propuesta del Plan Flexibilizar para Conectar busca ir más allá de las normas emitidas por el Regulador, incluyendo las normas del MTC lo que implica un esfuerzo colaborativo importante entre ambas entidades estatales, conducente a generar potentes espacios creativos, ante las circunstancias complejas de falta de conectividad, y de una real transformación digital. Ello sin duda involucra la colaboración de los agentes de mercado, no sólo en la generación de ideas, sino en el real compromiso de llevar a la realidad estos Laboratorios.
4. Para lograr una infraestructura que implique el acceso a más servicios de telecomunicaciones, se necesita un esfuerzo, no sólo sectorial, sino también a nivel del Poder Ejecutivo y con la asistencia de los gobiernos regionales y locales, para facilitar el despliegue de infraestructura.
5. Los impactos positivos en la conectividad son tangibles para los que vivimos en zonas urbanas, pero permitirán cambiar la vida de los peruanos que viven en zonas con limitada o sin conectividad.
6. La colaboración público-privada es esencial, hoy más que nunca, para lograr la conectividad y la transformación digital que requiere el País.

BIBLIOGRAFÍA

- Agudelo M, Chomali E, Suniaga J, Nuñez G, Jordán V, Rojas F, et al. (2020). *Las oportunidades de la digitalización en América Latina frente al Covid-19*. CEPAL.
- Aguilar, J.; Gil Malca, C.; Aparco, E.; Acosta, D.; Cajavilca, A.; Rusbel, A.; Asencios, L.; Roque, E. y Robles, F. (2020). *Impacto económico del acceso a internet en los hogares peruanos*. Documento de trabajo N° 01. MTC. <https://www.gob.pe/institucion/mtc/informes-publicaciones/1359614-impacto-economico-del-acceso-a-internet-en-los-hogares-peruanos>
- Aguilar, J.; Gil Malca, C.; Aparco, E.; Acosta, D.; Asencios, L. y Robles, F. (2021). *Impacto del acceso a internet en el crecimiento económico del Perú: Un enfoque ARDL*. Documento de trabajo N° 02. MTC. <https://www.gob.pe/institucion/mtc/informes-publicaciones/1625507-impacto-del-acceso-a-internet-en-el-crecimiento-economico-del-peru-un-enfoque-ardl>
- Banco Mundial. (2018). *Informe Diagnóstico del Estado Actual del Mercado de Banda Ancha y Posicionamiento de la Red Dorsal Nacional de Fibra Óptica (RDNFO) en el Mercado* (Informe). https://portal.mtc.gob.pe/comunicaciones/regulacion_internacional/regulacion/proy%20normativos/2019/Informe_DiagnosticoBancoMundial.pdf
- Banco Mundial. (2019). *Informe 2 – Escenarios y Modelos de Negocio para la RDNFO y Redes de Transporte Regionales* (Informe). https://cdn.www.gob.pe/uploads/document/file/493980/Informe_2_Banda_Ancha_Banco_Mundial.pdf
- Bijkerk, W. (2021). *Sandboxes regulatorios, hubs de innovación y más innovaciones*

- regulatorias en América Latina y el Caribe. BID.
- CAF. (2020). *El estado de la digitalización de América Latina frente a la pandemia del COVID-19*. Abril. CAF. <https://scioteca.caf.com/handle/123456789/1540>
- Centro de Estudios Avanzados en Banda Ancha para el Desarrollo (CEABAD). (2021). *Modulo 1. Sandbox Regulatorios*. Managua.
- Comisión de Regulación de Comunicaciones. (2021a). *Sandbox Regulatorio. Una zona segura de libertades creativas*. <https://www.crc.com.gov.co/es/pagina/sandbox-regulatorio>
- Comisión de Regulación de Comunicaciones. (2021b). *Informe preliminar de proponentes habilitados (Informe)*. https://www.crc.com.gov.co/uploads/images/files/INFORME_PRELIMINAR_SANDBOX_REGULATORIO_CRC.pdf
- Comisión de Regulación de Comunicaciones. (2021c). *Informe final de evaluación (Informe)*. <https://www.crc.com.gov.co/uploads/images/files/INFORME%20FINAL%20DE%20EVALUACION%20DE%20REQUISITOS%20HABILITANTES%20%20DE%20LA%20FASE%20DE%20APLICACI%C3%93N.pdf>
- Financial Conduct Authority. (2021). *FCA Innovation – fintech, regtech and innovative businesses*. <https://www.fca.org.uk/firms/innovation>
- Financial Regulatory Sandbox. (2021). *Financial Regulatory Sandbox Programs*. Corea. <https://sandbox.fintech.or.kr/>
- García, A. (2020). *Infraestructura digital como herramienta social y económica*. <https://blogs.iadb.org/innovacion/es/infraestructura-digital-como-herramienta-social-y-economica/>
- Garvey, Kieran and Li, Wenwei and Shenglin, Ben and Zhang, Bryan Zheng and Rowan, Philip and Rauchs, Michel and Rau, P. Raghavendra and Ziegler, Tania and Rui, Hao. (2018). *Guide to Promoting Financial & Regulatory Innovation: Insights from the UK*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701847/UK_financial__regulatory_innovation.pdf
- Ministerio de Transportes y Comunicaciones. (2019). *Base Legal OIMR*. <https://www.gob.pe/institucion/mtc/informes-publicaciones/355532-base-legal-oimr>
- Ministerio de Transportes y Comunicaciones. (2019). *Informe 946-2019-MTC/26. Informe de sustento del Decreto Supremo 002-2020-MTC*. https://cdn.www.gob.pe/uploads/document/file/493981/Informe_946-2019-MTC-26-comprimido.pdf
- Ministerio de Transportes y Comunicaciones. (2020). *Propuesta de asignación de bandas de frecuencia 3.5 GHz, y 26 GHz e Identificación de la banda de frecuencia de 6 GHz para el desarrollo de servicios y tecnologías digitales 5G Versión 2*. <https://www.gob.pe/institucion/mtc/normas-legales/1322679-0796-2020-mtc-01-03>
- Ministerio de Transportes y Comunicaciones. (2021). *Caducidad del Contrato de Concesión del Proyecto “Red Dorsal Nacional de Fibra Óptica: Cobertura Universal Norte, Cobertura Universal Sur y Cobertura Universal Centro (Informe 008-2021-MTC/27.01)*. <https://cdn.www.gob.pe/uploads/document/file/1736774/Informe%20N%C2%B0008-2021-MTC/27.01.pdf>

OSIPTEL. (2018). *Consulta Pública sobre el Proyecto “Mecanismos supervisados de compartición y acceso en la industria de servicios móviles”* (Informe 242-GPRC/2018). Lima.

Savona, M. (2020). ¿La “nueva normalidad” como “nueva esencialidad”? COVID-19, transformaciones digitales y estructuras laborales. *Revista de la Cepal*, (132), 209-224.



LA UNIVERSALIDAD HACIA LAS TIC EN COLOMBIA

UNIVERSALITY TOWARDS ICT IN COLOMBIA

LUZ MÓNICA HERRERA ZAPATA¹
LAURA DANIELA GONZÁLEZ ROZO²

RESUMEN

Las Tecnologías de la Información y las Comunicaciones (TIC) han revolucionado la forma de vivir de las personas. Sin embargo, como consecuencia de la brecha digital, no todos pueden beneficiarse de ellas, lo cual implica la vulneración de los derechos fundamentales que se ejercen a través de aquellos medios. Esta situación se ha visto especialmente acentuada a raíz de la pandemia de COVID-19.

En ese contexto, se ha hablado del acceso y servicio universal como herramientas para lograr la inclusión digital de toda la población, mediante su inserción en el ecosistema digital y la Cuarta Revolución Industrial. Para lograr esa universalidad, en Colombia se ha generado un marco legal y desarrollo jurisprudencial que busca aumentar la cobertura, infraestructura y apropiación de las TIC por parte de la población. Estas normas y decisiones serán analizadas en el presente artículo.

Adicionalmente, se hará una breve referencia al caso del Perú. Se le comparará con el caso colombiano a fin de encontrar puntos en común entre ambos. Finalmente, se brindará una serie de recomendaciones en aras de lograr el acceso y servicio universal en los dos países, con base principalmente en la experiencia colombiana.

ABSTRACT

Information and Communication Technologies have revolutionized people's lives. However, as a consequence of the digital divide, not everyone can benefit from them, which leads to the violation of fundamental rights that are exercised through these instruments. This situation has increased and become more noticeable as a result of the COVID-19 pandemic.

In this context, universal access and service have been discussed as tools to achieve digital inclusion through the insertion of the population into the digital ecosystem and the Fourth Industrial Revolution. To achieve this universality, Colombia has developed a legal framework and some jurisprudence looking forward to increase coverage, infrastructure, and appropriation of ICT by the population. The aforementioned legislation and decisions will be analysed in this article.

Additionally, a brief reference will be made to the case of Peru, comparing it with the Colombian case, trying to find common points between both. Lastly, the article will provide recommendations to achieve universal access and service in both countries.

1 Abogada, con especialización en Derecho de las Telecomunicaciones y en Derecho Comercial de la Universidad Externado de Colombia. Doctora en Sociología Jurídica e Instituciones Políticas de la misma Universidad. Docente Investigadora y directora (e) del Departamento de Derecho de las Telecomunicaciones de la Universidad Externado de Colombia. Contacto: luz.herrera@uexternado.edu.co

2 Abogada de la Universidad Externado de Colombia. Investigadora del Departamento de Derecho de las Telecomunicaciones de la Facultad de Derecho de la misma casa de estudios. Contacto: laura.gonzalez@uexternado.edu.co

PALABRAS CLAVE

Acceso universal | Servicio Universal
| Tecnologías de la Información y las
Comunicaciones | Brecha digital |
Colombia | Perú

KEY WORDS

Universal access | Universal service
| Information and Communication
Technologies | Digital divide | Colombia
| Peru

CONTENIDO

1. Introducción; **2.** Definición de acceso y servicio universal; **3.** Cifras de conectividad en Colombia; **4.** Marco legal; **4.1.** Disposiciones proferidas a raíz de la pandemia; **5.** Evolución jurisprudencial; **6.** Caso peruano; **7.** Recomendaciones en materia de acceso y servicio universal; **8.** Conclusiones.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 28 de abril de 2021 y aprobado para su publicación el 29 de junio de 2021.

1. Introducción

Las Tecnologías de la Información y las Comunicaciones (TIC) han cambiado la manera en que las personas viven, trabajan, se relacionan y ejercen sus derechos. Se trata de una herramienta que se encuentra transformando el mundo.

La humanidad se encuentra inmersa en un proceso conocido como la Cuarta Revolución Industrial (4RI), en el cual, a consecuencia del uso de las TIC y las nuevas tecnologías, se están impactando todos los ámbitos de la vida de las personas. Por ejemplo, su implementación en el campo laboral ha llevado a que desaparezcan varios puestos de trabajo y, a su vez, se creen nuevos en los que se demandan habilidades digitales. Asimismo, hoy en día la gente se comunica e informa de una manera diferente. Muchos procesos, cada vez más, están siendo automatizados y los ciudadanos acceden a ellos de una manera diferente, intermediada por las TIC, a la justicia y a la administración pública. La manera de aprender y de acceder al conocimiento se ha modificado por estas tecnologías. Incluso los mecanismos para expresarse y opinar son más democráticos. Esto, si se entiende, por ejemplo, el Internet como un espacio donde todas las personas están en la misma capacidad de dar su punto de vista en igualdad de condiciones.

En general, como se ha podido mencionar, las tecnologías han generado diversos cambios que se han dado en la cotidianidad de las personas. En esa línea, se hace evidente que se está viviendo una revolución tecnológica, cuyos cambios se dan cada vez de manera más rápida y cuyas consecuencias ya se están manifestando.

Dentro de este contexto, se tiene claro que la respuesta a este fenómeno debe ser una en la cual la humanidad prevalezca, donde todas las personas puedan participar y se puedan beneficiar de las ventajas que las TIC puedan traer a sus vidas. Asimismo, donde tanto el sector público como el privado estén involucrados, en aras de lograr un verdadero desarrollo económico y social del que toda la comunidad pueda sacar provecho. Esto es de gran importancia pues la implementación de las TIC, además de beneficiar a todos los individuos que las usan, en un nivel macro, trae consigo ventajas para la economía de los países.

Al respecto, el Banco Mundial (2016) ha señalado que incrementar en 10 puntos porcentuales la penetración de la banda ancha puede aumentar el PIB de la economía

de un país en vías de desarrollo en aproximadamente 1,38%. Adicionalmente, se ha establecido que triplicar la velocidad promedio de conexión a Internet podría aumentar el PIB per cápita hasta un 18.4 y que incrementar el índice de digitalización en 1% puede aumentar la productividad del país en un 0.23% (Departamento Nacional de Planeación de Colombia, 2018).

Debido a esto, resulta importante que todas las personas puedan acceder, utilizar y apropiarse de las TIC pues, de esta forma, es posible impactar positivamente en el desarrollo social y económico de su país y región.

Es en ese contexto en que el acceso y el servicio universal, conceptos que surgieron desde la liberalización de las telecomunicaciones a finales del siglo pasado, se convierten en el núcleo y esencia del servicio público en un mercado cuya gestión se da en competencia. En esa línea, la intervención del Estado es de suma importancia por tratarse de una actividad económica de interés general. En el presente escrito, se analizará la definición de dichos conceptos, su desarrollo legal y jurisprudencial en Colombia y, a partir de un breve análisis del caso peruano, se identificarán los retos y se brindarán las debidas recomendaciones sobre la materia, esperando que sean útiles para ambas naciones.

2. Definición de acceso y servicio universal

Las acepciones de acceso y servicio universal han evolucionado con el tiempo en Colombia. El concepto más reciente lo brindó el Ministerio de las Tecnologías de la Información y las Comunicaciones en 2020. Esta entidad, a través de la Resolución 1272 del 18 de julio, los definió así:

Acceso universal: Disponibilidad de servicios de Tecnologías de la Información y las Comunicaciones, de acceso público o comunitario, para los usuarios ubicados en las zonas del territorio nacional que determine el Ministerio de Tecnologías de la Información y las Comunicaciones.

Servicio universal: Disponibilidad de un conjunto mínimo de servicios de Tecnologías de la Información y las Comunicaciones, económicamente asequible, para todos los usuarios del territorio nacional (Ministerio de las Tecnologías de la Información y las Comunicaciones, 2020.a).

Los anteriores significados están en consonancia con los establecidos por la Unión Internacional de las Telecomunicaciones (UIT, s.f.), que los definió de la siguiente manera:

Acceso universal: Se entiende generalmente por acceso universal la posibilidad de que todos los miembros de una población tengan acceso a las instalaciones y servicios de la red de comunicación a disposición del público. Normalmente, esas prestaciones son proporcionadas en cabinas telefónicas, telecentros comunitarios y terminales comunitarias de acceso a Internet.

Servicio universal: Las políticas en esta esfera se centran generalmente en fomentar o mantener la conectividad universal de todos los hogares a las instalaciones y los servicios de la red pública, a precios razonables.

Además, estas acepciones están en concordancia con la Resolución 70/1 de la Asamblea General de la Organización de Naciones Unidas, que establece como uno de los Objetivos de Desarrollo Sostenible la construcción de infraestructuras resilientes, la promoción de

la industrialización inclusiva y sostenible y el fomento de la innovación y, específicamente, hace referencia a la importancia de “aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a internet en los países menos adelantados” (2015).

Lo anterior es importante porque, como se verá más adelante, las leyes que rigen las TIC en Colombia tienen como uno de sus principios y objetivos lograr el acceso y servicio universal en el territorio nacional, eliminando la brecha digital causada por factores como diferencias en términos socioeconómicos, de género, nivel educativo, etnia, edad y/o ubicación geográfica.

En ese sentido, se concibe el acceso y el servicio universal como un vehículo para lograr el propósito de hacer que toda la población tenga acceso a estas tecnologías y así pueda participar, en condiciones de igualdad, de la 4RI y todos los beneficios que ella conlleva, llegando, de esta manera, a un escenario de mayor desarrollo económico y social. Todo ello se traduce en la generación de un deber para las entidades del orden nacional y territorial de crear políticas públicas encaminadas a la promoción, coordinación y ejecución planes, programas y proyectos tendientes a garantizar que toda la población (incluyendo a las personas, empresas y entidades del sector público) pueda tener acceso, uso y apropiación de las TIC e implementarlas en su quehacer diario.

Es preciso mencionar que el objetivo de la universalidad requiere de recursos, inversión e infraestructura para lograrse. Por ello, resulta importante, por un lado, el esfuerzo estatal de generar una política pública que permita su materialización y, por otro, la participación del sector privado en su financiación y gestión. Sumado a lo anterior, y con el objetivo de lograr que se dé un efectivo aprovechamiento de las TIC, es imprescindible que se trabaje en la generación de las habilidades que estas requieren, para que todas las personas puedan explotar sus cualidades tanto como sea posible. Ello implica que se trabaje por su apropiación, de conformidad con las necesidades, usos y costumbres de la población y siempre de un marco respetuoso de los derechos de los usuarios de estas tecnologías.

Como antecedente, desde hace más de dos décadas, la OMC, en el Cuarto Protocolo anexo al Acuerdo General sobre el Comercio de Servicios, afirmó que los países tienen derecho a definir el tipo de obligación de servicio universal que deseen mantener. Asimismo, resaltó que las obligaciones de esa naturaleza no se consideran anticompetitivas per se, siempre y cuando sean administradas de manera transparente y no discriminatoria y con neutralidad en la competencia y no sean más gravosas de lo necesario para el tipo de servicio universal definido por el miembro (Ley 671, 2001).

Como ejemplo de que estos conceptos son objeto de estudio a nivel de la política pública, legal y regulatorio, se encuentra el Código Europeo de las Comunicaciones Electrónicas de 2018. En este se estableció que el servicio universal constituye una red de seguridad que garantiza que todos los usuarios finales dispongan, al menos, de un conjunto mínimo de servicios a un precio asequible para todos los consumidores, cuando exista riesgo de que la exclusión social provocada por la ausencia de tal acceso impida a los ciudadanos la plena participación social y económica en la sociedad (Directiva 1972 de 2018).

El caso español es referente para Colombia. En particular, las leyes de telecomunicaciones siempre han incluido el concepto de universalidad, por ejemplo, la Ley 9 del 2014 lo consagró como aquellos elementos que se han considerado como núcleo del servicio universal, al asociarlo a un conjunto definido de servicios cuya prestación se garantiza para todos los usuarios finales con independencia de su localización geográfica, con una

calidad determinada y a un precio asequible. No obstante, actualmente se encuentra un proyecto de ley de telecomunicaciones en el cual la universalidad será de nuevo objeto de un cambio legislativo en ese país, donde se hará especial referencia al acceso a los discapacitados y grupos de población con condiciones especiales. De la misma manera, se establecerán obligaciones de servicio público con una mayor exigencia para los operadores frente al sistema de comunicaciones de emergencia y se amplía la regulación para los servicios OTT (Over The Top) que antes estaban por fuera de esta reglamentación y que deberán empezar a contribuir para la financiación del servicio universal.

Esta propuesta de cambio normativo forma parte de España Digital 2025, que corresponde a una estrategia del país que se constituye en el plan hacia la transformación digital. Dicha estrategia tiene como principales objetivos reducir la desigualdad, para lo cual incluye la conectividad digital y el despliegue de las redes de 5G. Además, incluye otros aspectos como la ciberseguridad, que incluirá campañas de concientización y la digitalización de la administración (Ministerio de Asuntos Económicos y Transformación Digital, 2020).

Aunque en Colombia el servicio de telecomunicaciones es un servicio público y en España se cataloga como una actividad económica de interés general, la importancia de la universalidad es la misma, ligada a conceptos fundamentales como la asequibilidad, la calidad del servicio, su continuidad y la disponibilidad para todos.

3. Cifras de conectividad en Colombia

Si bien existen disposiciones normativas y políticas públicas en el país que han permitido que la conectividad y el acceso, uso y apropiación de las TIC haya aumentado en los últimos años, aún existen una serie de retos por superar en ese sentido. Ello se refleja en que, en la actualidad, aún existen cifras preocupantes en la materia, las cuales evidencian la dimensión de la brecha digital en Colombia.

Ejemplo de ello es que, para junio de 2020, solo un 52% de los hogares colombianos tenía acceso a Internet fijo o móvil (herramienta principal de las TIC). Aunque esta cifra se encuentra por encima del promedio de los países andinos, que es de 34%, no deja de ser preocupante que cerca de la mitad de habitantes del país se encuentren desconectados, pues este es un elemento que incide en la ampliación de la desigualdad, ya que se excluye a quienes no tienen acceso a las TIC de la participación, oportunidades económicas, herramientas educativas y demás beneficios que traen estas consigo (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020.b; Banco Interamericano de Desarrollo, 2018). Además, la anterior es una situación que ubica a Colombia en una clara posición de desventaja con el resto de los países de la Organización para la Cooperación y el Desarrollo Económicos (2016), que, en promedio, han logrado un 81% de conectividad. Esto, además de la desigualdad mencionada, dificulta el proceso de desarrollo del país, teniendo en cuenta lo importante que resultan las TIC en ese sentido.

Esta brecha digital se da como consecuencia de la desigualdad ya existente en el país en términos socioeconómicos, de género, educativos, idiomáticos, étnicos, etarios y geográficos. Estos factores condicionan la posibilidad de acceder a las TIC, lo cual hace que el impacto en la generación en esta nueva forma de desigualdad sea mayor.

A manera de ejemplo, las áreas rurales más alejadas del país coinciden con los lugares donde se encuentran los niveles más altos de pobreza multidimensional, los menores índices de calidad en la educación y con las zonas donde existen las tasas más bajas de penetración de Internet fijo. Asimismo, los departamentos más pobres y rurales

son aquellos que cuentan con menor cantidad de accesos fijos a Internet y velocidad de descarga promedio. (Instituto Geográfico Agustín Codazzi, 2015; Departamento Administrativo Nacional de Estadística, 2018; Portafolio, 2019; Semana, 2019; Comisión de Regulación de Comunicaciones, 2019; Ministerio de Tecnologías de la Información y las Comunicaciones, 2020).

Estas cifras evidencian la necesidad de generar políticas, que involucren al sector público y privado, las cuales deben estar encaminadas a lograr la inclusión de la población en el mundo de las TIC, a través del acceso y servicio universal. Estas políticas deben tener en cuenta los factores mencionados y un enfoque territorial y diferencial, valorando las particularidades y necesidades de las zonas y poblaciones relegadas del acceso y uso de las TIC. De esa manera, se logrará la mayor eficiencia posible de las mismas.

4. Marco legal

- Constitución Política de Colombia**

De conformidad con la legislación colombiana (Ley 1341, 2009, art. 10; Ley 1978, 2019, art. 7), las telecomunicaciones son un servicio público en el país. Esto debe leerse conforme a la Constitución Política de 1991 que, en su artículo 365, dispone que “los servicios públicos son inherentes a la finalidad social del Estado. Es deber del Estado asegurar su prestación eficiente a todos los habitantes del territorio nacional”.

Es preciso mencionar que, por disposición constitucional, si bien las telecomunicaciones son un servicio público en cabeza del Estado, este puede realizar su prestación de manera directa o indirecta, es decir, a través de particulares. En todo caso, el Estado mantiene la regulación, el control y la vigilancia de dichos servicios. De esta forma, en Colombia, los particulares están habilitados legalmente para prestar estos servicios y es deber del Estado propiciar escenarios de libre y leal competencia que incentiven la inversión actual y futura en el sector de las TIC, promoviendo la concurrencia de agentes al mercado en condiciones de igualdad (artículo 2 de la Ley 1341, 2009). En aquellos lugares donde no se logre la cobertura a través de estos mecanismos, será deber del Estado prestar los servicios correspondientes.

En ese sentido, en Colombia se mantiene el concepto de servicio público para actividades que se prestan en competencia y que pueden ser ejercido por todos (según el régimen de habilitación), pero las condiciones para ello están sujetas a fuertes intervenciones, en garantía del interés general. De esta manera, en un contexto liberalizado, se busca la igualdad social e interterritorial mediante la imposición de obligaciones de servicio público que, sin distorsionar la competencia, permitan asegurar la prestación de estos servicios en los casos que se consideren no rentables por los prestadores particulares (De la Quadra, 2010, p. 38 y 56).

Así, se deduce que existe una obligación a cargo del estado colombiano de garantizar la universalidad de la prestación del servicio de las telecomunicaciones a todos los ciudadanos. Para que este deber –que es derecho de las personas– se concrete, es necesario que exista acceso y servicio universal en los términos mencionados. Este deber concuerda con las obligaciones internacionales de Colombia en la materia, particularmente con las adquiridas por el país cuando ratificó, a través de la Ley 46 de 1985, el Convenio de la Unión Internacional de Telecomunicaciones –UIT–, organismo que tiene como uno de sus principales objetivos lograr la universalidad de las telecomunicaciones.

En Colombia, en materia de TIC hay dos leyes que establecen los lineamientos principales

del sector: la Ley 1341 de 2009 y la Ley 1978 de 2019. Estas normas serán expuestas a continuación, previa mención de sus antecedentes normativos.

Antecedentes normativos

Con la Ley 72 de 1989 y el Decreto Ley 1900 de 1990 se constituyó un hito en el sector de las telecomunicaciones en Colombia. Esto se debió a que, por primera vez, se definió una política integral para el mismo, que introdujo aspectos como el régimen de competencia, la participación privada para la prestación de estos servicios y la importancia de la interconexión (Guerra, 2010, p. 69). No obstante, en ese marco legal, existía un monopolio estatal en el cual, para que un particular pudiera prestar estos servicios, debía haber una concesión. En ese sentido, el Estado mantuvo la potestad de ejercer un control estricto en materia de redes y servicios para acceder al mercado.

Los cambios introducidos por la Ley 1341 de 2009, que será analizada a continuación, incluyó aspectos que destacan dentro de la normativa comunitaria europea del año 2002, en este caso, de la Directiva 2002/20/CE de servicio universal. Esta Directiva de la Unión Europea estableció que la actividad del sector de las comunicaciones debe tener la menor cantidad de restricciones posibles. Por ello, al estar liberalizada, puede ser desarrollada por quien se sujete a las condiciones establecidas con carácter general por los Estados, lo cual supone que quien las cumpla está habilitado para comenzar a ejercer la actividad, sin necesidad de obtener un documento previo que comunique su intención de hacerlo. En ese sentido, ningún Estado miembro puede impedir que un operador que cumpla las condiciones generales suministre el servicio (De la Quadra, 2010, p. 42). En esa línea, se procura garantizar la existencia de los servicios de comunicaciones electrónicas disponibles al público, de buena calidad y en toda la comunidad a través de una competencia y una libertad de elección reales.

Régimen legal actual

• Ley 1341 de 2009

En cuanto a la universalidad, la Ley 1341 de 2009, que tiene como fin principal crear un marco jurídico para la construcción de la política pública de acceso a las TIC, dispuso como objetivo de esta norma lograr el acceso y servicio universal a las TIC y definió varios instrumentos para lograrlo.

Esta norma estipuló que el Estado debe garantizar a todos los colombianos³ el derecho al acceso de las Tecnologías de la Información y las Comunicaciones básicas, pues estas últimas permiten ejercicio de derechos como la libre expresión, la información y la educación.

Además, señaló que el Estado y todos los agentes del sector TIC deberán priorizar el acceso y uso a estas tecnologías en condiciones no discriminatorias e indicó que el Estado debe generar programas para que los estratos menos favorecidos y la población rural tengan acceso y hagan uso de las plataformas de comunicación, en especial de Internet, de contenidos informáticos y de educación integral. En este punto, el MinTIC, como ente rector que define y adopta políticas en relación con el acceso a las TIC, deberá examinarlas periódicamente para verificar que estas reflejen realmente las necesidades de la población, fruto de un dialogo positivo en especial con las comunidades de las

³ Es preciso evaluar la exequibilidad de la diferenciación que hace esta norma por motivos de nacionalidad, en su artículo 2, modificado por el artículo 2 de la Ley 1978 de 2019.

zonas rurales, apartadas y de bajos ingresos para fijar los objetivos de forma concertada (Herrera, 2010, p. 821).

Adicionalmente, esta ley creó el Fondo de Tecnologías de la Información y las Comunicaciones (antes FONTIC, actualmente FUTIC). Los recursos de este fondo están directamente destinados a la reducción de la brecha digital, a través de la financiación de planes, programas y proyectos encaminados a lograr el acceso universal prioritariamente y el servicio universal cuando haya lugar a ello, y a masificar el uso y apropiación de las TIC.

Asimismo, esta norma facultó al Estado para intervenir en el sector TIC, cuando tenga el objetivo de promover el acceso a estas tecnologías, teniendo como fin último el servicio universal.

Finalmente, esta ley definió un principio según el cual el Estado debe propiciar escenarios de libre competencia y concurrencia al mercado de todos los agentes en condiciones de igualdad. Esto es de gran importancia, pues significa la generación de escenarios favorables para la inversión y la participación de más proveedores de redes y servicios de telecomunicaciones (PRST). Lo último implica una participación de más agentes en el mercado a través de la habilitación general, la cual conlleva la mejora en la calidad del servicio y la reducción de precios al consumidor, haciendo estos servicios más asequibles.

- **Ley 1978 de 2019**

Por su parte, la Ley 1978 de 2019, que tuvo como finalidad modernizar el sector TIC, trajo modificaciones a la Ley 1341 de 2009. Así, estableció como principios el despliegue de infraestructuras y la promoción de las inversiones, a través de la generación de condiciones de certidumbre en las mismas.

Por un lado, en cuanto al despliegue de infraestructuras, esta norma definió que uno de los mecanismos para lograrlo son las obligaciones de hacer. Así, creó la posibilidad para los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) de cancelar máximo el 60% del valor correspondiente a la contraprestación por el uso del espectro a través de este tipo de obligaciones, siempre y cuando, como consecuencia de ello, se beneficie la población pobre y vulnerable o aquella que esté ubicada en zonas apartadas, rurales o instituciones como escuelas públicas o centros de salud. El resto del valor de la contraprestación está destinado al FUTIC que, como se mencionó, está enfocado prioritariamente a lograr el acceso y servicio universal.

Por otro lado, en cuanto a la promoción y certidumbre en la inversión, esta norma estableció, entre otras medidas, que el permiso para el uso del espectro radioeléctrico se otorgará hasta por 20 años prorrogables por la misma cantidad de tiempo, en contraste con el término de 10 años que establecía la norma de 2009.

Además, esta ley estipuló que la asignación del espectro radioeléctrico que determine el Estado debe buscar siempre la maximización del bienestar social, definida por la misma norma como "la reducción de la brecha digital, el acceso universal, la ampliación de la cobertura, el despliegue y uso de redes e infraestructuras y la mejora en la calidad de la prestación de los servicios a los usuarios" (Ley 1978, 2019, art. 8, par. 3). Por ello, en virtud de esta disposición, los recursos que se recauden por este concepto se destinan al FUTIC.

Adicionalmente, la norma estableció que se deben crear programas para que la población pobre y vulnerable, la mayor de 45 años sin ingresos fijos y la rural puedan tener acceso

y hacer uso de estas tecnologías, siempre respetando el principio de autodeterminación de las comunidades étnicas y minoritarias (indígenas, afrocolombianas, palenqueras, raizales y Rrom).

Esta disposición también hizo énfasis en la necesidad de la apropiación de estas tecnologías por parte de los habitantes del territorio colombiano. Específicamente, menciona el aprovechamiento por parte de estas con enfoque productivo para el sector rural y de la apropiación tecnológica por medio del desarrollo de contenidos y aplicaciones con enfoque social.

- **Ley 1955 de 2019**

La Ley 1341 de 2009 y la Ley 1978 de 2019 deben leerse en conjunto con el Plan Nacional de Desarrollo⁴ actual, establecido en la Ley 1955 de 2019. Esta norma dispuso, respecto del acceso a las TIC y el despliegue de infraestructura, que los alcaldes de cada municipio del país pueden buscar la modificación de los Planes de Ordenamiento Territorial que tengan barreras que impidan el desarrollo de esos dos asuntos (acceso y despliegue).

Además, determinó que el gobierno debe diseñar e implementar planes, programas y proyectos que promuevan de forma prioritaria el acceso y el servicio universal a las TIC y que busquen aumentar y masificar el acceso a Internet. Para ello, según esta norma, el gobierno podrá impulsar estrategias que fomenten el uso de tecnologías costo-eficientes y que optimicen la inversión; podrá implementar iniciativas de estímulo a la oferta y la demanda, en beneficio de la población pobre y vulnerable; y podrá establecer obligaciones de hacer.

- **Plan TIC 2018–2022**

El gobierno actual expidió, a través del MinTIC, el Plan TIC 2018-2022. Esta política tiene como uno de sus objetivos principales lograr el cierre acelerado de la brecha digital. Para lograrlo, establece algunas herramientas como el Programa para Masificar la Última Milla, que tiene como meta reducir el déficit de redes de última milla en todo el país y aumentar la penetración al servicio de Internet, principalmente en los estratos 1 y 2. También contiene proyectos dirigidos especialmente a la inclusión digital de mujeres, minorías étnicas, comunidades rurales, entre otros; asimismo, incluye programas encaminados a la formación en habilidades para las TIC y propone soluciones de conectividad comunitarias para garantizar el acceso universal a Internet.

En particular, el Plan TIC “El Futuro Digital es de Todos” estableció sus bases bajo cuatro pilares o ejes que se pueden resumir de la siguiente manera:

- Primer eje - Entorno TIC para el desarrollo digital: su objetivo principal es construir un entorno favorable para masificar las TIC al 100%. Apunta hacia una institucionalidad sectorial eficiente, para focalizar recursos a fin de cerrar la brecha de acceso a las TIC.
- Segundo eje - Inclusión social digital: busca crear programas para llevar conectividad a todos aquellos que el mercado no atiende, a través de iniciativas

4 El Plan Nacional de Desarrollo es la hoja de ruta que cada cuatro años establece el gobierno que llega al poder. En ella se fijan los objetivos, programas, inversiones y metas para el cuatrienio. Esto permite evaluar sus resultados y garantiza la transparencia en el manejo del presupuesto (Departamento Nacional de Planeación, s.f.).

basadas en la asequibilidad y la apropiación. Pretende lograr el acceso universal por medio de soluciones de conectividad comunitaria.

- Tercer eje - Ciudadanos y hogares empoderados del entorno digital: su finalidad es lograr el uso y apropiación de las TIC y brindar incentivos para el desarrollo. Para ello, dispone de mecanismos como la creación de contenidos multiplataforma, la promoción de RTVC play⁵, la digitalización del archivo de televisión y la construcción de una política integral de tecnologías para aprender.
- Cuarto eje - Transformación digital sectorial y territorial: su objetivo es crear las condiciones para que el sector privado y público en el orden nacional y territorial puedan avanzar hacia la Cuarta Revolución Industrial. Pretende lograrlo a través de acciones dirigidas a digitalizar los trámites, del uso de la información para la toma de decisiones de política, de la creación de protocolos para facilitar el intercambio de información hacia un portal único del Estado, entre otras medidas.

- **Proyectos de ley**

Es oportuno mencionar que, en aras de reducir la brecha digital y lograr el acceso y servicio universal, actualmente existen varios proyectos de ley relacionados a esta materia y, particularmente, con la garantía de acceso a Internet. Entre ellos, destacan los siguientes: el Proyecto de Ley No. 030 de 2020 de la Cámara de Representantes⁶, por medio del cual se crea el mínimo vital de Internet y se dictan otras disposiciones”; el Proyecto de Ley No. 109 de 2020 de la Cámara de Representantes⁷, por el cual se busca declarar el Internet como un Servicio Público esencial y universal”; el Proyecto de Ley 321 de 2020 del Senado, “por medio del cual se implementa el mínimo vital en los servicios públicos domiciliarios de Energía, Agua, Alcantarillado y Gas domiciliario” y, finalmente, el Proyecto de Ley 285 de 2020 del Senado, “por medio de la cual se dictan medidas para disminuir las brechas de acceso universal a Internet”.

De ellos, es preciso resaltar el Proyecto de Ley No 109 de 2020, Cámara y No 324 de 2020 Senado, que, dentro del trámite legislativo, tiene un gran avance. Se compone de 12 artículos cuyas temáticas se centran en consagrar el acceso a Internet como un servicio de carácter esencial. Asimismo, adiciona a los principios orientadores de la Ley 1341 un párrafo que contempla que los proveedores de redes y servicios de telecomunicaciones no podrán suspender las labores de instalación, mantenimiento y adecuación de las redes requeridas para la operación de este servicio público esencial. En esa línea, garantizarán la continua provisión del servicio, sin perjuicio de los deberes de los usuarios.

También se incluyeron medidas a favor de los usuarios de telefonía móvil en la modalidad pospago y prepago para mantener la posibilidad de comunicarse en estados de excepción y emergencias sanitarias como la ocasionada por pandemia por COVID-19. Por otra parte, en cuanto al despliegue de infraestructura, define un plazo de 30 días para resolver solicitudes de licencia para la construcción, conexión, instalación, modificación u operación de cualquier equipamiento para la prestación de servicios de telecomunicaciones fijas y móviles, que incluye silencio administrativo positivo.

Por último, adiciona una función al FUTIC para que apoye a los pequeños PRST (aquellos con menos de treinta mil usuarios) mediante su fomento, a través de la financiación

5 RTVC Play: Plataforma de entretenimiento gratuito, que pertenece al sistema de medios públicos. Fuente: <https://www.rtvcplay.co>

de líneas de crédito y exceptuándolos del pago de contraprestación a favor del FUTIC por cinco años. Ahora bien, el texto incluyó una condición especial para mantener la excepción. Esta dejará de ser aplicable si, posterior al 31 de diciembre de 2020, los proveedores beneficiarios llegan a ser controlantes de manera directa o indirecta de otra sociedad o controlados de manera directa o indirecta por parte de otra sociedad a través de cualquier operación o figura jurídica, sin limitarse a adquisiciones, fusiones, escisiones o cualquier forma de transformación societaria. Este beneficio debe reglamentarse por el MinTIC, que, dentro de los cuatro meses siguientes a la promulgación de la presente ley, deberá definir las inversiones que deberán realizar estos proveedores durante el tiempo de la exención, las condiciones para mantener el beneficio, así como los mecanismos de verificación de su cumplimiento.

4.1 Disposiciones proferidas a raíz de la pandemia

El COVID-19 develó la magnitud de la brecha digital en Colombia y la desigualdad que esta genera. Durante la pandemia, se evidenció con mayor fuerza este asunto, pues fue un momento en el que la mayoría de los derechos (trabajo, educación, información, libre expresión, salud, entre otros) tuvieron como único mecanismo para ser ejercidos las TIC, especialmente la conectividad a Internet. En consecuencia, todas las personas relegadas del acceso, uso y apropiación de estas tecnologías vieron vulnerados sus derechos.

Al respecto, la Comisión Interamericana de Derechos Humanos (CIDH) señaló lo siguiente:

Ante las medidas de aislamiento y/o distanciamiento físico aplicadas en la mayoría de Estados, se hace más evidente la necesidad de acelerar las políticas de acceso universal a internet, ampliando la infraestructura que lo sostiene, facilitando el acceso a dispositivos idóneos y promoviendo la alfabetización digital. El déficit de acceso a internet en el contexto de la pandemia afecta, deteriora o dilata la garantía de todos los derechos humanos que hoy se ejercen total o parcialmente por esta vía (...). El acceso universal a una internet libre, abierta e incluyente depende fundamentalmente de las medidas positivas que los Estados están obligados a adoptar para alcanzar a las personas y grupos que por diversos factores (socioeconómicos, la ubicación geográfica, la edad, entre otros) no han podido acceder aún a la red global. Así también son cruciales las acciones y las medidas que adopten otros actores del ecosistema digital. Las empresas privadas, de telecomunicaciones y prestadoras de servicio en internet son cada vez más relevantes en el desafío de reducir la brecha digital (2021).

De lo anterior se desprende que el contexto de pandemia hizo más necesario que nunca trabajar de forma rápida y eficiente en la reducción de la brecha digital. En el caso colombiano, por ejemplo, a raíz de la declaratoria del estado de emergencia sanitario, se profirieron medidas que buscaron que no se interrumpiera y que se ampliara la prestación de estos servicios de telecomunicaciones, en aras de garantizar los derechos ejercidos por su conducto.

Así, se tomaron medidas como: la declaratoria de los servicios de telecomunicaciones como esenciales, que implica que no se pueda suspender su operación y que los usuarios más vulnerables no pueden dejar de acceder al servicio en caso de dificultad del pago; la ampliación de plazos para que quienes se encontraban en mora de pago de estos servicios pudiesen ponerse al día; la provisión de mensajería de texto gratuita; la reducción de tiempos de los trámites asociados a solicitudes de licencia de infraestructura de telecomunicaciones; la exención de impuesto de valor agregado (IVA) a algunos servicios

de voz e Internet; la navegación sin costo en el dominio, subdominio y páginas adyacentes del portal de educación dispuesto por el Ministerio de Educación Nacional y el Ministerio de Tecnologías de la Información y las Comunicaciones; la obligación para los canales de televisión abierta a incluir, al menos una emisión noticiosa al día; la interpretación de lengua de señas para aquellas notas relacionadas con la pandemia; el establecimiento de un auxilio de conectividad⁶, en vez de un auxilio de transporte, para los trabajadores que desarrollaren sus labores desde su domicilio y no devengasen más de dos salarios mínimos, entre otras (Decreto Ley 464, 2020; Decreto Ley 540, 2020; Decreto Ley 555, 2020; Decreto Ley 771, 2020; Resolución CRC 5960 de 2020).

Adicionalmente, con ocasión de la pandemia, se emitió un documento del Consejo Nacional de Política Económica y Social (CONPES), cuyo objetivo se centró en declarar de importancia estratégica el Proyecto Nacional de Acceso Universal a las Tecnologías de la Información y las Comunicaciones en Zonas Rurales o Apartadas. Dicho proyecto tiene como propósito promover la inclusión digital en zonas rurales mediante la oferta de acceso público a Internet en los 32 departamentos del país, para garantizar el acceso a la conectividad en un horizonte de largo plazo (CONPES 4001, 2020). Así, este proyecto, que fue dividido en dos zonas, dará conectividad hasta el año 2031 y proporcionará Internet a Centros Digitales y a 13.708 sedes educativas oficiales. Esta política pública debe armonizarse entre el MinTIC y el Ministerio de Educación Nacional y Computadores para Educar⁷, para concatenar acciones y lograr mayor eficiencia en el uso de los recursos.

5. Evolución jurisprudencial

Pese a que no existe un diverso desarrollo jurisprudencial en materia de acceso y servicio universales, en este acápite se traerán a colación dos sentencias recientes (de 2019 y 2020) de las Altas Cortes colombianas, que dan cuenta de la importancia que está tomando este asunto y del reconocimiento jurisprudencial que están realizando los jueces del país en ese sentido, particularmente en lo relacionado con la conectividad a Internet.

La primera de las providencias es de la Sala de Casación Civil de la Corte Suprema de Justicia, que, en Sentencia del 4 de junio de 2020, indicó lo siguiente:

De tal modo, que hoy el acceso a internet es un derecho humano y, por lo tanto, es fundamental, digno de protección para el acceso masivo; también, como herramienta esencial es un servicio público, que debe servir para cerrar brechas, para avanzar en todo el desarrollo humano, especialmente en educación, en acceso a la justicia y en progreso tecnológico. Nuestra Constitución de 1991, el bloque de constitucionalidad, decisiones emanadas del Consejo de Derechos Humanos de las Naciones Unidas, como la - "promotion, protection, and enjoyment of human rights on the internet" constituyen premisas básicas para el acceso de las personas al internet, en concordancia con el art. 19 de la Declaración Universal de los Derechos Humanos y el Pacto Internacional de

6 El auxilio de transporte como auxilio de conectividad: Aspecto que quedó incluido en la Ley 2088 de 2021 recientemente expedida, que habilitó el trabajo en casa como una forma de prestación del servicio en situaciones ocasionales, excepcionales o especiales, que se presenten en el marco de una relación laboral, legal y reglamentaria con el Estado o con el sector privado.

7 Computadores para Educar es un programa del gobierno nacional que impulsa la innovación educativa mediante el acceso, uso y apropiación de la tecnología en las sedes educativas del país (CPE, s.f.).

Derechos Civiles y Políticos (Corte Suprema de Justicia, Sala de Casación Civil, STC 3610, 2020).

La segunda de ellas es la sentencia T-030 de 2020 de la Corte Constitucional. En esta providencia, el Tribunal discutió el caso de una escuela rural donde se suspendió el servicio de Internet por recortes de presupuesto, impidiendo el acceso a la red a sus estudiantes y docentes. La Corporación determinó que debía continuarse prestando el servicio, por su relación directa con el derecho a la educación. Puntualmente, dispuso que:

El internet es una herramienta que, empleada de forma adecuada, puede ayudar a asegurar el goce efectivo del derecho fundamental a la educación, en especial de personas que se encuentran en zonas apartadas, lejos de las ciudades capitales y de cabeceras municipales (...). Las instituciones educativas no pueden dejar de preparar a los niños y a las niñas a ser parte de una sociedad estructurada en tecnologías de la información, hace parte de su desarrollo armónico e integral

No obstante, la Corte Constitucional colombiana indicó lo siguiente sobre la red:

Se encuentra dentro de la faceta prestacional del derecho a la educación y, por tanto, su garantía es progresiva. Ello quiere decir que está supeditada a la existencia de una política pública mediante la cual gradualmente se haga extensiva a la totalidad de la población, atendiendo a las condiciones propias de cada ente regional. Por ende, no se trata de una exigencia inmediata al Estado colombiano.

Así, si bien esta última sentencia no clasificó el acceso a Internet como un derecho fundamental, expuso una serie de argumentos que, según lo dicho, permiten colegirlo como tal por su intrínseca conexión con el derecho a la educación. Por ello, en el caso concreto, la Corte decidió que debía continuar prestándose tal servicio.

6. Caso peruano

Es posible afirmar que, al igual que ocurre en el caso colombiano, en el Perú también existe una marcada brecha digital. Tan solo el 40.1% de los hogares peruanos tiene acceso a Internet. Esto es causado por motivos socioeconómicos, de género, educativos, de infraestructura, etarios y geográficos. En este país, además de la cobertura, preocupa la calidad en las telecomunicaciones, especialmente en áreas rurales (Instituto Nacional de Estadística e Informática, 2020; ESAN Graduate School of Business, 2019; Tello, 2019).

En el Perú, el Estado es el titular de la prestación del servicio de las telecomunicaciones, actividad que desarrolla a través de operadores y concesionarios. En este país también existe un marco normativo que busca el acceso y servicio universal a las TIC; no obstante, se da prevalencia al primero de estos conceptos. Entre las medidas tomadas, resalta la creación del Fondo de Inversión en Telecomunicaciones (FITEL), cuyos fondos provienen de los PRST y cuya gestión está a cargo del Ministerio de Transportes y Comunicaciones (MTC). El FITEL, según el Decreto Supremo No. 010-2020, está destinado a la provisión del acceso universal a los servicios de telecomunicaciones. En líneas generales, se busca lograr el acceso en el territorio nacional a un conjunto de servicios de telecomunicaciones esenciales, capaces de transmitir voz y datos (Ley 28900; Decreto Supremo No. 010, 2020).

El FITEL financia únicamente los "servicios de telecomunicaciones en áreas rurales

o lugares preferentes de interés social, así como la infraestructura necesaria para garantizar el acceso a tales servicios" (Zegarra, 2018). Se considera oportuno analizar la posibilidad de tener en cuenta, además de criterios geográficos, los demás mencionados como causantes de la brecha digital en el Perú, para lograr que más personas puedan acceder y apropiarse de las TIC.

A su vez, el servicio universal se ha definido como "un conjunto mínimo de servicios de buena calidad que deben ser prestados a un precio asequible a todos los usuarios finales, independientemente de la localización geográfica" (Zegarra, 2018).

También cabe destacar la Ley de promoción de la banda ancha y construcción de la red dorsal nacional de fibra óptica (Ley 29904) del año 2012, que le da facultad al Fitel para financiar las redes de transporte y el despliegue de redes de alta capacidad, para brindar conectividad a nivel distrital. Esta normativa declaró como de "necesidad pública e interés nacional" la construcción de la red dorsal y el acceso y uso de la infraestructura asociada a la prestación de servicios públicos de energía eléctrica –incluida la coubicación⁸ y el derecho de vía de la red vial nacional–, aspectos de suma importancia para facilitar la provisión de banda ancha fija o móvil, que se constituyen en un medio para el ejercicio de los derechos fundamentales.

En este punto, se resalta que el derecho de vía requiere un único título habilitante para su uso (que es otorgado por el Ministerio) y que supera las jurisdicciones de los gobiernos regionales y gobiernos locales, superando las barreras existentes a nivel territorial.

Por otra parte, la función del Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL)⁹ es actualizar periódicamente las características técnicas de las conexiones a Internet de banda ancha, salvo la velocidad mínima, que es determinada por el Ministerio de Transportes y Comunicaciones (s/f).

Ahora bien, en este punto es importante señalar la creación del Programa Nacional de Telecomunicaciones (PRONATEL, s.f.), realizada por el Decreto Supremo 018-2018 del MTC, que también dispuso la fusión del Fitel en el Ministerio de Transportes y Comunicaciones. El Ministerio fue la entidad absorbente y le correspondió la administración del Fondo. La provisión del acceso universal a nivel nacional es el principal objetivo del PRONATEL, así como el desarrollo de la banda ancha, la reducción de la brecha en la infraestructura, la promoción de habilidades digitales, servicios, contenidos y aplicaciones.

La conectividad en las regiones es un aspecto de la mayor importancia, como ya se ha mencionado, y al cual se siguen destinando recursos por los fondos de universalidad, y promoviendo inversión por parte de los operadores, aspecto que en Colombia es objeto

-
- 8 Coubicación: "Es el uso de espacio físico, energía, infraestructura de soporte de redes y otras facilidades de la infraestructura de telecomunicaciones, requeridas por un concesionario de servicios públicos de telecomunicaciones para la ubicación y operación de sus equipos y/o elementos de telecomunicaciones, así como para la interconexión. La Coubicación puede ser física o virtual. Decreto Legislativo 1019 del 9 de junio de 2008, artículo 5 numeral 3.
 - 9 El OSIPTEL –Organismo Supervisor de Inversión Privada en Telecomunicaciones– es un organismo público especializado, regulador y descentralizado adscrito a la Presidencia del Consejo de Ministros, que cuenta con autonomía técnica, administrativa, económica y financiera. Este organismo tiene competencia para evitar conductas anticompetitivas y acuerdos de restricción vertical, para lo cual puede implementar mecanismos de control como obligaciones de información, calidad del servicio, contabilidad separada, separación estructural, entre otras.

de la política pública, y que se encuentra plasmado, en particular, en las leyes mencionadas de 2009 y de 2019, y en las leyes del Plan Nacional de Desarrollo desde hace más de una década. En el Perú, el MTC –a través del PRONATEL– dentro de los grandes proyectos para el mejoramiento de la conectividad próximamente desarrollará proyectos regionales para beneficiar comunidades rurales de un gran número localidades, que esperan impactar generando plataformas para desarrollar habilidades digitales en los pobladores, donde se beneficiaran también instituciones educativas y hospitales.

Por último, es preciso mencionar que en este país también hay varios proyectos legislativos relacionados con la materia y, especialmente, con el acceso a Internet y su declaratoria como derecho fundamental o humano (PL 2780-2017; PL 3156-2018-CR; PL 3607-2018-CR; PL 5600/2020-CR; y PL 5843/2020-CR)¹⁰. La modificación que incorporará el derecho de acceso a Internet en la Constitución política se encuentra pendiente para ser aprobada en la siguiente legislatura. Este cambio normativo traerá cambios en el pensum de las instituciones educativas incluyendo asignaturas relativas a brindar competencias y resultados de aprendizaje en el uso del internet y general de las tecnologías de la información y las comunicaciones, con especial atención a las zonas rurales¹¹.

Así, se ve que la situación actual del Perú es, en cierta forma, similar a la de Colombia, en términos de la dimensión de la brecha digital, las iniciativas que hay al respecto y, de cierta manera, la existencia de los fondos de recursos destinados a la universalidad

10 Como ejemplo se encuentra el caso de México, que es uno de los pocos países que han reconocido el derecho de acceso a Internet en la Constitución Política. El acceso a las TIC en México es un derecho constitucional e incluye el acceso a banda ancha e internet. Álvarez (2018), afirma que es un derecho instrumental, pues las TIC son un medio sin el cual no será posible tener en el mundo contemporáneo el pleno goce de diversos derechos humanos. Resalta, además, que el Estado mexicano está obligado a establecer un entorno habilitador y las condiciones para que el sector privado, en un ambiente de competencias y libre concurrencia, pueda hacer disponible el acceso a las TIC y prestar servicios de radiodifusión y telecomunicaciones, incluyendo servicios de banda ancha y de acceso a Internet. También les da gran valor a las asociaciones público privadas como una solución para aquellos lugares donde el sector privado no participa.

En Colombia, la Ley 1978 de 2019 consagró que el Fondo de servicio universal (FUTIC) podrá participar y aportar recursos para el desarrollo de proyectos bajo esquemas de participación público privada, según lo previsto, entre otras, en la Ley 1819 de 2016 y Ley 1508 de 2012. El Gobierno nacional reglamentó lo relacionado con las asociaciones público privadas en Tecnologías de la Información y las Comunicaciones. Para mayor ilustración ver el Decreto 1974 de 2019 expedido por el Departamento Nacional de Planeación, en el cual se consagró que recaerán sobre proyectos en los que se encargue a un inversionista privado el diseño y construcción de una infraestructura y sus servicios asociados, o su construcción, reparación, mejoramiento o equipamiento, todas estas actividades deberán involucrar la operación y mantenimiento de dicha infraestructura. En particular, la Ley 1508 consagró que en los contratos de asociaciones público-privadas se indicarán los bienes afectos a la prestación del servicio que se revertirán al Estado.

11 Para mayor ilustración se transcribe el artículo que sería modificado en la Constitución Política, el cual quedaría así: "Artículo 2.- Toda persona tiene derecho: 4. 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 alguno, bajo las responsabilidades de ley. El Estado garantiza el acceso al internet y las tecnologías de la información y comunicación, priorizando su cobertura en el sector rural. (...)" Y el artículo 14 sobre Educación: (...) El Estado reconoce el derecho al acceso al internet, las tecnologías de la información y comunicación. En especial para el sector educativo y las zonas rurales del país, sobre la base de la protección y la defensa de los intereses sociales y ambientales. (...)" (PL 5843/2020 CR)

en cada país. En ese sentido, existen algunos retos y sugerencias para lograr el acceso y servicio universal, que se expondrán en el siguiente acápite.

7. Recomendaciones en materia de acceso y servicio universal

Como se ha podido apreciar, si bien existen varias normas y decisiones judiciales encaminadas a lograr el acceso y servicio universal, aún se tienen presente diversos retos y desafíos para que aquello se materialice en la realidad.

En primer lugar, es imprescindible que el Estado continúe tomando medidas afirmativas y generando programas y proyectos para la inclusión de la población tradicionalmente relegada del acceso y uso de las TIC. En este punto, es especialmente importante que estas políticas se desarrolle con un enfoque territorial, atendiendo a las necesidades y cultura de las comunidades. Por ello, es importante que se generen datos sobre el uso de las TIC en las comunidades, con el mayor detalle posible en términos de género, edad, nivel socioeconómico, lugar geográfico. De tal manera, se podrán generar mejores políticas públicas que respondan a las necesidades de la población y que permitan acelerar soluciones que el mercado no atendería o que puede resolver en forma tardía.

Adicionalmente, debe continuar promoviéndose la inversión en el país y el pago mediante obligaciones de hacer para los PRST. Así, por medio del despliegue de infraestructura, se llegará a las poblaciones más remotas. Para ello, deben crearse escenarios de seguridad jurídica, de libre competencia y de eliminación de trámites largos y regulaciones restrictivas e innecesarias que no responden a la agilidad que requiere el sector TIC. También se debe apoyar la generación y funcionamiento de redes comunitarias. Será tarea del Estado procurar la cobertura de aquellos lugares donde no se logre hacerlo mediante iniciativas privadas.

Resulta importante enfatizar en la noción del ámbito digital como un ecosistema, pues de esa manera se entiende que debe existir una conexión entre los múltiples agentes que intervienen en él. Estos, al unir sus esfuerzos y cooperar, acelerarán el proceso de universalización de las TIC. En otras palabras, la financiación de la universalidad de las TIC no sólo debe provenir de los operadores de telecomunicaciones, sino de múltiples sectores que cada día aprovechan el acceso y uso de una conectividad segura, más rápida y de calidad. Para ello, es importante que se analicen, en términos de costo-eficiencia, las tecnologías que responden mejor a las necesidades específicas de la población para así optimizar las inversiones. Esto implicaría estudiar alternativas como el aumento de la capacidad satelital. En esos análisis es necesaria una visión prospectiva, es decir, que se anticepe a los posibles cambios tecnológicos, como el ingreso del 5G y se planee conforme a ello, de tal manera que el país logre estar actualizado en materia TIC.

Lo anterior es un reto para la CRC y el OSIPTEL, organismos que deben procurar la flexibilización de las normas de compartición y trabajar con herramientas como los *sandbox* regulatorios, para generar un marco normativo que facilite el tránsito hacia la transformación digital. La red troncal de fibra óptica en Colombia, como uno de los principales proyectos del Plan Vive Digital 2010-2014 y del Plan TIC 2018-2022, y la Red dorsal de fibra óptica en el Perú¹², son desafíos para los dos países, pues su principal

12 Recientemente, el Ministerio de Transportes y Comunicaciones (MTC) inició, en marzo de 2021, el proceso para poner fin al contrato de concesión de la red con su actual operador, Azteca Comunicaciones, de manera unilateral. Para ello, argumenta la causal de interés público, ya que se trata de una iniciativa planteada con el objetivo de universalizar el acceso a la banda ancha. Se prevé llevar a cabo una audiencia en los próximos meses para decidir este asunto. Existe el riesgo de que Azteca acuda a los tribunales si los términos no le favorecen, por lo

objetivo es atender la necesidad de banda ancha de la comunidad. Para esto, se requiere mayor dinamismo, promover la seguridad jurídica y la inversión privada.

En cuanto a la habilitación para prestar los servicios y en aras de fomentar un mercado y el cierre de la brecha digital, se debe reflexionar si un sistema concesional es el mejor camino en el Perú, pues se puede estar sacrificando un mayor dinamismo del mercado y generando sobrecostos (Zegarra 2018, p. 89). Esta situación puede traer retrasos en los proyectos de universalidad. La habilitación general como se estructuró en Colombia comprende todas las actividades relacionadas con la prestación del servicio, salvo el uso del espectro radioeléctrico, que en la mayoría de los casos requiere un proceso de selección objetiva¹³.

Es importante señalar que no solo el sector TIC, sino todo el sector público y privado se ven beneficiados por estas tecnologías. Así, se hace necesario que, para contribuir a la universalidad, el Estado procure el cierre de la brecha digital, especialmente si se tiene en cuenta que las TIC son una herramienta necesaria para el ejercicio de varios derechos fundamentales en el siglo XXI. Además, aparte de la ampliación de la cobertura y el aumento en la calidad en la conectividad, es necesario que se generen políticas encaminadas a la apropiación de las TIC. De lo contrario, todo lo que se avance en términos de infraestructura y equipos no será explotado suficientemente, los que implica perder los beneficios que conllevan estas tecnologías.

Por otra parte, todas las entidades territoriales y de orden nacional, de conformidad con sus funciones, deberán velar por la universalidad de las TIC. De hecho, su papel es clave como mecanismo para el ejercicio de derechos fundamentales, en un marco de cooperación, coordinación y colaboración. En general, es importante que todos los países implementen una política de universalidad que no deje atrás a la población más vulnerable del progreso tecnológico.

Adicionalmente, es importante, en materia tributaria, generar condiciones de certeza jurídica para los inversionistas, a través de la conservación de los beneficios ya existentes (como la exención de impuestos a equipos que tengan un determinado valor máximo). Asimismo, debe contemplarse la posibilidad de crear nuevos, como la exención del Impuesto de Valor Agregado –IVA–, especialmente a quienes aún no tienen acceso a estos servicios –estratos 1 y 2–, pues la regulación tributaria debe propiciar la conectividad del país (Contreras, 2021).

Una excelente práctica peruana que debería ser implementada en Colombia es la disponibilidad de los contratos de los servicios públicos de telecomunicaciones en lenguas nativas, pues más de 820.000 personas en el país las hablan y es necesario que esta población, en aras de lograr su inclusión y la garantía de sus derechos, comprendan plenamente dichos acuerdos jurídicos (Diario El Peruano, 2021; DANE, 2019).

Finalmente, resulta importante recordar que la Ley de 2019 reiteró que el Estado y todos los agentes deben colaborar en priorizar el acceso y uso de las TIC en la producción de bienes y servicios, en condiciones no discriminatorias en la conectividad, la educación, los contenidos y la competitividad. En ese sentido, es necesario evaluar periódicamente

que el MTC deberá demostrar ampliamente que se da la causal señalada (Contreras, 29 de abril de 2021).

13 Artículo 11 de la Ley 1341 de 2009 modificado por la Ley 1978 de 2019: "...El Gobierno nacional podrá establecer bandas de frecuencias de uso libre de acuerdo con las recomendaciones de la UIT. Así mismo, podrá establecer bandas exentas del pago de contraprestaciones para programas sociales del Estado que permitan la ampliación de cobertura en zonas rurales".

la eficiencia, eficacia e impacto de los planes, programas y proyectos orientados a cerrar la brecha digital.

8. Conclusiones

Las Tecnologías de la Información y las Comunicaciones han revolucionado la forma de vida de las personas. Sin embargo, por efecto de la brecha digital existente, no todos tienen la posibilidad de beneficiarse de ellas. Esto implica la vulneración de los derechos fundamentales que se ejercen por aquella vía, situación que se ha visto especialmente afectada a raíz de la pandemia de COVID-19.

Por ello, en Colombia, se han tomado diversas medidas para lograr la universalidad de las TIC. No obstante, estos esfuerzos no son suficientes, tal como lo reflejan las cifras de conectividad del país. Situación similar ocurre en el Perú.

En este escrito, se recomienda continuar promoviendo políticas públicas que busquen lograr el acceso y servicio universal de la población a las TIC, por ejemplo, mediante medidas afirmativas para la inclusión de la población relegada de las TIC, desarrolladas con un enfoque territorial; la generación de datos relevantes frente a las medidas ya implementadas, que permitan monitorearlas y mejorarlas; la promoción de la inversión, a través de la seguridad jurídica, la libre competencia y la eliminación de barreras en términos de trámites y servicios para desplegar infraestructura y ampliar la cobertura y apropiación de las TIC; la promoción de la participación de todos los agentes del ecosistema digital y aporte de los mismos, considerando que todos se benefician de la conectividad; la evaluación costo-eficiencia y visión prospectiva de las tecnologías a implementar en el país; el incentivo al pago de los PRST a través de obligaciones de hacer; el aumento de la calidad y apropiación de las TIC; y mantener una política de gobierno digital que involucre a toda la población en la transformación digital.

El acceso a Internet como un servicio público de telecomunicaciones de carácter esencial y universal deberá responder a un concepto evolutivo y dinámico que reconozca la importancia de construir una sociedad conectada con internet de calidad.

Referencias bibliográficas

- Álvarez, C. (2018). *Telecomunicaciones y Radiodifusión en México*. Posgrado de Derecho de la UNAM.
- Asamblea General de las Naciones Unidas (21 de octubre de 2015). Resolución 70/1. https://unctad.org/meetings/es/SessionalDocuments/ares70d1_es.pdf
- Banco Interamericano de Desarrollo. (2018). *Estudio del BID insta a América Latina y el Caribe a modernizar la gobernanza de las telecomunicaciones para reducir la brecha digital*. <https://www.iadb.org/es/noticias/estudio-del-bid-insta-america-latina-y-el-caribe-modernizar-la-gobernanza-de-las>
- Banco Mundial. (2016). *Exploring the Relationship Between Broadband and Economic Growth*. Disponible en: <http://documents.worldbank.org/curated/en/17870146798875888/pdf/102955-WP-Box394845B-PUBLIC-WDR16-BP-Exploring-the-Relationship-between-Broadband-and-Economic-Growth-Minges.pdf>
- Cámara de Representantes de Colombia. (2020). [Proyecto de Ley 109 de 2020]. <https://congresovisible.uniandes.edu.co/proyectos-de-ley/pley-de-internet->

[como-servicio-publico-esencial-y-universal-o-por-medio-de-la-cual-se-modifica-la-ley-1341-de-2009-y-se-dictan-otras-disposiciones-internet-como-servicio-esencial/10801/](https://www.congresovisible.uniandes.edu.co/proyectos-de-ley/ppor-medio-del-cual-se-crea-el-minimo-vital-de-internet-y-se-dictan-otras-disposiciones-crea-el-minimo-vital-de-internet/10801/)

Cámara de Representantes de Colombia. (2020). [Proyecto de Ley 30 de 2020]. <https://congresovisible.uniandes.edu.co/proyectos-de-ley/ppor-medio-del-cual-se-crea-el-minimo-vital-de-internet-y-se-dictan-otras-disposiciones-crea-el-minimo-vital-de-internet/10615/#tab=0>

Comisión Interamericana de Derechos Humanos. (26 de marzo de 2021). *¿Cómo promover el acceso universal a Internet durante la pandemia de Covid-19?* http://www.oas.org/es/cidh/sacroi_covid19/documentos/03_guias_practicas_internet_esp.pdf

Comisión de Regulación de Comunicaciones (2019). Observaciones al documento condiciones de acceso, uso y remuneración para utilización de infraestructura del sector de energía eléctrica, en el despliegue de redes y/o la prestación de servicios de telecomunicaciones. Disponible en: <https://www.crc.com.gov.co/uploads/images/files/OBSERVACIONES%20MEDIA%20COMMERCE%20PARTNERS.%20SAS.pdf>

Comisión de Regulación de Comunicaciones. (05 de abril de 2020). [Resolución 5960]. https://normativa.colpensiones.gov.co/colpens/docs/resolucion_crc_5960_2020.htm

Congreso de la Republica de Colombia. (25 de mayo de 2019). [Ley 1955 de 2019]. Plan Nacional de Desarrollo 2018-2022. DO: 50.964.

Congreso de la Republica de Colombia. (30 de julio de 2001). [Ley 671 de 2001]. DO: 44.503

Congreso de la Republica de Colombia. (30 de julio de 2009). [Ley 1341 de 2009]. DO: 47.426

Congreso de la Republica de Colombia. (25 de julio de 2019). [Ley 1978 de 2019]. DO: 51.025

Congreso de la Republica de Colombia. (12 de mayo de 2021). [Ley 2088 de 2021]. DO: 51.672

Congreso de la República de Perú. (2006). [Ley 28900]. Ley que otorga al Fondo de Inversión de las Telecomunicaciones – Fitel la calidad de persona jurídica de derecho público, adscrita al sector de transportes y comunicaciones. https://leyes.congreso.gob.pe/Documentos//2006_2011/ADLP/Normas_Legales/28900-LEY.pdf

Congreso de la República de Perú. (2008). [Decreto Ley 1019]. Decreto Legislativo que aprueba Ley de Acceso a la Infraestructura de los Proveedores Importantes de Servicios Públicos de Telecomunicaciones. <https://leyes.congreso.gob.pe/Documentos/DecretosLegislativos/01019.pdf>

Congreso de la República de Perú. (2012). [Ley 29904]. Ley de Promoción de la Banda ancha y Construcción de la red dorsal nacional de fibra óptica. <https://leyes.congreso.gob.pe/Documentos/Leyes/29904.pdf>

- Congreso de la República del Perú. (2017). [Proyecto de Ley 2780-CR]. https://leyes.congreso.gob.pe/Documentos/2016_2021/Dictamenes/Proyectos_de_Ley/02780DC23MAY20200721.pdf
- Congreso de la República del Perú. (2018). [Proyecto de Ley 3156-CR]. https://leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL0315620180801.pdf
- Congreso de la República del Perú. (2018). [Proyecto de Ley 3607-CR]. https://leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL0360720181106.pdf
- Congreso de la República del Perú. (2020). [Proyecto de Ley 5600-CR]. http://www.congreso.gob.pe/Docs/comisiones2020/ConstitucionReglamento/files/dictamen_com/dictamen_acceso_internet.pdf
- Congreso de la República del Perú. (2020). [Proyecto de Ley 5843-CR]. http://www.congreso.gob.pe/Docs/comisiones2020/ConstitucionReglamento/files/presentaciones/14.10_presentaciOn_del_pl_5843-2020-pl_acceso_a_internet.pdf
- Constitución Política de Colombia [C.P.]. (1991). <https://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf>
- Contreras. (18 de mayo de 2021). *Digital Series Colombia | “Regulación tributaria debe propiciar la conectividad en el país”*: Carlos Zenteno, presidente de Claro. <https://digitalpolicylaw.com/regulacion-tributaria-debe-propiciar-la-conectividad-en-colombia-claro/>
- Contreras. (29 de abril de 2021). *Perú se juega el rumbo de la red dorsal de fibra con elecciones en puerta y la urgente brecha digital*. <https://digitalpolicylaw.com/peru-se-juega-el-rumbo-de-la-red-dorsal-de-fibra-con-elecciones-en-puerta-y-la-urgente-brecha-digital/>).
- Corte Constitucional. (29 de enero de 2020). Sentencia T-030 de 2020. [M.P. Fajardo, D.]
- Corte Suprema de Justicia, Sala de Casación Civil. (4 de junio de 2020). Sentencia STC 3610-2020. [M.P. Tolosa, L.]
- CPE. (s.f.). *¿Qué es computadores para educar?* <https://www.computadoresparaeducar.gov.co>
- DANE. (2019). *Población Indígena de Colombia*. <https://www.dane.gov.co/files/investigaciones/boletines/grupos-etnicos/presentacion-grupos-etnicos-2019.pdf>).
- De la Quadra. (2010). *Reflexiones Sobre el Nuevo Marco Normativo de las Tecnologías de la Información y las Comunicaciones en Colombia. Comentarios a la Ley de Tecnologías de la Información y las Comunicaciones –TIC (Ley 1341 de 2009)*. Ed. Universidad Externado de Colombia.
- Departamento Administrativo Nacional de Estadística. (2018). *Medida de pobreza multidimensional municipal de fuente censal 2018*. <https://www.dane.gov.co/index.php/estadisticas-por-tema/pobreza-y-condiciones-de-vida/pobreza-y-desigualdad/medida-de-pobreza-multidimensional-de-fuente-censal>

- Departamento Nacional de Planeación. (2018). *Aumentar acceso a internet de calidad de población vulnerable disminuirá el índice de desigualdad de ingresos*. Disponible en: <https://www.dnp.gov.co/Paginas/Aumentar-acceso-a-Internet-de-calidad-de-poblacion-vulnerable-disminuira-el-indice-de-desigualdad-de-ingresos.aspx>
- Departamento Nacional de Planeación. (2020). CONPES 4001. <https://colaboracion.dnp.gov.co/CDT/Copres/Econ%C3%B3micos/4001.pdf>
- Departamento Nacional de Planeación. (s.f.). *Plan Nacional de Desarrollo 2018-2022*. <https://www.dnp.gov.co/DNP/Paginas/Plan-Nacional-de-Desarrollo.aspx>
- Diario El Peruano. (30 de mayo de 2021). *Aprueban contratos para los servicios públicos de telecomunicaciones en lenguas originarias*. (<https://elperuano.pe/noticia/121691-aprueban-contratos-para-los-servicios-publicos-de-telecomunicaciones-en-lenguas-originarias>)
- ESAN Graduate School of Business. (13 de diciembre de 2019). *Telecomunicaciones en el Perú: actualidad y retos para el país. Entrevista a Peter Yamakawa*. [Archivo de video]. YouTube. <https://www.youtube.com/watch?v=p9lTi1iHd5k>
- Guerra. (2010). *La Ley de las Tecnologías de la Información y las Comunicaciones (Ley 1341 de 2009). Comentarios a la Ley de Tecnologías de la Información y las Comunicaciones – TIC (Ley 1341 de 2009)*. Ed. Universidad Externado de Colombia.
- Herrera, L. (2010). *Acceso y servicio universal y las obligaciones de servicio público. Comentarios a la Ley de Tecnologías de la Información y las Comunicaciones – TIC (Ley 1341 de 2009)*. Ed. Universidad Externado de Colombia.
- Instituto Geográfico Agustín Codazzi. (2015). *Tan solo el 0,3 por ciento de todo el territorio colombiano corresponde a áreas urbanas: IGAC*. <https://igac.gov.co/es/noticias/tan-solo-el-03-por>
- Instituto Nacional de Estadística e Informática. (25 de junio de 2020). *El 40,1% de los hogares del país tuvo acceso a internet en el primer trimestre del 2020*. http://m.inei.gob.pe/media/MenuRecursivo/noticias/np_90_2020.pdf
- Ministerio de las Tecnologías de la Información y las Comunicaciones. (2020.a). Resolución 1272 de 18 de julio de 2020. Por la cual se adiciona y modifica el artículo 1º de la Resolución número 202 de 2010. <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=94870&dt=S>
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2020.b). *Colombia cuenta con el 52% de los hogares conectados: MinTIC*. <https://www.mintic.gov.co/portal/inicio/Sala-de-Prensa/MinTIC-en-los-Medios/145214:Colombia-cuenta-con-el-52-de-los-hogares-conectados-MinTIC>
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2020.c). *Boletín Trimestral de las TIC. Cifras del Primer Trimestre de 2020*. https://mintic.gov.co/portal/715/articles-151386_Boletin_Trimestral.pdf
- Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). *Plan TIC 2018-2022*. https://micrositios.mintic.gov.co/plan_tic_2018_2022/pdf/plan_tic_2018_2022_20200107.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (23 de marzo de 2020). [Decreto 464]. http://www.secretariosenado.gov.co/senado/basedoc/decreto_0464_2020.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (13 de abril de 2020). [Decreto 540]. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=112198>

Ministerio de Tecnologías de la Información y las Comunicaciones. (15 de abril de 2020). [Decreto 555]. <https://dapre.presidencia.gov.co/normativa/normativa/DECRETO%20555%20DEL%2015%20DE%20ABRIL%20DE%202020.pdf>

Ministerio de Tecnologías de la Información y las Comunicaciones. (03 de junio de 2020). [Decreto 771]. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=127302>

Ministerio de Transporte y Comunicaciones. (07 de diciembre de 2018). [Decreto Supremo 018]. <https://www.gob.pe/institucion/mtc/normas-legales/308452-018-2018>

Organización para la Cooperación y el Desarrollo Económicos. (2016). *Más allá de la banda ancha en América Latina y el Caribe*. <https://www.oecd-ilibrary.org/docserver/9789264259027-4-es.f?expires=1617304624&id=id&accname=guest&checksum=8772767D8CBED326F5D802331391E2E7>

OSPITEL. (s.f.). Nosotros. <https://www.osiptel.gob.pe/informacion-institucional/nosotros/>

Parlamento Europeo y del Consejo (2018). Código Europeo de las Comunicaciones Electrónicas. <https://eurlex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:32018L1972&from=ES>

Portafolio. (12 de julio de 2019). Colombia es cada vez más desigual, asegura el DANE. Portafolio. <https://www.portafolio.co/economia/colombia-es-cada-vez-mas-desigual-asegura-el-dane-531503>

Presidencia de la República del Perú. (2021). [Decreto Supremo No. 010]. [https://cdn.www.gob.pe/uploads/document/file/1761063/DS%20N%200010-2021-MTC.pdf](https://cdn。www.gob.pe/uploads/document/file/1761063/DS%20N%200010-2021-MTC.pdf)

PRONATEL. (s.f.) Programa Nacional de Telecomunicaciones. <https://www.gob.pe/pronatel>

Senado de Colombia. (2020). [Proyecto de Ley 285 de 2020]. <https://congresovisible.uniandes.edu.co/proyectos-de-ley/ppor-medio-de-la-cual-se-dictan-medidas-para-disminuir-las-brechas-de-acceso-universal-a-internet-y-se-dictan-otras-disposiciones--mas-conectados-acceso-universal-a-internet/11277/>

Senado de Colombia. (2020). [Proyecto de Ley 321 de 2020]. <https://congresovisible.uniandes.edu.co/proyectos-de-ley/ppor-medio-del-cual-se-implementa-el-minimo-vital-en-los-servicios-publicos-domiciliarios-de-energia-agua-alcantarillado-y-gas-domiciliario-y-en-el-servicio-de-acceso-a-internet-y-se-dictan-otras-disposiciones-minimo-vital-en-servicios-publicos/11340/#tab=0>

Tello, M. (2019). Brecha digital en el Perú: Diagnóstico, acceso, uso e impactos. <https://departamento.pucp.edu.pe/economia/wp-content/uploads/Mario-Tello.-Brecha-digital.-INEI.pdf>

UIT. (s.f.). *Reformular el Acceso Universal*. <https://www.itu.int/itunews/manager/display.asp?lang=es&year=2007&issue=07&ipage=universal-access&ext=html>

Zegarra, D. (2018). *Introducción al Derecho de las Telecomunicaciones*. <http://www.untumbes.edu.pe/vcs/biblioteca/document/varioslibros/0986.%20Introducción%20al%20derecho%20de%20las%20telecomunicaciones.pdf>



LA AUTONOMIA DE FACTO DEL REGULADOR DE LAS TELECOMUNICACIONES

THE 'DE FACTO' AUTONOMY OF THE TELECOMMUNICATIONS REGULATOR

GONZALO RUIZ DIAZ¹

RESUMEN

La autonomía del organismo regulador constituye un requisito importante que busca garantizar que las decisiones que éste adopta sean técnicas e imparciales. En el caso del regulador peruano de las telecomunicaciones, estudios pasados (Ruiz y Granda (2015) y UIT (2016)) basados en la metodología introducida por Gilardi (2002) han mostrado que el estándar de autonomía formal o 'de jure' del OSIPTEL es relativamente alto respecto de sus pares de la región. Sin embargo, el nivel de autonomía de una agencia reguladora también puede estar relacionado con reglas informales, así como con la efectividad con la cual dichas reglas se cumplen en la práctica. El presente artículo, utilizando la metodología introducida por Maggetti (2007) y usando información secundaria, así como los resultados del estudio de OECD (2019), estima el nivel de autonomía 'de facto' del regulador. El principal resultado alcanzado es que los niveles de autonomía de facto de OSIPTEL estimados son inferiores comparados con los obtenidos en el caso de la autonomía formal, debido principalmente a la influencia del poder ejecutivo en las decisiones de carácter presupuestal y organizacional del regulador.

ABSTRACT

The autonomy of the regulatory body is an important requirement that seeks to ensure its technical and impartial decisions. Studies applied to the Peruvian telecommunications regulator (Ruiz and Granda (2015) and ITU (2016)), based on the methodology introduced by Gilardi (2002) have shown that the formal or 'de jure' autonomy standard held by OSIPTEL is relatively high compared to its peers in the region. However, the degree of autonomy of a regulatory agency can also be related to informal rules as well as the effectiveness with which those rules are enforced in practice. This article, using the methodology introduced by Maggetti (2007), secondary information as well as the results of the OECD study (2019), estimates the 'de facto' degree of autonomy of the regulator. The main result achieved is that the 'de facto' degree of autonomy estimated for OSIPTEL are lower compared to those obtained in the case of formal autonomy, mainly due to the influence of the central government in the budgetary and organizational decisions of the regulator.

1 Director de la Maestría en Regulación de Servicios Públicos. Ha sido Presidente del Consejo Directivo del Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL), Vice Ministro de Comunicaciones del MTC y Secretario Técnico del FITEL, miembro del Comité de Promoción de la Inversión en Carreteras, Aeropuertos y Ferrocarriles de PROINVERSION. Es Doctor en Economía de la PUCP; Master of Arts in Economics, Programa de Postgrado en Economía ILADES/Universidad de Georgetown, Santiago de Chile. Ha sido también Presidente de la Comisión de Protección al Consumidor, Director de la Escuela de la Competencia y la Propiedad Intelectual y Gerente de Estudios Económicos en INDECOPI; así como Gerente de Regulación de OSITRAN. Actualmente es Economista Asociado de Macroconsult. Contacto: gruiz@pucp.edu.pe

PALABRAS CLAVE

Autonomía Regulatoria | Partes Interesadas
| Organismo Regulador | OSIPTEL

KEY WORDS

Regulatory Autonomy | Stakeholders |
Regulatory Body | OSÍPTEL

CONTENIDO

1. Introducción; **2.** Autonomía regulatoria y entorno institucional; **2.1.** De la Autonomía formal a la autonomía de facto; **2.2.** Autonomía frente a actores políticos; **2.3** Autonomía frente a Regulados; **3.** Resultados y reflexiones finales.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 16 de mayo de 2021 y aprobado para su publicación el 12 de agosto de 2021.

1. INTRODUCCIÓN

Entre los cambios institucionales impulsados en la región destinados a atraer la inversión privada a sectores de infraestructura, durante la década del noventa, destaca especialmente la creación de agencias autónomas a cargo de la regulación y supervisión de servicios públicos. Según Levi-Faur y Jordana (2004), entre 1990 y 2000, el número de agencias reguladoras² se triplicó en América Latina. La literatura (Levi y Spiller, 1994) ha asociado este proceso con la necesidad de dotar a la regulación de la independencia e imparcialidad necesarias que permita mitigar los riesgos asociados a la intervención administrativa de los gobiernos en los mercados.

Uno de los primeros intentos de conceptualizar y medir el grado de independencia de agencias reguladoras fue planteado por Gilardi (2002), quien construye un índice que busca capturar el conjunto de reglas formales que caracterizan a una agencia reguladora, entre los que destacan, el *status* del líder de la agencia, el *status* de los miembros de sus consejos directivos, la relación entre la agencia y el parlamento, la organización y autonomía presupuestaria y las competencias reguladoras. Ruiz y Granda (2015) y UIT (2016) en estudios distintos aplicados al OSIPTEL encontraron que este regulador ha gozado de niveles de autonomía formal relativamente altos respecto de sus pares de la región.

Si bien el conjunto reglas formales asociadas a los aspectos listados arriba, puede influir de manera importante en el grado de autonomía de un organismo regulador; Maggetti (2007) y Gilardi y Maggetti (2010) subrayan que el nivel de independencia de una agencia reguladora también puede estar relacionado con reglas informales, así como de la efectividad con la cual dichas reglas se cumplen en la práctica. Estos autores resaltan que el grado de autonomía con el que cuenta un organismo regulador está asociado con su capacidad de definir sus objetivos regulatorios y la ausencia de interferencias o

2 El uso del término agencia independiente recoge la terminología empleada por la literatura y su uso proviene de la tradición sajona. Es importante tener en cuenta, sin embargo, el diseño institucional establecido en el Perú, proviene en gran medida de modelos tomados precisamente de esos países. Igualmente, la literatura hace uso indistinto de los términos de autonomía e independencia. Por otro lado, la legislación peruana, en particular la Ley Marco de Organismos Reguladores (art. 2), define a los organismos reguladores como entidades con autonomía administrativa, funcional técnica, económica y financiera. En tal sentido, aún reconociendo que ambos términos pueden tener interpretaciones y matices diferentes, para efectos del presente artículo, ambos se utilizarán de manera indistinta.

restricciones en la aprobación y aplicación de sus regulaciones.

El presente artículo, complementa el elaborado por Ruiz y Granda (2015), buscando cuantificar el nivel de autonomía de facto del regulador de las telecomunicaciones. El análisis utiliza la metodología introducida por Maggetti (2007) y se basa principalmente en información proveniente de los hallazgos resultantes del estudio elaborado por OECD (2019). Un resultado importante de la evaluación, es que el nivel de autonomía de facto del regulador peruano es menor al nivel de autonomía formal calculado por estudios previos; debido fundamentalmente a su menor autonomía relativa respecto de la influencia proveniente de actores del sector público.

En la siguiente sección, se discuten los conceptos de autonomía, así como los principales resultados obtenidos de la medición de autonomía formal aplicada al Perú y otros países de la región. En una tercera sección, se presenta la implementación de la metodología introducida por Maggetti (2007). En una cuarta sección se presentan las conclusiones.

2. AUTONOMIA REGULATORIA Y ENTORNO INSTITUCIONAL

OECD (2016, p. 35-36) identifica cuatro argumentos en favor de la autonomía regulatoria como un atributo deseable del organismo regulador:

- (i) **Externalidades:** Valor privado y social de la infraestructura. Con frecuencia la valoración privada de la infraestructura, representada por la disposición a pagar del consumidor es inferior al valor social de la misma. Ello hace necesario que el organismo regulador establezca tarifas que reflejen dicho valor social. No obstante ello, el regulador puede recibir presiones del gobierno o de la industria en búsqueda de condiciones tarifarias más favorables al consumidor o a la propia industria.
- (ii) **Falta de neutralidad frente a empresas establecidas (incumbentes o entrantes).** Un regulador que carezca de autonomía, puede ceder a presiones de empresas establecidas inhibiendo la entrada de competidores al mercado. En contextos en los que el incumbente o empresa establecida es una empresa estatal, las presiones del gobierno podrían afectar la neutralidad del regulador.
- (iii) **Tecnicismo del regulador y asimetrías de información.** La autonomía constituye un requisito importante que asegura que el regulador pueda construir y retener las capacidades técnicas y el conocimiento de la industria necesarios para enfrentar los problemas de información asimétrica (riesgo moral y selección adversa, ver Tirole y Laffont (1993)).
- (iv) **Riesgo de Captura.** Un regulador sin autonomía es más proclive a sucumbir a las presiones de la industria regulada y adoptar decisiones que afecten su imparcialidad y tecnicismo.

Estos cuatro argumentos, tienen en común el hecho de que la autonomía regulatoria contribuye a la corrección de lo que se denomina 'fallas de mercado'³.

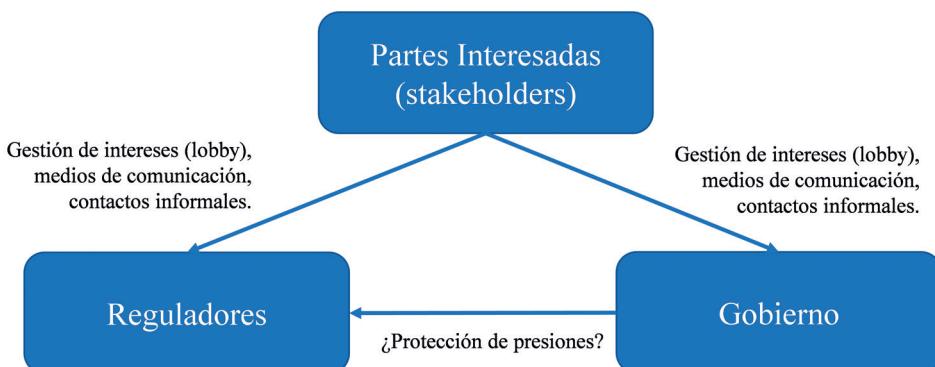
En términos generales, el concepto de autonomía del regulador tiene una doble dimensión.

3 Para una revisión del concepto de falla de mercado ver Stiglitz (1989).

Una primera está vinculada a las presiones de la industria y sectores regulados mientras una segunda puede provenir del ámbito político, que involucra a diversos poderes del Estado y a partidos políticos. La literatura económica sobre la captura del regulador (ver Stigler (1971) y Peltzman (1976)) describe a los reguladores como organizaciones cuya función objetivo pondera los intereses de los votantes (producto de la presión política) y de la industria regulada (producto de la presión económica).

Una noción algo distinta es la que plantea la OECD (2016) al introducir al gobierno, como un actor importante en el proceso regulatorio. Como muestra el Diagrama N°1, el regulador enfrenta principalmente las presiones provenientes de la industria y del gobierno; pudiendo estas últimas ser un reflejo indirecto de las primeras. En este contexto, el gobierno puede optar por servir de protección al regulador de dichas presiones o, por el contrario, ser un canalizador de dichas presiones.

Diagrama N°1. Autonomía del Regulador, frente a partes interesadas y gobierno.



Fuente: OECD (2016), adaptado por el autor.

El grado de interferencia tanto del gobierno como de los *stakeholders* en la labor regulatoria, es influenciado por el marco institucional formal (funciones y competencias conferidas por ley a los organismos reguladores) así como por factores informales, políticos y económicos. Los primeros pueden influir en los segundos; sin embargo, no necesariamente son determinantes.

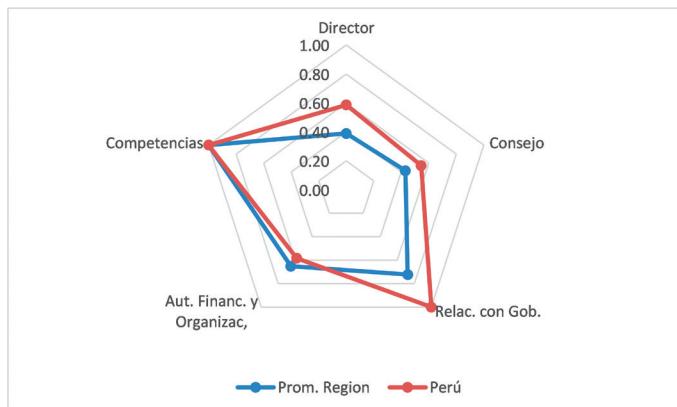
En efecto, en el caso del Organismo Supervisor de la Inversión Privada en Telecomunicaciones (OSIPTEL), Ruiz y Granda (2015) y UIT (2016) han evaluado el nivel de autonomía formal del regulador a partir de la metodología introducida por Gilardi (2002), encontrando que los niveles de independencia registrados son relativamente altos comparados con el resto de regladores de las telecomunicaciones.

A partir de la metodología desarrollada por Gilardi (2002), Ruiz y Granda (2015) calcularon un índice de autonomía, que en una escala del 0 al 1 (donde 1 es total autonomía y cero es ausencia absoluta de autonomía), registra un valor de 0.67⁴. Un nivel similar fue registrado por UIT (2016) ascendente a 0.66. Estos niveles resultan

4 Para una descripción de la metodología ver Ruiz y Granda (2015, pp. 215-224).

relativamente altos si se comparan con el promedio de la región el cual asciende a 0.52⁵. El Gráfico N°1 muestra el resultado de dicha medición descomponiendo la medición por categoría de evaluación:

Gráfico N°1. Medición de Autonomía Formal



Fuente: UIT (2016), adaptado por el autor.

Como se aprecia, Perú aventaja en promedio a la región en los niveles de autonomía formal referidos a los órganos de dirección del regulador (presidencia y consejo directivo), así como en la categoría relativa a la relación con el gobierno. En contraste, muestra una puntuación inferior en lo que respecta a los aspectos financieros y organizacionales.

En la siguiente sección se describen los resultados de la medición del grado de autonomía de facto aplicada al caso del OSIPTEL.

2.1 DE LA AUTONOMIA FORMAL A LA AUTONOMIA DE FACTO

El artículo 2 de la Ley Marco de los Organismos Reguladores (LMOR) establece que estos son organismos públicos descentralizados adscritos a la Presidencia del Consejo de Ministros con autonomía administrativa, funcional, técnica, económica y financiera. Un análisis formal de los artículos contenidos en esta ley marco, así como de las normas específicas y reglamentos aplicables a cada organismo regulador llevaría a concluir que el estándar de autonomía establecido por el marco regulatorio peruano es relativamente alto, en comparación con otros países.

Si bien el análisis de las reglas formales a partir de las cuales se desarrolla la labor del regulador resulta útil para conocer su entorno institucional; es posible que en los hechos, los grados de libertad con que este cuente para llevar adelante sus mandatos legales, respondan a factores adicionales que afecten positiva o negativamente su autonomía. Gilardi y Maggetti (2010) y Maggetti (2007) señalan que la autonomía de facto consta de dos componentes: (i) la capacidad relativa de 'autodeterminación' de las preferencias u objetivos regulatorios por parte de las agencias reguladoras o, y, (ii) la ausencia

5 Considera el cálculo para los siguientes países miembros de Regulatel: Brasil, Chile, Colombia, Costa Rica, Guatemala, México, República Dominicana, Puerto Rico y Uruguay. Se ha tomado solo la información de los países que respondieron los cuestionarios remitidos por los consultores de UIT.

relativa de restricciones para la aprobación y aplicación de regulaciones de parte de las autoridades políticas y/o los regulados. Ambos componentes, buscan evaluar en qué medida los objetivos y decisiones regulatorias pueden ser diseñados, implementados y supervisados con independencia “relativa” por la agencia reguladora. Es importante resaltar el adjetivo “relativa” pues se entiende que la autonomía absoluta de cualquier entidad pública, en regímenes políticos democráticos y con mecanismos de rendición de cuentas, con pesos o contrapesos; resultaría inviable.

A fin de evaluar los dos componentes arriba mencionados, Maggetti (2007) considera necesario separar el nivel de autonomía en función de distintos tipos de actores: autoridades políticas y regulados (ver Tabla N°1). En ambos casos se evalúan aspectos relacionados con la existencia de “puertas giratorias” en la salida y entrada de funcionarios del regulador hacia/desde organizaciones que pertenezcan a uno u otro sector. Asimismo, se examina la frecuencia de los contactos con ambos tipos de organización.

Adicionalmente, en el caso de las autoridades políticas, se evalúa su influencia en la determinación o uso del presupuesto o en la organización interna del regulador. En cambio, en el caso de las entidades reguladas, se examina cuán adecuado es el presupuesto o su organización interna para desempeñar su labor frente a los regulados. Otro ítem importante en el caso de la autonomía frente a autoridades políticas está referido a la participación de partidos políticos en la designación de funcionarios y la vulnerabilidad política de la entidad. En el caso de la autonomía frente a las entidades reguladas, se evalúa la relación entre la especialidad o profesión de los miembros de los órganos de dirección (presidente o miembros del consejo directivo) y el perfil de profesionales requerido en la industria. Por último, tanto para la medición de la autonomía frente a actores políticos como entidades reguladas; se evalúa la influencia externa de ambos tipos de organización sobre la regulación.

Es importante advertir, que cada uno de estos conceptos utilizados para medir autonomía de facto no involucra necesariamente una connotación negativa de ciertas actividades que pueda desplegar el organismo regulador con stakeholders o entidades públicas; sino debe entenderse como situaciones que, sin las precauciones y salvaguardas necesarias, pueden poner en riesgo dicha autonomía.

Tabla N° 1. Determinantes de Autonomía ‘De Facto’⁶

| | |
|-----------------------------------|--|
| Frente a Actores Políticos | <ul style="list-style-type: none">- Flujo de funcionarios hacia y desde regulador hacia a organizaciones (puerta giratoria).- Frecuencia de contactos.- Influencia en el presupuesto.- Influencia en la organización interna.- Participación de partidos en designaciones.- Vulnerabilidad Política.- Influencia externa en la regulación. |
|-----------------------------------|--|

⁶ En el Apéndice 1 de Maggetti (2007) se presenta la relación de preguntas específicas que propone dicho autor a fin de evaluar cada uno de los aspectos listados en la Tabla 1.

| | |
|-------------------------------------|---|
| Frente a Entidades Reguladas | <ul style="list-style-type: none"> - Flujo de funcionarios hacia y desde regulador hacia a organizaciones (puerta giratoria). - Frecuencia de contactos. - Presupuesto adecuado. - Organización Interna Adecuada. - Actividad Profesional del Presidente/Miembros del Consejo. - Influencia externa en la regulación. |
|-------------------------------------|---|

Fuente: Maggetti (2007).

La metodología general utilizada para dar respuesta a las preguntas relacionadas con los ítems listados en la Tabla N°1, aplicada por dicho autor, consistió en el envío de cuestionarios a directores de agencias reguladoras y el uso de información secundaria. En el presente caso, nos basaremos exclusivamente en información secundaria y de manera especial en los resultados del estudio elaborado en 2019 por la OCDE (2019) titulado “Driving the Performance at Peru’s Telecommunications Regulator”, elaborado por un grupo de expertos que hizo un examen general del status institucional y organizacional del OSIPTEL.

A fin de que el indicador que se obtenga sea comparable con el calculado para determinar la autonomía formal, se utilizará una escala del 0 al 1; donde 0 indica total ausencia de autonomía mientras 1, plena autonomía. Como categorías intermedias asignaremos un valor de 0.25 en el caso de la evaluación arroje un nivel bajo, de 0.5 si se considera un nivel medio y de 0.75 si se considera un nivel alto de autonomía.

2.2 AUTONOMÍA FRENTE ACTORES POLÍTICOS

Siguiendo a Maggetti (2007), el término “actores políticos” que se emplea en el presente artículo engloba tanto a otras entidades distintas de los reguladores, que forman parte del Poder Ejecutivo; como el Ministerio de Transportes y Comunicaciones (MTC), el Ministerio de Economía y Finanzas (MEF) o la Presidencia del Consejo de Ministros (PCM) así como el Poder Legislativo y partidos políticos. En tal sentido se busca determinar en qué medida el comportamiento de estos 3 tipos de organización puede afectar la autonomía del regulador.

– **Flujo de funcionarios hacia y desde regulador hacia a organizaciones (puerta giratoria).**

El desarrollo de experiencia y habilidades en el sector de las telecomunicaciones por lo general requiere de años de trabajo y/o estudio, indispensables para alcanzar cierto grado de especialización. A pesar de que, durante los últimos años, en el Perú, se han desarrollado programas de pregrado y posgrado vinculados a la regulación, al estudio del sector de las telecomunicaciones y de los esfuerzos desplegados por el OSIPTEL a través de sus cursos de extensión universitaria; el número de especialistas y profesionales con experiencia en regulación continúa siendo limitado. En tal sentido, no debe sorprender la rotación de profesionales con experiencia en esta rama, entre distintas instituciones que tienen competencias en el sector.

Con relación al influjo de profesionales desde otras instituciones públicas hacia el regulador, en la actualidad no existen impedimentos formales para que funcionarios que han laborado en otras organizaciones del Poder Ejecutivo puedan ingresar al OSIPTEL. No obstante, esta figura al menos en los órganos ejecutivos y de dirección, ha sido

poco frecuente⁷. Es importante reconocer como lo hace OECD (2019) que el número de cargos de confianza designados por el regulador es bastante reducido (1.5% del total) y el proceso de selección de profesionales en el regulador se ha basado en competencias institucionales y personales.

En contraste, dado el perfil técnico de gran parte de los funcionarios del OSIPTEL, se aprecia que, durante los últimos años, el flujo de profesionales desde el regulador hacia otras entidades públicas y, en particular, el MTC se ha incrementado. En efecto, se ha observado una presencia creciente de ex funcionarios del regulador en direcciones generales del MTC vinculadas a la regulación y/o supervisión de servicios públicos⁸. Esta tendencia se ha venido observando con cierta regularidad en el último lustro. En virtud de ello consideramos razonable asignar a esta categoría un puntaje de 0.75.

– Frecuencia de contactos.

Como menciona OECD (2019), OSIPTEL interactúa con diversas entidades del Poder Ejecutivo así como con el Congreso de la República, a través de distintos canales, en base al llamado “Principio de Colaboración Efectiva”. Estos mecanismos de coordinación o contacto, no son sistemáticos y estructurados, siendo a menudo facilitados mediante canales “ad hoc” basados en relaciones inter-personales:

The relationship between these entities is governed by the principle of effective collaboration through agreements of inter-institutional collaboration that facilitate activities of co-ordination and mutual co-operation. There are no structured coordination mechanisms with other public administration bodies, including the other economic regulators. Co-ordination is often facilitated rather through ad hoc channels based on personal relationships established between senior officials at OSIPTEL and the public administration bodies. OECD (2019, p. 66).

Existen diversos espacios de encuentro y colaboración entre funcionarios del MTC y OSIPTEL. Por ejemplo, para la definición de posiciones en foros internacionales como la Comisión Interamericana de Telecomunicaciones (CITEL) en diversas ocasiones se ha solicitado del apoyo técnico del regulador en aspectos técnicos vinculados con la regulación.

Por otro lado, ha sido común que el MTC solicite al regulador informes técnicos respecto a proyectos de medidas o iniciativas que estén relacionadas con las competencias del regulador.

Si bien OECD (2019) recomienda que estos espacios de relacionamiento sean más sistemáticos y estructurados, no apreciamos que en este aspecto existan riesgos significativos que puedan afectar la autonomía de facto del regulador. Por esta razón, consideramos razonable asignar a este ítem un puntaje de 0.75.

7 Ejemplos recientes son el del Presidente de OSIPTEL (2012-2017) que años antes fue Viceministro de Comunicaciones o el de un ex Miembro del Consejo Directivo, quien se desempeñara previamente como Director General de Gestión y Autorizaciones, ambos en el MTC. En ambos casos, sin embargo, la designación en el cargo ocupado en el regulador se dio varios años después de que ambos funcionarios dejaron el MTC; y el tránsito entre ambas instituciones no fue directo sino proveniente de otras instituciones.

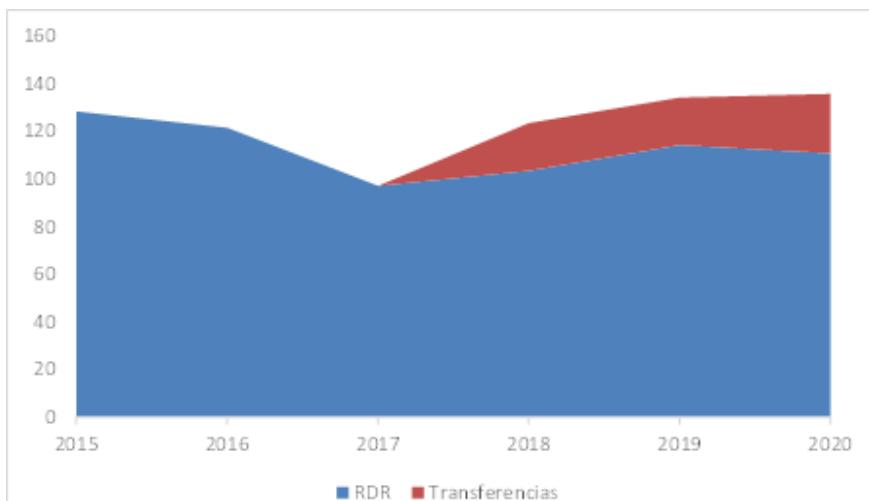
8 A la fecha de redacción del presente artículo, el Director General de Políticas y Regulación en Comunicaciones (y su antecesor) y el Director General de Fiscalizaciones y Sanciones en Comunicaciones son ex funcionarios de OSIPTEL.

– Influencia en el presupuesto

Si bien como se señaló anteriormente el artículo 2 de la LMOR confiere a los organismos reguladores de autonomía económica y financiera; en los hechos, OSIPTEL ha venido enfrentando diversas restricciones sobre la disponibilidad y uso de recursos para el cumplimiento de sus funciones. El aporte por regulación establecido en el artículo 10º de dicha Ley puede ascender hasta 1%, sin embargo, en el caso de OSIPTEL este ha permanecido en un nivel del 0.5% desde el año 2002, en que se aprobó el DS 012-2002-PCM, siendo potestad del Consejo de Ministros su modificación. Durante el 2021, mediante DS 134-2021-PCM se ha revisado por primera vez dicho porcentaje el cual se ha elevado niveles entre 0.75% y 0.80% pero solo para el caso de los servicios móviles. Como resultado de ello y de la reducción de la base imponible (los ingresos totales del sector sujetos al pago de este aporte) los recursos directamente recaudados por el regulador se han mantenido estancados durante los últimos años. A fin de hacer frente a las mayores demandas y encargos regulatorios que se verán más adelante, desde el año 2018 los ingresos de OSIPTEL han requerido ser suplementados por transferencias del gobierno central⁹.

Como muestra el Gráfico N°2, los ingresos totales del regulador registraron un incremento sostenido desde el año 2017. Sin embargo, dado que los ingresos por concepto de recursos directamente recaudados del OSIPTEL durante el período 2015 al 2020, se han mantenido relativamente estables (entre S/. 80 millones y S/. 94 millones), a partir del año 2018, las mayores demandas regulatorias, han requerido que dichos ingresos sean suplementados en cerca de S/. 20 millones adicionales (aproximadamente 15% del presupuesto total). Esta dependencia puede involucrar un riesgo para la autonomía económica y financiera del regulador establecida en la LMOR.

Gráfico N°2. Evolución de Ingresos: Recursos Directamente Recaudados y Transferencias al OSIPTEL (S/. millones)



9 OECD (2019, p.14) reconoce que actualmente los ingresos del regulador se encuentran restringidos por el gobierno central: "OSIPTEL is entirely funded by resources received from the regulated sector. In practice, its budget has been limited by central government rules that cap the amount received from the sector below what is allowed by legislation, as well as by austerity measures, leaving the regulator feeling under-resourced and unable to manage its funds freely".

Fuente: Consulta amigable – MEF, Elaboración: el autor.

Sin perjuicio de lo anterior, como la mayoría de entidades del Poder Ejecutivo, la ejecución del gasto de OSIPTEL se encuentra sujeta a las normas del Sistema Integrado de Administración Financiera (SIAF) y normativa presupuestal emitida por el MEF.

Por último, durante los últimos años, el MEF ha trasladado los saldos de balance acumulados por los organismos reguladores, entre ellos, OSIPTEL, al tesoro público; afectando con ello de manera importante la sostenibilidad económica del regulador.

En virtud de lo señalado anteriormente, el puntaje asignado a este ítem asciende a 0.0.

– Influencia en la organización interna.

Como se ha mencionado en el acápite anterior, el nivel de recursos propios con el que cuenta OSIPTEL se ha visto limitado por el gobierno central, lo cual ha obligado a éste último durante los últimos años a transferir recursos a fin de que el regulador pueda hacer frente a la creciente demanda de labores regulatorias y de supervisión. La Tabla N°2 muestra un listado no exhaustivo de funciones adicionales que ha venido asumiendo el OSIPTEL durante los últimos años, basado en información tomada de OECD (2019, p. 68) y que implican mayores niveles de gasto.

Tabla N° 2. Nuevas funciones asumidas por OSIPTEL durante los últimos años

- Supervisión y administración Registro Nacional de Equipos Terminales Móviles para la Seguridad (Renteseg).
- Regulación y Supervisión de la Red Dorsal de la Fibra Óptica (RDNFO).
- Regulación y Supervisión de los Proyectos Regionales (redes de acceso y transporte).
- Supervisión y bloqueo de señales móviles en prisiones.
- Supervisión y regulación de las reglas de acceso aplicables de dinero electrónico.
- Supervisión y regulación de las reglas de acceso para Operadores Móviles Virtuales.
- Supervisión y regulación de reglas de neutralidad de la red.
- Supervisión y regulación de mandatos de compartición de infraestructura.

Fuente: OECD (2019), adaptado por el autor.

Al mismo tiempo, como se observó en el acápite anterior, el OSIPTEL ha enfrentado restricciones financieras lo cual ha impacto en los esfuerzos de la institución para dimensionar la organización y hacer frente a las nuevas necesidades. Así, ante las mayores demandas de labores de supervisión y fiscalización, el OSIPTEL no ha podido incrementar su “tamaño” y se ha visto obligado a reasignar personal entre distintas

funciones.

La Tabla N°3 muestra la evolución del personal de OSIPTEL desde 2014 hasta 2018 reportado en OCDE (2019). A nivel general se aprecia una reducción del total del personal de la organización. Sin embargo, se observan reducciones importantes en las áreas “core” de la organización tales como la Dirección de Fiscalización y Supervisión, la Dirección de Políticas Regulatorias y Competencia y en menor medida las áreas de solución de controversias y protección al usuario. Asimismo, se observan reducciones significativas de personal en las oficinas desconcentradas; las cuales se han visto parcialmente compensadas en número por personal de apoyo.

Tabla N° 3. Evolución del Personal de OSIPTEL (2014–2018)

| | 2014 | 2015 | 2016 | 2017 | 2018 |
|--------------------------------------|------------|------------|------------|------------|------------|
| Solución de controversias | 37 | 36 | 39 | 37 | 35 |
| Oficinas desconcentradas | 75 | 76 | 71 | 66 | 45 |
| Fiscalización y Supervisión | 79 | 76 | 67 | 53 | 66 |
| Políticas Regulatorias y Competencia | 44 | 44 | 44 | 45 | 38 |
| Protección al Usuario | 29 | 28 | 26 | 25 | 27 |
| Personal de Apoyo y otros | 162 | 163 | 149 | 187 | 189 |
| TOTAL | 426 | 423 | 396 | 413 | 400 |

Fuente: OCDE (2019, p. 77), adaptado por el autor.

La información reportada por OCDE muestra que las restricciones económicas y financieras que ha venido enfrentando la organización habrían afectado su capacidad operativa y obligado a hacer ajustes en la asignación de sus recursos, en un contexto de mayor carga de trabajo. Especial mención merece el área de solución de controversias cuya labor se ha visto recargada sustancialmente durante los últimos años debido al aumento significativo de las apelaciones por concepto de reclamos de usuarios.

En virtud de lo anterior, consideramos razonable establecer una puntuación de 0.25 por este concepto.

– Participación de partidos en designaciones.

A diferencia de otros marcos institucionales como el de Estados Unidos, donde la proporción de comisionados que conforman el Consejo de las agencias reguladoras durante un determinado período presidencial guardan correspondencia con la participación de las

organizaciones políticas¹⁰; en el caso del Perú, no existe, ni se ha institucionalizado un mecanismo de este tipo en los procesos de designación de los miembros de los consejos directivos de los organismos reguladores.

En efecto, el artículo 6 de la LMOR establece que los Consejos Directivos están conformados por dos miembros a propuesta de la PCM, uno a propuesta del MEF, uno a propuesta del sector al que pertenece la actividad económica regulada (en el caso del sector telecomunicaciones, es el MTC) y un miembro en representación del Instituto de Defensa de la Competencia y la Propiedad Intelectual (INDECOPI). Los procesos de designación se rigen por mecanismos de concurso público, cuyas reglas actualmente están reguladas por el Decreto Supremo N°103-2012-PCM.

Es importante mencionar que el hecho de que los funcionarios designados, hayan sido propuestos por alguna de las entidades mencionadas anteriormente, no los convierte en representantes de los mismos ni los obliga a reportar o coordinar sus posiciones con estos; conservando dichos funcionarios libertad de decisión frente a las temáticas que aborda el regulador.

En virtud de lo anterior, consideramos que en este ítem corresponde asignar un puntaje de 1.00.

– Vulnerabilidad Política

Han sido relativamente escasos, los episodios de salida de un miembro del Consejo Directivo de OSIPTEL antes del término de su mandato. Es importante recordar que el artículo 6.6 de la LMOR establece como causales de vacancia del cargo de Miembro del Consejo Directivo, el fallecimiento, incapacidad permanente, renuncia aceptada, impedimento legal sobreviniente a la designación, remoción por falta grave e inasistencia injustificada por 3 sesiones seguidas o 5 no consecutivas en el período de un año. Sobre el particular, en los últimos años, se han dado algunos casos de renuncia al cargo de miembro del consejo directivo, por razones personales expresadas en su momento y un caso por falta grave en el año 2012. Debe mencionarse que las faltas graves se determinan luego de un proceso administrativo, en el que se otorga al funcionario el derecho a presentar sus descargos, entre otras garantías de debido proceso, y es conducido por PCM y resuelto por dicha entidad con el refrendo del MEF y el MTC¹¹.

10 Ver Feinstein B. y Hemel D. (2018) "Partisan Balance with Bite", Columbia Law Review, Vol. 118, N°1; para un análisis del caso de Estados Unidos.

11 Según el Artículo 12 del Reglamento de la LMOR constituyen faltas graves:

- (...) a) La condena por comisión de delitos dolosos, con sentencia firme;
- b) La obtención o procuración de beneficios o ventajas indebidas, para sí o para otros, mediante el uso de su cargo, autoridad o influencia;
- c) La participación en transacciones u operaciones financieras utilizando información privilegiada del Organismo Regulador o permitir el uso impropio de dicha información para el beneficio de algún interés.
- d) Incumplimiento de sustentar su voto singular o en discordia, en tres (3) acuerdos que haya adoptado el Consejo Directivo en el período de un (1) año, en la oportunidad prevista en el numeral 3 del artículo 97 de la Ley N° 27444, Ley del Procedimiento Administrativo General;
- e) La realización de actividades de proselitismo político a través de la utilización de sus funciones o por medio de la utilización de infraestructura, bienes o recursos públicos, ya sea a favor o en contra de partidos u organizaciones políticas o candidatos.

En consecuencia, puede afirmarse que es poco frecuente la salida de un miembro de Consejo Directivo antes del término de su mandato y, en aquellos casos, que ello ha ocurrido dicha salida se ha enmarcado dentro de lo establecido por la LMOR y su reglamento.

Sin perjuicio de lo anterior, no debe soslayarse un incidente importante ocurrido durante el año 2020 en el caso de OSINERGMIN, regulador que se rige por las mismas normas de la LMOR arriba citadas, y que puede sentar un grave precedente para el resto de organismos reguladores (ver Ruiz (2020))¹².

Durante dicho año, un accidente que originó la deflagración del gas que trasladaba un camión cisterna en el distrito de Villa El Salvador, cobró 34 víctimas mortales y un gran número de heridos. Pese a que se demostró que las causas del accidente fueron de diversa índole (fallas en el vehículo, desniveles en la pista y los procedimientos seguidos por el chofer), el gobierno atribuyó la responsabilidad de los hechos exclusivamente a OSINERGMIN, debido a aparentes deficiencias en sus procesos de supervisión. En virtud de ello, el Presidente del Consejo de Ministros hizo pública la solicitud de renuncia al Presidente de OSINERGMIN así como a su Consejo Directivo. Tras la renuncia del Presidente de OSINERGMIN, mediante Decreto Supremo N°023-2020-PCM se declaró en reorganización al OSINERGMIN. Este hecho sin duda pone de relieve la influencia de determinados agentes del Poder Ejecutivo a través del uso político de la figura del regulador; lo cual da cuenta de la vulnerabilidad que éstos enfrentan actualmente.

Por dicha razón consideramos que, en este acápite, corresponde asignar un puntaje de 0.25.

– Influencia externa en la regulación.

Tal como refiere OECD (2019, p. 65), la LMOR y la Ley 27336 asignan al OSIPTEL funciones de agencia de competencia, fijación de tarifas, regulatorias, de fiscalización y supervisión, de solución de controversias y solución de reclamos.

Tabla N° 4 Principales Funciones de OSIPTEL

| Función | Descripción general |
|---------------------|--|
| Competencia | Promueve competencia entre los operadores del servicio de telecomunicaciones |
| Fijación de tarifas | Fija tarifas y estándares de calidad para las empresas de servicios públicos |
| Regulatorias | Establece reglas y normas, determina infracciones y fija sanciones |

f) La demora injustificada en el cumplimiento de sus funciones y/o la inobservancia injustificada de los plazos legales correspondientes que traigan como consecuencia el retraso en el cumplimiento de los plazos legales y/o contractuales en la ejecución de obras bajo el ámbito de regulación del Organismo Regulador”.

12 Ruiz, G. (2020) “Luces y Sombras de la Regulación: las 10 medidas que marcaron la agenda durante el 2020”, Blog de la Maestría en Regulación de Servicios Públicos, <http://blog.pucp.edu.pe/blog/mregulacionsp/2020/12/23/luces-y-sombras-de-la-regulacion-las-10-medidas-que-marcaron-la-agenda-durante-el-2020/> (acceso el 21/04/2021).

| | |
|-----------------------------|--|
| Fiscalización | Califica infracciones e impone sanciones |
| Resolución de Controversias | Resuelve disputas en el sector telecomunicaciones. |
| Solución de reclamos | Actúa como segunda instancia en la solución de reclamos de usuarios. |
| Supervisión | Supervisa el cumplimiento de las normas aprobadas por el regulador. |

Fuente: OECD (2019, p. 65).

Durante los últimos años, OSIPTEL ha gozado de independencia para la definición de su agenda regulatoria y la aprobación de sus iniciativas. Si bien durante el proceso de desarrollo de sus regulaciones, los Ministerios pueden participar mediante la emisión de opiniones en el marco del proceso de consulta pública, en general, el regulador ha gozado de autonomía respecto de otras entidades del gobierno, en el diseño y aprobación de sus regulaciones.

Del mismo modo, existen un conjunto de iniciativas regulatorias lideradas por el MTC. En este aspecto, si bien OECD (2019, p. 20) reconoce que el nivel de comunicación entre el regulador y el MTC es fluido, también resalta el hecho de que las opiniones del regulador son no vinculantes y que en algunos casos, el Ministerio ha actuado de manera contraria a lo recomendado por OSIPTEL¹³.

Es importante mencionar sin embargo que a partir de 2016 con la aprobación del DL 1310 y el DL 1448 del año 2018, toda regulación que genere o modifique procedimientos administrativos debe pasar por una aprobación de la Secretaría de Gestión Pública de la PCM. Es importante mencionar además que la normativa de Análisis de Calidad Regulatoria (ACR), establece también la revisión periódica de estas regulaciones por parte de las entidades que las emitan. Si bien el ACR hasta la fecha no ha significado una restricción al nivel de autonomía del organismo regulador, podría potencialmente afectarla en casos de discrepancias entre la PCM y/o OSIPTEL respecto del ACR correspondiente a alguna regulación específica.

Por otro lado, debe mencionarse que recientemente mediante del Decreto Supremo N°063-2021-PCM el gobierno aprobó lineamientos generales para la aplicación del Análisis de Impacto Regulatorio (AIR) ex ante. En su Disposición Complementaria Final Séptima, esta norma establece que en el caso de los organismos reguladores se rigen supletoriamente por lo establecido en dichos lineamientos con la finalidad de mantener coherencia con el proceso integral del AIR Ex Ante y el ordenamiento jurídico. Asimismo, la norma establece que el Consejo Multisectorial de Calidad Regulatoria (CMCR) conformado por representantes de la PCM, el MEF y el Ministerio de Justicia, puede emitir recomendaciones con el fin de mantener coherencia con el ordenamiento jurídico. A diferencia del caso del ACR, la lectura de las normas vinculadas con el AIR mostraría que éstas así como las recomendaciones de la CMCR no serían vinculantes para el regulador. Por el contrario, el hecho de que la CMCR pueda emitir recomendaciones reflejaría la

13 OECD (2019, p. 20) "In general, communication between the regulator and the line ministry is constructive and fluid, and by law MTC can solicit technical support from the regulator. OSIPTEL does this regularly and informally before open consultations, relying on the regulator's high level of technical expertise and capacity. Both institutions can provide comments to the other's open consultations. However, OSIPTEL's technical opinions on Ministry consultations are non-binding in nature and in some instances the Ministry has acted contrary to the regulator's recommendations".

voluntad de que establecer una relación de carácter colaborativo entre esta y el regulador, a fin de que las normas que se aprueben guarden armonía con el ordenamiento jurídico.

Por último, debe mencionarse que durante los últimos años, se ha observado un activismo regulatorio creciente del Congreso de la República en temas relacionados con telecomunicaciones. Durante la legislatura 2016-2021, a la fecha de culminación del presente artículo¹⁴ se habían registrado 28 iniciativas legislativas en materia de telecomunicaciones. Algunas de ellas, ya se han materializado en normas aprobadas, como la ley que establece una velocidad mínima garantizada de 70%. Se ha observado que, en este como en otros casos, el poder legislativo no ha recogido los comentarios efectuados por el OSIPTEL, dando lugar a propuestas antitécnicas.

En virtud de lo anterior, se considera que en esta categoría correspondería un puntaje de 0.50.

2.3 AUTONOMÍA FRENTE A REGULADOS

Como se analizó en la sección precedente, otro frente importante que puede representar una amenaza a la autonomía del regulador es el relacionado con la influencia indebida o presión de actores que son sujetos de la regulación. Esta medición tiene la dificultad práctica de distinguir entre aquellas influencias provenientes de los regulados y que forman parte de la interacción regular y orgánica de los procesos regulatorios, de aquellas que pueden traspasar límites éticos o legales. En esta sección se ha procurado hacer dicha distinción, aunque ello no ha sido un ejercicio sencillo.

– Flujo de funcionarios hacia y desde regulador hacia a organizaciones (puerta giratoria).

En el caso de OSIPTEL, como del resto de la administración pública, actualmente rigen normas aplicables a funcionarios que dejan una institución pública, que les impiden ocupar cargos o prestar servicios a empresas o entidades reguladas en el ámbito específico de su función pública. Tal como lo reconoce OECD (2019, p. 99), la Ley 27588 establece prohibiciones e incompatibilidades para funcionarios o altos funcionarios que hayan tenido acceso a información privilegiada o hayan tenido injerencia en la toma de decisiones regulatoria; una vez que haya cesado su actividad en la organización pública. Estos impedimentos se extienden hasta un año posterior a la culminación de sus servicios en la organización pública. En el caso de OSIPTEL, los directores y altos funcionarios que dejan de laborar en la organización, se encuentran además impedidos de defender, asesorar o trabajar en alguna entidad que se encuentra dentro del ámbito de competencia del regulador, por el plazo de un año. A fin de implementar esta regla, las personas que dejan de laborar en OSIPTEL deben suscribir un documento de compromiso con dichas reglas. Finalmente, los miembros del Consejo Directivo deben suscribir anualmente una declaración de conflicto de interés.

Es importante acotar que esta regulación no impide que luego de transcurrido un año contado desde la salida del regulador, los profesionales que hayan dejado el OSIPTEL, puedan trabajar en empresas que se encuentren bajo el ámbito de competencia del regulador.

Por otro lado, si bien no existen impedimentos formales o normas que regulen la incorporación de personas que formen parte de entidades reguladas como funcionarios de OSIPTEL; en la práctica el flujo de profesionales desde empresas reguladas hacia el

14 Al 16/05/2021.

regulador ha sido poco frecuente, en especial, a nivel de funcionarios senior. Ello guarda especial relación con las condiciones económicas que ofrece el regulador comparadas con las que brinda la industria, aspecto que se analiza más adelante.

En virtud de lo anterior, consideramos que el nivel de autonomía correspondiente a este ítem debería ser 0.75.

– Frecuencia de contactos.

En esta categoría se busca determinar el tipo e intensidad de los contactos inter-personales entre los funcionarios del organismo regulador y ejecutivos de las entidades reguladas; bajo el supuesto de que cuanto más frecuente y cercano sea dicho contacto, mayor sería el riesgo de afectación de la autonomía. Este supuesto debe ser evaluado con cuidado, pues si bien es cierto que la existencia de diversos espacios y oportunidades de contacto entre funcionarios y ejecutivos podría incrementar la posibilidad de que se presenten escenarios de influencia indebida en las decisiones regulatorias; también es indudable que la existencia de instancias de comunicación e intercambio de información con estos y otros stakeholders relevantes, permite al regulador contar con insumos y elementos de juicio indispensables para el desarrollo de sus labores.

En este contexto, consideramos que la frecuencia de contactos que ha venido teniendo el OSIPTEL durante los últimos años, en términos generales, ha sido la necesaria para el desarrollo de sus labores. OECD (2019, p. 98) reconoce además la existencia de políticas de OSIPTEL vinculas a la transparencia e integridad de sus funcionarios (código de ética), así como sus lineamientos aplicables a situaciones de conflictos de interés.

Si bien no se aprecia que la frecuencia de contactos, en el caso de OSIPTEL, constituya un elemento que ponga en riesgo su autonomía resulta importante advertir la recomendación planteada por OECD (2019, p.19) en el sentido de que es necesario el diseño de una estrategia más proactiva de relacionamiento del regulador frente a los stakeholders a fin de poder comunicar los beneficios de una regulación independiente y mitigar lo que refieren como 'riesgos externos'¹⁵. Sobre el particular, en dicho documento, OECD plantea que una estrategia que contribuiría a reducir el riesgo de una afectación de su autonomía consistiría en establecer una comunicación más efectiva con sus stakeholders que permita a estos últimos entender la importancia de contar con un regulador independiente, valorando adecuadamente los costos de una potencial intervención 'política' sobre la institucionalidad regulatoria.

En tal sentido, consideramos que el puntaje que correspondería en este punto sería de 1.00.

– Presupuesto adecuado.

15 OECD (2019 p. 19) "A more proactive external relations strategy can help stakeholders understand the role and benefits of independent economic regulation and help tackle external risks. A robust external relations strategy, built around communicating the core contributions and impact of economic regulators on the economy, would provide a counterweight to the instability that is outside of the control of the regulatory authority. While independence is important, it does not mean that regulators act in isolation; on the contrary, such a strategy should aim for constructive engagement, setting up an on-going dialogue and building trust. The impact could be amplified by implementing such a strategy jointly, when relevant, with Peru's other economic regulators. It could contribute to the better understanding of the role of the regulator and the construction of a "no surprises" relationship with other branches of government and the regulated sector that could lay the foundation for addressing more structural shortcomings when the time is right."

En los acápite correspondientes a la influencia de los actores políticos sobre el presupuesto y organización interna del regulador se pudo apreciar que, pese a que se vienen asignando al regulador de manera creciente funciones adicionales a las establecidas en el marco de sus mandatos centrales, el volumen de recursos obtenido a través de la recaudación del aporte por regulación de OSIPTEL se ha estancado con una ligero aumento decretado recientemente (como se vió en secciones anteriores); lo cual ha obligado a recurrir a transferencias del gobierno central.

Al mismo tiempo, debe tenerse en cuenta que, desde diciembre de 2006, mediante Decreto de Urgencia N°038-2006 se estableció un tope a las remuneraciones de los funcionarios equivalente a 6 unidades de ingreso del sector público. Desde esa fecha, las remuneraciones de los cargos gerenciales del OSIPTEL no se han reajustado. Ello ha hecho que la brecha remunerativa entre regulador y sector privado durante los últimos años se haya venido ampliando de manera significativa. Es importante mencionar que actualmente, un incremento remunerativo de dichos funcionarios debería pasar por el cumplimiento de regulaciones tanto de SERVIR como del MEF. No obstante ello, en la actualidad, dicho incremento difícilmente sería sostenible en el mediano plazo con los recursos que el OSIPTEL viene recaudando. En virtud de lo anterior, consideramos que en este aspecto corresponde un puntaje de 0.25.

– Organización Interna Adecuada.

Con relación a este ítem, tal como se pudo apreciar cuando se analizó la influencia externa en la organización del regulador por parte del gobierno central; durante los últimos años, se aprecia una gradual reducción del tamaño de la organización, producto de las restricciones presupuestales que ésta ha venido enfrentando. En particular, en áreas sensibles, como la de atención de apelaciones por concepto de reclamos de usuarios, se ha venido un enfrentando un incremento significativo de la carga administrativa que ha obligado a OSIPTEL a desplegar esfuerzos dirigidos a dotar de mayores recursos a dichas áreas, así como a la digitalización de procesos. No obstante ello, existe el riesgo de que estos esfuerzos no sean suficientes, dada la tendencia de los ingresos que recibe el regulador. Igualmente, hemos apreciado que el personal dedicado a áreas "core" de la labor de OSIPTEL (supervisión y fiscalización, así como regulación) se han visto reducidas.

Esta tendencia puede poner en riesgo la capacidad supervisora y regulatoria del OSIPTEL, en un contexto en el cual, durante los últimos años, como se vio anteriormente, se le han venido agregando tareas y funciones adicionales a sus mandatos centrales. Teniendo en cuenta el crecimiento importante que viene experimentando el sector de las telecomunicaciones en el Perú, consideramos que en el caso de este ítem correspondería un valor de 0.5.

– Actividad Profesional del Presidente y Miembros del Consejo.

El cargo del Presidente del Consejo Directivo de OSIPTEL es a tiempo completo, cumpliendo labores de Presidente Ejecutivo, con funciones claramente especificadas en la normativa. Por su parte, el resto de miembros del Consejo Directivo tienen un régimen de tiempo parcial y participan a través de sesiones que pueden efectuarse regularmente con una frecuencia de dos a cuatro veces al mes (solo dos sesiones son remuneradas), dependiendo de las necesidades de la agenda. Según la OECD (2019, p. 86) esta estructura puede limitar la capacidad de los consejeros de examinar de manera completa y detallada todos los temas sometidos a decisión, en la medida que estos sean tópicos nuevos y complejos.

En cuanto a la ocupación de los profesionales que han desempeñado el cargo de Presidente, históricamente dos de ellos han sido abogados, dos ingenieros y uno economista. En cuanto al resto de miembros del Consejo Directivo también históricamente sus perfiles han correspondido a estas tres profesiones. Previamente, algunos han desempeñado labores en la academia mientras otros se desempeñan en sectores distintos al ámbito de competencia del OSIPTEL.

En términos generales, salvo por la observación puntual planteada por OECD (2019) con relación al régimen de los miembros de Consejo Directivo, en este aspecto, no se aprecian elementos que pudieran configurar un riesgo de afectación de la autonomía del regulador, razón por la cual, consideramos razonable asignar un puntaje a este punto de 0.75.

– Influencia externa en la regulación.

El informe de OECD (2019) no reporta riesgos de influencia indebida por parte de las entidades reguladas sobre las decisiones o medidas regulatorias de OSIPTEL. Tras revisar las prácticas del regulador con relación a los procesos de consulta, audiencias públicas, o solicitud de uso de la palabra al Consejo Directivo, entre otras; el informe presenta algunas oportunidades de mejora, entre las que destacan el fortalecimiento de la supervisión del cumplimiento del Código de Ética, mejorar el portal de transparencia institucional a fin de permitir brindar mayor información respecto de las reuniones sostenidas con entidades reguladas y brindar lineamientos y directivas al staff de OSIPTEL vinculadas al tratamiento de este tipo de reuniones a fin de promover un diálogo constructivo con la industria (OECD, pp. 38-39).

En tal sentido, se ha considerado razonable asignar en este acápite un puntaje de 0.75

3. RESULTADOS Y REFLEXIONES FINALES

La Tabla N°5 sintetiza los resultados de la evaluación de la autonomía de facto de OSIPTEL, detallada en la sección 3, mostrando un nivel de autonomía en la escala del 0 al 1 de 0.58. Estos resultados se explican por los siguientes factores:

- El nivel de autonomía de facto respecto de entidades reguladas, es relativamente alto (0.67) en contraste con el nivel de autonomía respecto de autoridades políticas, en particular del Poder Ejecutivo, ascendente a 0.50.
- En el caso de la autonomía respecto de las autoridades políticas, destacan de manera especial, los bajos valores registrados en las categorías relacionadas con influencia en la determinación del presupuesto y organización interna. Asimismo, se ha otorgado un puntaje bajo al factor vulnerabilidad política, vinculado a los precedentes recientes generados por “el caso OSINERGMIN”.

Tabla N°5. Cálculo de Autonomía *de facto* para OSIPTEL

| | Puntaje | Peso |
|-----------------------------------|----------------|-------------|
| A De autoridades políticas | 0.50 | 0.50 |
| 1 Frecuencia de puerta giratoria | 0.75 | |
| 2 Frecuencia de contactos | 0.75 | |
| 3 Influencia en presupuesto | 0.00 | |

| | | |
|----------|---|-------------|
| 4 | Influencia en organización interna | 0.25 |
| 5 | Influencia de partidos en nombramientos | 1.00 |
| 6 | Vulnerabilidad Política | 0.25 |
| 7 | Influencia externa sobre la regulación | 0.50 |
| B | De regulados | 0.67 |
| 8 | Frecuencia de puerta giratoria | 0.75 |
| 9 | Frecuencia de contactos | 1.00 |
| 10 | Presupuesto adecuado | 0.25 |
| 11 | Organización Interna Adecuada | 0.50 |
| 12 | Actividad Profesional del Presidente/Miembros del Consejo Directivo | 0.75 |
| 13 | Influencia externa sobre la regulación | 0.75 |
| | TOTAL | 0.58 |

- En el caso de la autonomía de facto frente a los regulados, si bien se han registrado niveles relativamente altos de autonomía asociados con influencia externa, frecuencia de contactos o puerta giratoria; constituye un motivo de preocupación la necesidad de dotar al regulador de un presupuesto adecuado y actualizar el nivel remunerativo de sus áreas gerenciales.

Estos resultados evidencian que los niveles de autonomía de facto con los que goza el regulador (0.58), son significativamente menores a los registrados en las estimaciones de la autonomía formal (0.66-0.67).

OSIPTEL históricamente ha sido considerada una isla de excelencia, generadora de conocimiento en materia de telecomunicaciones y una cantera de profesionales de primer nivel. En la medida que los aspectos presupuestales y organizacionales reseñados en este artículo se mantengan o profundicen, se corre el riesgo no sólo de debilitar la labor regulatoria del OSIPTEL, sino de generar una pérdida gradual del principal activo con que cuenta la organización: sus profesionales y técnicos.

REFERENCIAS BIBLIOGRÁFICAS

- Feinstein B. y Hemel D. (2018). "Partisan Balance with Bite", *Columbia Law Review*, Vol. 118, N°1.
- Gilardi F. (2002). "Policy Credibility and Delegation to Independent Regulatory Agencies: A comparative empirical analysis", *Journal of European Public Policy*, 9:6 December, pp 873–893.
- Gilardi, F. y M. Maggetti (2010). "The Independence of regulatory authorities", en Levi-Faur, David Eds., *Handbook of Regulation*, Cheltenham, Edward Elgar
- Levy, B. y P. Spiller (1994). "The Institutional Foundations of Regulatory Commitment: A Comparative Analysis of Telecommunications Regulation", *Journal of Law, Economics and Organization*, 10(2), pp. 201-246.
- Levi-Faur D. y Jordana J. (2005). "¿Hacia un Estado Regulador latinoamericano? La

- difusión de agencias reguladoras por países y sectores" Documentos CIDOB América Latina, N°7.
- Maggetti M. (2007). "De facto independence after delegation: A fuzzy-set analysis" *Regulation & Governance* (2007) 1, 271-294.
- Perez-Reyes R. (2011). "La Autonomía de los Organismos Reguladores", *Revista de Derecho Administrativo*, Num. 10, Tomo 1, 129-136.
- Quintanilla E. (2004). "Autonomía Institucional de los Organismos Reguladores", Documento de Trabajo N°14, ESAN, Noviembre.
- Ruiz, G. (2020). "Luces y Sombras de la Regulación: las 10 medidas que marcaron la agenda durante el 2020", Blog de la Maestría en Regulación de Servicios Públicos, <http://blog.pucp.edu.pe/blog/mregulacionsp/2020/12/23/luces-y-sombras-de-la-regulacion-las-10-medidas-que-marcaron-la-agenda-durante-el-2020/> (acceso el 21/04/2021).
- Ruiz, G. y Granda A. (2015). "Una Estimación de la Autonomía Formal del Regulador de las Telecomunicaciones en el Perú", *Derechos & Sociedad*, 45, Octubre, pp. 211-226.
- Stigler, G. (1971). "The Theory of Economic Regulation", *Bell Journal of Economics and Management Science* 2, N°1, Spring, pp. 1-21.
- Stiglitz, J. (1989). "Markets, Market Failures and Development", *American Economic Review*, Vol. 79, N°2, May, pp. 197-203.
- Tirole J. y Laffont J. (1993). "A Theory of Incentives in Procurement and Regulation", The MIT Press.
- Peltzman S. (1976). "Toward a More General Theory of Regulation", *Journal of Law and Economics* 19, N°2, August, pp. 211-240.
- OECD. (2019). *Driving Performance at Peru's Telecommunications Regulator, The Governance of Regulators*, OECD Publishing, Paris. <https://doi.org/10.1787/9789264310506-en>
- OECD. (2016). "The Governance of Regulators. Being an Independent Regulator", OECD Publishing, Paris. <http://dx.doi.org/10.1787/9789264255401-en>.
- UIT. (2016). "Medición de la Independencia Formal de las Autoridades Regulatorias en Telecomunicaciones utilizando una adaptación del Índice de Gilardi", Oficina Regional de UIT. Oficina de Desarrollo de las Telecomunicaciones.

APÉNDICE 1

PROYECTOS DE LEY SOBRE TELECOMUNICACIONES PROPUESTOS DURANTE LA LEGISLATURA 2016–2021 AL 16/05/21

| NUMERO | FECHA | ESTADO | TITULO |
|---------------|------------|--------------------------------|--|
| 07484/2020-CR | 8/04/2021 | En comisión | Ley para la Inclusión Digital de Estudiantes de Pobreza y Extrema Pobreza con Participación del Sector Privado "Willay Perú". |
| 07222/2020-CR | 26/02/2021 | En comisión | Ley que regula el uso de Medios Tecnológicos en Telecomunicación como las Redes Sociales Aplicaciones |
| 07132/2020-CR | 15/02/2021 | En comisión | Ley para la Promoción de la Conectividad y la Calidad de Servicios Públicos de Telecomunicaciones |
| 06883/2020-CR | 29/12/2020 | En comisión | Ley que Modifica la Ley 27037 sobre Promoción de la Inversión en la Amazonía, que incorporando una Décima Disposición Complementaria, que exonera temporalmente el pago del IGV sobre los servicios de energía eléctrica y telecomunicaciones, por el Covid-19 |
| 06757/2020-CR | 9/12/2020 | En comisión | Ley que modifica la Ley 29022, Ley para el Fortalecimiento de la Expansión de Infraestructura en Telecomunicaciones a fin de Promover la Inversión Privada Regulada y Sostenible. |
| 06106/2020-CR | 1/09/2020 | En comisión | Ley que incorpora los Servicios Públicos de Electricidad, Telecomunicaciones e Internet en los Alcances de la Ley 27037, la Ley de Promoción de la Inversión en la Amazonía. |
| 05772/2020-CR | 13/07/2020 | Dictamen | Ley que Acumula Megas de Internet que no se utilizan dentro del Plan Mensual. |
| 05757/2020-CR | 13/07/2020 | Dispensado 2da. Votación | Ley contra la Violación de Derechos del Consumidor de Servicios de Telefónica Cable e Internet. |

| | | | |
|---------------|------------|--------------------------------|--|
| 05713/2020-CR | 7/07/2020 | En comisión | Ley que establece la Moratoria en el Sistema Financiero, seguros y Servicios Básicos durante la Declaratoria de Estado de Emergencia. |
| 05582/2020-CR | 23/06/2020 | Orden del Día | Ley que Promueve la Expansión de la Infraestructura en Telecomunicaciones. |
| 05488/2020-CR | 11/06/2020 | En comisión | Ley que suspende el Cobro de los Servicios Públicos de Energía Eléctrica, Agua y Alcantarillado, Gas Natural domiciliario, Telecomunicaciones e Internet durante la Declaración de Estado de Emergencia Nacional. |
| 05091/2020-CR | 28/04/2020 | Dispensado 2da. Votación | Ley que modifica los artículos 2, 3 y 4 del Decreto Legislativo N°1182, que regula el uso de los datos derivados de las Telecomunicaciones para la Identificación, Localización y Geolocalización de Equipos de Comunicación, en la lucha contra la Delincuencia y el Crimen Organizado. |
| 04866/2020-CR | 24/03/2020 | Publicado El Peruano | Ley que establece la Moratoria en el Sistema Financiero, seguros y Servicios Básicos durante la Declaratoria de Estado de Emergencia. |
| 04843/2019-CR | 24/09/2019 | Dictamen | Ley que Modifica los Artículos 5 y 6 de la Ley 29022, Ley para el Fortalecimiento de la Expansión de Infraestructura en Telecomunicaciones. |
| 04526/2018-CR | 5/07/2019 | En comisión | Ley de Telecomunicaciones. |
| 04333/2018-CR | 15/05/2019 | En comisión | Ley de Telecomunicaciones y Tecnologías de la Información y Comunicación. |
| 04305/2018-CR | 9/05/2019 | Dictamen | Ley que modifica la Ley 29022, Ley para el Fortalecimiento de la Expansión de Infraestructura en Telecomunicaciones a fin de Promover la Inversión Privada Regulada y Sostenible. |

| | | | |
|---------------|------------|----------------------|--|
| 04102/2018-CR | 22/03/2019 | En comisión | Ley que Modifica la Ley 27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones-OSIPTEL. |
| 04048/2018-CR | 15/03/2019 | Dictamen | Ley que Modifica el Artículo 114 del Decreto Ley 25844, Ley de Concesiones Eléctricas, a fin de regular la instalación de Cableado de los Servicios Eléctricos y Telecomunicaciones. |
| 03057/2017-CR | 19/06/2018 | Dictamen | Ley que delimita el Derecho de Servidumbre y de las Instalaciones realizadas por las Empresas Concesionarias de los Servicios Eléctricos y de Telecomunicaciones. |
| 02962/2017-CR | 5/06/2018 | En comisión | Ley que modifica el Primer Párrafo, Numeral 4 del Artículo 230 del Código Procesal Penal, referido a la Intervención de Comunicaciones y Telecomunicaciones. |
| 02502/2017-CR | 6/03/2018 | Orden del Día | Ley de Acumulación Justa de Minutos y Megas. |
| 01400/2016-CR | 16/05/2017 | En comisión | Ley de Uso Compartido de Infraestructura en Telecomunicaciones. |
| 01210/2016-CR | 11/04/2017 | Publicado El Peruano | Ley de Facilitación de Inversiones en las Zonas Especiales de Desarrollo. |
| 00738/2016-CR | 6/12/2016 | En comisión | Ley que faculta al OSIPTEL a supervisar la calidad del Servicio de Comunicaciones Postales y a Resolver las Controversias que se susciten entre los concesionarios de los servicios de comunicaciones postales y los usuarios, en segunda instancia. |
| 00579/2016-CR | 8/11/2016 | Orden del Día | Ley que Promueve la Expansión de la Infraestructura en Telecomunicaciones. |
| 00317/2016-CR | 27/09/2016 | Orden del Día | Ley que establece disposición complementaria a la Ley 29022, Ley para el Fortalecimiento de la Expansión de Infraestructura en Telecomunicaciones. |

Fuente: Congreso de la República



EL USO DE HERRAMIENTAS TECNOLÓGICAS EN LA LUCHA CONTRA EL COVID-19 Y SUS IMPLICANCIAS EN EL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES: UNA APROXIMACIÓN

THE USE OF TECHNOLOGICAL TOOLS IN THE FIGHT AGAINST COVID-19 AND ITS IMPLICATIONS ON THE FUNDAMENTAL RIGHT TO THE PROTECTION OF PERSONAL DATA: AN APPROXIMATION

DIEGO ZEGARRA VALDIVIA¹

RESUMEN

El presente trabajo analiza algunos de los supuestos en que el uso variado de tecnologías para hacer frente a la propagación de la pandemia del COVID-19 y proteger la salud de las personas ha impactado en el derecho fundamental a la protección de datos personales; para ello, parte de la premisa de que la utilización de estas tecnologías no puede significar una afectación al referido derecho fundamental ni mucho menos un tratamiento indiscriminado de dichos datos sin control mínimo alguno.

PALABRAS CLAVE

Derecho Fundamental | Protección de datos personales | Pandemia | COVID-19 | Consentimiento | Salud Pública | Tecnología

CONTENIDO

1. Introducción. **2.** Las bases de legitimación del tratamiento de datos de salud. **2.1.** El consentimiento. **2.2.** Finalidad, proporcionalidad y minimización de datos. **2.3.** Seguridad. **2.4.** Calidad o almacenamiento por tiempo limitado. **3.** El uso de herramientas tecnológicas sustentadas en el tratamiento de datos personales para luchar contra la pandemia del COVID-19. **3.1.** Principales riesgos que se generan cuando se emplean herramientas tecnológicas que tratan datos personales. **3.2.** Ámbitos en los que se han

ABSTRACT

This paper analyzes some of the cases in which the varied use of technologies to cope with the spread of the COVID-19 pandemic and protect people's health has impacted on the fundamental right to the protection of personal data; to this end, it starts from the premise that the use of these technologies cannot affect that fundamental right, much less an indiscriminate processing of said data without any minimum control.

KEYWORDS

Fundamental Right | Protection of personal data | Pandemic | COVID-19 | Consent | Public Health | Technology

¹ Profesor Principal de Derecho Administrativo. Doctor en Derecho por la Universidad de Alicante, Master en Derecho de las Telecomunicaciones y de las Tecnologías de la Información por la Universidad Carlos III de Madrid, Director de la Maestría en Derecho Administrativo y del Programa de Segunda Especialidad en Derecho Administrativo en la Pontificia Universidad Católica del Perú. Jefe de la Oficina Académica de Internacionalización y Coordinador del Área de Derecho Administrativo en la Facultad de Derecho en la Pontificia Universidad Católica del Perú.

La presente investigación se enmarca dentro de las actividades de la Línea de Investigación de Protección de Datos Personales y Transparencia del Grupo de Investigación en Derecho Administrativo GIDA y su elaboración contó con la colaboración de Camila Chinchay, Ángela Casafranca, Christian Hernández, Alexandra Olivera, Piero Curi y Camila Atencio.

implementado herramientas tecnológicas: identificación de algunos riesgos y de posibles afectaciones al derecho fundamental a la protección de datos personales. **4.** A modo de conclusión.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 8 de agosto de 2021 y aprobado para su publicación el 27 de octubre de 2021.

1. INTRODUCCIÓN

La pandemia del COVID-19 ha generado que en casi todos los países a nivel mundial adopten, de forma progresiva, diversos tipos de medidas con la finalidad de contener su propagación, proteger la salud pública y la vida de las personas (Gómez-Córdoba et al., 2020, p. 273). Entre dichas medidas, se identifican el aislamiento social obligatorio, el distanciamiento social, el control del aforo, el uso de herramientas tecnológicas para el procesamiento de datos y mitigación de contagios, el establecimiento de canales informativos sobre el COVID-19, la geolocalización de contagiados, los estudios de movilidad, rastreo y registro de contactos, control y medición de la temperatura corporal, entre otros.

Todas estas acciones de una u otra forma han limitado derechos y libertades fundamentales como la privacidad, la protección de datos personales, la libre circulación, la libertad de expresión, la libertad de reunión, entre otros derechos. De los mencionados, importa para los efectos del presente trabajo el derecho fundamental a la protección de datos personales, debido al tipo de información recogida y requerida para la implementación de los sistemas de vigilancia epidemiológica y de control de la propagación de la enfermedad (Gómez-Córdoba et al., 2020, p. 273).

En efecto, las medidas para mitigar el COVID-19 implican necesariamente el procesamiento de diferentes datos personales, con lo cual se debe garantizar un tratamiento adecuado y legal de los mismos. Si bien la gravedad de la actual crisis de salud permite el uso de poderes de emergencia en respuesta a amenazas importantes – como ha sido señalado por un grupo de expertos en derechos humanos de las Naciones Unidas el 16 de marzo de 2020 -, es indispensable que la respuesta a ser implementada por los Estados frente al COVID-19 sea proporcionada, necesaria y no discriminatoria (ONU, 2020).

Debe repararse entonces, que, en ninguna circunstancia, la declaración de emergencia sanitaria asumida globalmente por los países supone, ni expresa ni tácitamente la suspensión del derecho fundamental a la protección de datos personales, tan sólo implica adoptar determinadas medidas que traen consigo la limitación y no la suspensión en el ejercicio de derechos y libertades (Piñar, 2020). Sin embargo, como sostiene Arenas (2020), lo importante, es que las referidas limitaciones deben cumplir con una serie de requisitos y ofrecer una serie de garantías y responsabilidades en caso de incumplimiento: ser necesarias, apropiadas y proporcionales en una sociedad democrática (p. 10).

Cuestión distinta es que sea necesario adaptar este derecho fundamental para, conforme lo ha expresado la Agencia Española de Protección de Datos (en adelante, AEPD), “(...) permitir legítimamente los tratamientos de datos personales en situaciones, como la presente, en que existe emergencia sanitaria de alcance general” (2020, p.1). Esto último ha sido reiterado por el Comité Europeo de Protección de Datos Personales, al haber puesto énfasis en que el respeto a la privacidad de los individuos no constituye un escollo en la toma de decisiones que impliquen contener la pandemia actual, cuando se esté

hablando de datos sensibles como son los relativos a la salud de las personas (EDPB, 2020, p. 1).

En los meses en que lleva esta pandemia, han surgido voces para expresar si “la privacidad será una de las víctimas de la COVID-19” (Renda, 2020), se han acuñado expresiones como “a la muerte por protección de datos” (Martínez, 2020) o planteamientos respecto a si las concesiones y restricciones en materia de vigilancia, tracing, tracking y seguridad de la ciudadanía pudieran llegar a ser permanentes (Calzada citado por Recuero Linares, 2020, p. 141), lo que hace manifiesta la incertidumbre respecto a las garantías que los ordenamientos jurídicos han establecido para el ejercicio de este derecho fundamental y de los derechos vinculados al mismo. Es por ello que autores como Andreu (2020) consideran problemática la aplicación de la normativa “en el uso de soluciones tecnológicas para la lucha contra la pandemia, lo que ha llevado a declaraciones restrictivas sobre su uso y a una gran confusión sobre su eficacia y seguridad” (p. 851).

En efecto, estas innovaciones han generado nuevas preocupaciones a nivel mundial sobre el uso inadecuado de determinados aplicativos que afectan el derecho fundamental a la protección de datos personales y la privacidad de los ciudadanos, lo que ha supuesto una tensión entre el derecho a la salud colectiva y los derechos individuales. Y es que, lamentablemente,

Estas estrategias no siempre se contextualizan dentro de un régimen de protección de datos personales robusto, ni de instrumentos jurídicos que garanticen que en su desarrollo e implementación se protejan los derechos de las personas, se obtengan únicamente datos realmente necesarios, se evalúe el impacto en la salud humana que justifique las restricciones de libertades, o se garantice que la información obtenida no será empleada a largo plazo con otros fines estatales o privados (Gómez-Córdoba et al., 2020, pp. 274-275).

Es por estas consideraciones que el presente trabajo tiene como finalidad analizar que, si bien el contexto del COVID-19 requiere de medidas rápidas para hacer frente a su expansión y mitigar sus impactos, contando para ello con la tecnología como un medio idóneo y necesario para dicha finalidad accediendo a datos sensibles como la salud de las personas o datos personales y su geolocalización, existe una gran preocupación por el tratamiento y uso adecuado de estos datos personales recopilados en estas circunstancias debido a que el uso de estas tecnologías no puede significar una afectación del derecho fundamental a la protección de los datos personales ni mucho menos un tratamiento indiscriminado de dichos datos sin control mínimo alguno.

El tratamiento de datos personales en estas situaciones de emergencia sanitaria sigue realizándose de conformidad con la normativa de protección de datos personales, por lo que se aplican todos sus principios entre ellos el tratamiento de los datos personales con licitud, lealtad y transparencia, de limitación de la finalidad, principio de exactitud y minimización de datos (AEPD, 2020, pp. 6-7). Por ello, sin llegar al exceso alarmista de las citadas expresiones, bajo la premisa que los ordenamientos jurídicos legitiman los tratamientos de datos personales que sean imprescindibles para luchar contra la pandemia global del COVID-19, en el presente artículo se identifican los posibles riesgos y afectaciones al derecho fundamental a la protección de datos personales derivados de la implementación por parte de los Estados y los particulares de herramientas tecnológicas con motivo de controlar la propagación del virus, proteger la salud pública y la vida de las personas, y se formulan algunas reflexiones sobre el alcance de los mismos en la garantía del referido derecho fundamental.

2. LAS BASES DE LEGITIMACIÓN DEL TRATAMIENTO DE DATOS DE SALUD

La protección de datos personales es un derecho fundamental reconocido en diversos textos internacionales, en la legislación comparada, así como en el ordenamiento jurídico peruano. A nivel internacional, como señala Razquin, la protección de datos personales está prevista en:

El art. 12 de la Declaración Universal de Derechos Humanos de 1948 y el art. 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966, que se refieren a la protección de la vida privada y de la intimidad. También en el ámbito del Consejo de Europa, el art. 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950 establece el principio de protección de la intimidad; el Convenio nº 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981 garantiza la protección de datos frente al tratamiento automatizado; y asimismo el Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos de 2009 recoge como uno de los límites del derecho de acceso a los documentos el de la protección de la intimidad (artículo 3.1.f). Los Tratados de la Unión Europea amparan asimismo la protección de los datos personales (art. 16 TFUE y art. 39 TUE). Y la Carta de los Derechos Fundamentales de la Unión Europea regula el derecho a la protección de datos de carácter personal (art. 8). (2019, p. 142).

Asimismo, a nivel europeo, en el 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), se encuentra regulado el tratamiento de los datos personales y la libre circulación de estos datos en una realidad asociada a la nueva sociedad digital, habiendo recogido para ello en su artículo 5 los principios básicos que deben regirlos, como son la licitud (cuyo alcance ha sido desarrollado en el artículo 6 del RGPD), lealtad y transparencia; limitación de la finalidad; minimización de datos; exactitud; limitación del plazo de conservación; e, integridad y confidencialidad.

Por su parte, en el ordenamiento jurídico peruano, el reconocimiento de la protección de datos personales como derecho fundamental ha sido recogida en el artículo 2, inciso 6 de la Constitución Política del Perú, al estipularse el derecho de toda persona a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

El desarrollo normativo del citado precepto constitucional ha sido realizado en la Ley No. 29733 – Ley de Protección de Datos Personales (en adelante, LPDP), promulgada en el año 2011 y en plena vigencia desde el año 2013, y en su Reglamento aprobado por Decreto Supremo No. 003-2013-JUS (en adelante, RLPDP). A través de esta regulación se busca garantizar el derecho fundamental de los titulares de los datos personales, es decir, la capacidad de los mismos de controlar su tratamiento en el ámbito de Administración Pública como aquel que se da en el sector privado.

Durante esta pandemia es constante la recopilación y tratamiento de datos personales relativos a la salud, los mismos que son considerados como una categoría especial en la normativa de protección de datos personales cuya característica principal es el carácter sensible de mismos. Se trata de datos cuyo tratamiento puede suponer mayor riesgo de vulneración de los derechos y libertades del interesado y por ello son merecedores de

especial protección porque pueden afectar de manera significativa al individuo.

Los datos de salud consisten en aquellas informaciones “que se refieren a la salud pasada, presente o futura en personas sanas o enfermas, con enfermedades de carácter físico o psicológico, y que incluye la adicción al alcohol y a las drogas” (Cristea, 2018, p. 46). Los datos personales referidos a la salud, contienen, como señala Cristea, información de las personas que hace posible conocer las dolencias o enfermedades que han padecido, padecen o incluso podrán padecer (2018, p. 46). Solernou refiere además que el Grupo Europeo de Ética en la Ciencia y en las Nuevas Tecnologías considera que el dato personal de salud incluye la información relativa no sólo a las enfermedades, sino también a las intervenciones, medicamentos prescritos, diagnósticos, etc.; así como los datos administrativos sanitarios referidos al registro, y a las admisiones, a los seguros, etc. (2006, pp. 51-52).

Se trata, en definitiva, de datos personales que forman parte de la esfera más íntima de la persona, que pueden estar revelando situaciones críticas relativas a determinadas enfermedades, a la aplicación de técnicas de reproducción asistida o relativa a información genética, cuyo potencial vulnerador de la intimidad personal nadie se atreve a poner en duda (Piñar, citado por Cristea, 2018, p. 46).

Es por el alcance que tiene la definición de los datos de salud que resulta indispensable analizar el marco de garantías de los principios de legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad, disposición del recurso, y, nivel de protección adecuado, recogidos en la LPDP (Título I) y en el RLPDP (Título II) ya que delimitan el tratamiento de datos personales, tienen fuerza vinculante, aplicación práctica y definen si un tratamiento de datos se está o no realizando de manera leal, lícita, transparente y adecuada. No obstante, en la situación de emergencia sanitaria, los citados principios recogidos en la legislación peruana, al que es razonable sumarle - por su vinculación - los que han sido recogidos en el RGPD europeo, son de difícil cumplimiento para el tratamiento de datos de salud un entorno digital. Por ello,

Existe una improrrogable necesidad de clarificar y precisar la aplicación de los principios de la protección de datos a las nuevas tecnologías, con el fin de garantizar una protección real y efectiva de los datos personales, cualquiera que sea la tecnología utilizada para tratar estos datos, y que los responsables del tratamiento de los datos tengan plena conciencia de las implicaciones de las nuevas tecnologías en la protección de datos personales (Cristea, 2018, p. 224).

Resulta entonces necesario identificar el alcance de los citados principios y los efectos derivados de la implementación de herramientas tecnológicas que involucran el tratamiento de datos de salud en el entendido de que se trata de una serie de reglas materiales concebidas para desarrollar y asegurar la consecución de los fines de la normativa de protección de datos personales.

2.1 EL CONSENTIMIENTO EN EL TRATAMIENTO DE DATOS DE SALUD

El principio de consentimiento implica que terceros podrán acceder a datos personales, siempre que exista consentimiento libre, expreso, inequívoco e informado por parte del titular. Este principio se encuentra recogido en el artículo 5² de la LPDP y los artículos 7, 11, 12 y 14 del RLPDP.

² Ley N° 29733, Ley de Protección de Datos Personales

“Artículo 5. Principio de consentimiento

En concordancia con lo regulado en la LPDP, en el artículo 7³ del RLPD, dispone que el consentimiento del interesado implica toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen. De esta forma, como sostiene Arias (2016. p. 122), el consentimiento tiene una forma propia de otorgarse:

- Mediante un acto afirmativo claro que refleja una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen. Puede ser una declaración por escrito, inclusive por medios electrónicos o una declaración verbal, si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar y necesariamente el uso del servicio para el que se presta;
- Para todas las actividades de tratamientos realizados con el mismo o los mismos fines, es decir, cuando el tratamiento tenga varios fines, debe darse el consentimiento para cada uno de ellos;
- Mediante un medio que permita al responsable del tratamiento ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento.

Asimismo, la LPDP ha previsto en el artículo 14⁴ los supuestos en que es legítimo el tratamiento de los datos personales prescindiendo del consentimiento. Así, en el inciso 6 del citado artículo se dispone que no se requiere el consentimiento del titular de los datos personales, para los efectos de su tratamiento, “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”.

Para el tratamiento de los datos personales debe mediar el consentimiento de su titular”.

3 Decreto Supremo No. 003-2013-JUS, Reglamento de la Ley 29733

“Artículo 7.- Principio de consentimiento.

En atención al principio de consentimiento, el tratamiento de los datos personales es lícito cuando el titular del dato personal hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco. No se admiten fórmulas de consentimiento en las que éste no sea expresado de forma directa, como aquellas en las que se requiere presumir, o asumir la existencia de una voluntad que no ha sido expresa. Incluso el consentimiento prestado con otras declaraciones, deberá manifestarse en forma expresa y clara”.

4 Ley N° 29733, Ley de Protección de Datos Personales

“Artículo 14. Limitaciones al consentimiento para el tratamiento de datos personales

No se requiere el consentimiento del titular de datos personales, para los efectos de su tratamiento, en los siguientes casos:

(...)

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.

(...)”.

El alcance de esta norma ha sido explicado en la Opinión Consultiva N° 07-2019-JUS/DGTAIPD-DPDP de la Autoridad Nacional de Protección de Datos Personales, según la cual, la excepción que regula el inciso 6 del artículo 14 de la Ley de Protección de Datos Personales “refiere a situaciones específicas que implican una circunstancia de riesgo, como por ejemplo una epidemia, en la que se pone en peligro la vida o salud del titular del dato personal y de personas cercanas a él” (2019). De esta forma, cuando median razones de interés público o salud pública declaradas, como la Emergencia Sanitaria vigente en el Perú, se permite el tratamiento de datos personales sin que requiera para ello el consentimiento del titular de los datos personales con el objetivo de adoptar medidas de prevención frente a posibles contagios. Similar disposición ha sido prevista en el literal i del artículo 9⁵ del RGPD europeo: “*sensitive data may be processed for reasons of public interest in the area of public health, such as protecting against threats to public health or ensuring medical device quality*” (Scheibner et al., 2020, p. 12).

Entonces, ante la necesidad de contar con información para el manejo adecuado de la pandemia, es admisible el tratamiento de datos personales de carácter general y aquellos que son relativos a la salud sin el consentimiento de los titulares. Sin embargo, este tratamiento debe ser justificado, necesario proporcional, razonable y eficaz como medida para contener la propagación, y se debe garantizar la seguridad en el tratamiento de los datos.

No debe perderse de vista además que es legítimo el tratamiento de datos de salud para la prevención o el diagnóstico médico, para la prestación de asistencia sanitaria y para la gestión de servicios sanitarios, siempre y cuando el tratamiento se realice por personas sujetas al deber de secreto (Solernou, 2006, p. 56). “Este tratamiento incluye la recogida, el almacenamiento y la comunicación de los datos y será legítimo siempre y cuando persiga el cumplimiento de estos fines y lo lleven a cabo personas sujetas al secreto profesional” (Solernou, 2006, p. 56).

Con relación a las iniciativas que desde los Estados y el sector privado han supuesto la implementación de soluciones técnicas y aplicaciones móviles para la recopilación de datos de salud con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como para conseguir la mejor atención y la accesibilidad por parte de los ciudadanos, no se encuentran dentro de la excepción antes señalada ya que estamos frente a funcionalidades que se ponen a disposición de los ciudadanos y su uso es voluntario y requieren consentimiento expreso.

El uso de aplicaciones (“app”) que le permitan al titular de los datos personales la autoevaluación en base a los síntomas médicos que comunique, de la probabilidad que esté infectado de COVID-19, de recibir información, consejos y recomendaciones, o de

5 Reglamento (UE) 2016/679

“Artículo 9. Tratamiento de categorías especiales de datos personales

(...)

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

(...)

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del derecho de la Unión o de los Estados miembros que establezcan medidas adecuadas y específicas para proteger los derechos y libertades del interesado en particular el secreto profesional.

(...)”.

posibilitarle la geolocalización para verificar que se encuentra donde declara estar, debe ser enteramente voluntario, de manera que toda aquella persona que quiera someterse a ellas tendrá que prestar su consentimiento expreso, donde el responsable de tratamiento será la autoridad sanitaria estatal o la empresa privada que ponga a disposición la misma (Rodríguez, 2020, p. 143).

2.2 FINALIDAD, PROPORCIONALIDAD Y MINIMIZACIÓN DE DATOS

El tratamiento de los datos de salud que sean recopilados debe estar exclusivamente limitados a la finalidad pretendida, sin que pueda extender dicho tratamiento a cualesquiera otros datos personales no estrictamente necesarios para dicha finalidad, o que pueda confundirse conveniencia con necesidad, porque el derecho fundamental a la protección de datos debe seguir aplicándose sin perjuicio de las situaciones de emergencia establecidas en la normativa para la protección de intereses esenciales de salud pública (Piñar, 2020).

De acuerdo con esto último, la recopilación de datos personales debe ser mínima para el logro de objetivos de salud pública, estando ello acorde con el principio de proporcionalidad, cuya finalidad es “evitar que se recopilen información que no es razonablemente pertinente para cumplir la finalidad del tratamiento, lo que supone una limitación para cualquier forma de recopilación que no esté justificada” (Zegarra 2014, p. 631).

La garantía de que en el tratamiento de datos personales sea determinado, explícito, lícito y que el mismo no será incompatible para los fines para los que fueron recopilados; así como lo referido a que el tratamiento de los datos personales sea adecuado, relevante y no excesivo, todo ello con el propósito de lograr que las medidas de prevención en salud sean eficaces; se encuentran regulados en los artículos 6⁶ y 7⁷ de la LPDP, respectivamente. De acuerdo con las citadas normas, es necesario que se verifique el cumplimiento de la finalidad y la pertinencia de los datos personales solicitados con la normativa que las autoridades de salud han aprobado cuya finalidad es hacer frente al COVID-19 y disminuir su propagación.

Vinculado con el principio de proporcionalidad de la normativa peruana, se encuentra el principio de minimización de datos, recogido en el artículo 5⁸ de la RGPD europeo, de acuerdo con el cual sólo pueden recopilarse datos personales estrictamente necesarios

6 Ley N° 29733, Ley de Protección de Datos Personales

“Artículo 6. Principio 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.”

7 Ley N° 29733, Ley de Protección de Datos Personales

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.”

8 Reglamento (UE) 2016/679

“Artículo 5. Principios relativos al tratamiento

1. Los datos personales serán:

(...)

para el tratamiento y en la oportunidad que vayan a ser tratados no para usarlos tiempo después; asimismo, la solicitud de datos personales a sus titulares debe encontrarse plenamente justificada, en función a la finalidad que se persigue por dicho tratamiento (Puyol, 2017, p. 138).

Ante los nuevos desafíos en tiempos de pandemia, se deben reinterpretar los principios que sustentan el tratamiento de datos personales de manera que pueda contarse con un marco normativo que ofrezca seguridad jurídica, proteja los derechos de las personas y genere confianza en la sociedad (Gómez-Córdova et al., 2020, p. 285). Así, por ejemplo, el principio de finalidad del tratamiento de datos personales está vinculado con las recomendaciones éticas de la OMS en la pandemia de COVID-19 referidas a (i) la restricción de su uso; (ii) la proporcionalidad en la recolección de datos; y, (iii) la recolección mínima de datos para el logro de objetivos de salud pública (Gómez-Córdova et al., 2020, p. 286).

Es necesario reparar en que se tiende a recoger muchos datos de salud y en ello contribuye el uso de tecnologías de la información, afectando por tanto la eficacia de la prestación sanitaria (Souleron, 2006, p. 57). "El sistema debe asegurar que el personal sanitario dispone de información necesaria y relevante cuando ejerce sus funciones y eso implica decidir y, si cabe, cuestionar qué datos se introducen en el sistema y de qué forma". (Souleron, 2006, p. 57).

De lo expresado, resulta claro que, si bien estas consideraciones son previas a la emergencia sanitaria generada por el COVID-19, apuntan a advertir que el uso de tecnologías de la información en el tratamiento de datos de salud puede derivar en la inobservancia de los principios de finalidad, proporcionalidad y minimización de datos, lo que tiene un impacto significativo en caso se produzca el acceso a datos personales por terceros no autorizados, debido a que el mismo puede derivar en un tratamiento destinado a usos no autorizados o a tratamientos que limiten el ejercicio de los derechos del titular de los datos personales, de ahí la importancia de establecer mecanismos que garanticen el cumplimiento de los citados principios.

2.3 SEGURIDAD

El principio de seguridad implica que cualquier mecanismo de tratamiento de datos personales que se adopte debe garantizar la seguridad de los datos personales que eviten cualquier pérdida, desviación o adulteración de los datos personales obtenidos. En el caso específico de los datos de salud, las medidas de seguridad que se implementen son de nivel alto, atendiendo a la naturaleza de los referidos datos y en función a la mayor necesidad de garantizar la confidencialidad y la integridad de dicha información cuando es tratada (Cristea, 2018, p. 108).

La normativa peruana ha recogido dichos términos. Así, de conformidad con el artículo

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados ("minimización de datos").

(...)"

9º de la LPDP y el artículo 10¹⁰ del RLPD, el principio de seguridad garantiza que el titular del banco de datos personales y el encargado de su tratamiento deben adoptar medidas técnicas, organizativas y legales necesarias para salvaguardar la seguridad de los datos personales, evitando cualquier tratamiento contrario a la Ley o al Reglamento, incluyéndose la adulteración, pérdida, desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Por su parte, el artículo 4.12¹¹ del RGPD europeo establece que la violación de la seguridad de los datos personales implica toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Asimismo, el artículo 5¹² del RGPD garantiza la seguridad adecuada de los datos personales, lo cual implica la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (“integridad y confidencialidad”).

La garantía del principio de seguridad está directamente vinculada con el derecho a la confidencialidad de los datos personales. Sin embargo, al disponerse de medidas cuyo objetivo sea garantizar el derecho a la salud y que hagan posible que el suministro de la información sea oportuno y veraz, mejorando el acceso a los datos de salud con el uso de tecnologías de la información, no se está garantizando necesariamente la seguridad

9 Ley N° 29733, Ley de Protección de Datos Personales

“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”.

10 Decreto Supremo No. 003-2013-JUS, Reglamento de la Ley 29733

“Artículo 10.- Principio de seguridad

En atención al principio de seguridad, en el tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley o al presente reglamento, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado”.

11 Reglamento (UE) 2016/679

“Artículo 4. Definiciones

(...)

12. violación de la seguridad de los datos personales”: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o lícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

(...)”.

12 Reglamento (UE) 2016/679

“Artículo 5. Principios relativos al tratamiento

1. Los datos serán:

(...)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (“integridad y confidencialidad”)

de los mismos.

Es necesario reparar en que la confianza del paciente sobre la confidencialidad depende de la seguridad del aparato técnico y la transparencia sobre el tratamiento de los datos personales en salud, tanto de médicos como no-médicos involucrados en las operaciones y procesos. (Almada & Maranhão, 2021) Por ello, el acceso no debe ser indiscriminado, incluso cuando el mismo se sustente en razones científicas, por lo que deben implementarse mecanismos que eviten afectar la seguridad de los datos de salud, es decir, su integridad y confidencialidad.

2.4 CALIDAD O ALMACENAMIENTO POR TIEMPO LIMITADO

El tratamiento de datos personales recopilados en el marco de la excepción de la obligación de del consentimiento por autoridades sanitarias o por empresas privadas, en el marco de la excepción de la obligación del consentimiento, deben limitarse, como sucede con cualquier tipo de tratamiento, al tiempo de duración de la situación de emergencia sanitaria, por ello debe garantizarse que la información obtenida no será empleada a largo plazo con otros fines estatales o privados.

Esta regla ha sido recogida en el artículo 8¹³ de la LPDP, norma que dispone que los datos personales deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento. Asimismo, en el artículo 28¹⁴ de la LPDP se establece la obligación del responsable de tratamiento, cuando los datos hayan dejado de ser pertinentes, necesarios y adecuados para la finalidad establecida, de suprimirlos o anonimizarlos o deberá aplicarles un mecanismo de disociación o de seudonimización con código, permaneciendo los datos seguirán activos, pero sin poder identificar de manera sencilla al titular de los mismos, salvaguardando su derecho a la protección de los datos personales.

El RGPD europeo recoge un precepto cuyo contenido está en armonía con las citadas normas de la LPDP peruana. En su artículo 5¹⁵, el RGPD dispone que los datos personales

13 Ley N° 29733, Ley de Protección de Datos Personales

“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 fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad del tratamiento”.

14 Ley N° 29733, Ley de Protección de Datos Personales

“Artículo 28. Obligaciones

(...)

7. Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimización o disociación.

(...)”.

15 Reglamento (UE) 2016/679

“Artículo 5. Principios relativos al tratamiento

1. Los datos serán:

(...)

e) Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales

deben mantenerse de forma que se permita la identificación de los interesados durante no más del tiempo necesario para los fines del tratamiento de los datos personales (“limitación del plazo de conservación”).

Superado ese tiempo sólo pueden conservarse durante períodos más largos con las finalidades de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, siendo en ocasiones preciso, en orden a salvaguardar el principio de minimización, proceder a la seudonimización de los datos (RGPD art. 89.1), y sin perjuicio de la aplicación de técnicas organizativas apropiadas que impone el RGPD para proteger los derechos del interesado (López, L.F., 2016, p. 61).

3. EL USO DE HERRAMIENTAS TECNOLÓGICAS SUSTENTADAS EN EL TRATAMIENTO DE DATOS PERSONALES PARA LUCHAR CONTRA LA PANDEMIA DEL COVID-19: IDENTIFICACIÓN DE ALGUNOS RIESGOS Y AFECTACIONES AL DERECHO FUNDAMENTAL DE PROTECCIÓN DE DATOS PERSONALES

Con la declaratoria de la pandemia por el COVID-19, diversas naciones del mundo han implementado numerosas iniciativas encaminadas a paliar los efectos nocivos del virus mediante el desarrollo de herramientas tecnológicas sustentadas en el tratamiento de datos de salud. La latente amenaza que para la vida humana representa el COVID-19 hace necesaria su contención a través de una gestión de datos personales correcta y medios idóneos que coadyuven a dicho fin.

Por ello, en los últimos meses diversos gobiernos y empresas privadas han implementado estrategias digitales que complementan los instrumentos de vigilancia epidemiológica para la detección de casos, el rastreo de contactos, el diagnóstico de la enfermedad, la documentación de lugares donde las personas han estado, la determinación de sitios y momentos de mayor afluencia, para así implementar medidas que limiten el contagio. Además, se han usado para comunicar y educar a la ciudadanía o darle atención sanitaria a través de telepresencia (Gómez-Córdoba et al., 2020, p. 274). Esto ha sido reconocido a nivel internacional en la Resolución No. 1/2020 de la Corte Interamericana de Derechos Humanos, titulada “Pandemia y Derechos Humanos en las Américas”:

En cuanto a las medidas de contención con el fin de enfrentar y prevenir los efectos de la pandemia, la CIDH ha observado que se han suspendido y restringido algunos derechos, y en otros casos se han declarado “estados de emergencia”, “estados de excepción”, “estados de catástrofe por calamidad pública”, o “emergencia sanitaria”, a través de decretos presidenciales y normativa de diversa naturaleza jurídica con el fin de proteger la salud pública y evitar el incremento de contagios. Asimismo, se han establecido medidas de distinta naturaleza que restringen los derechos de la libertad de expresión, el derecho de acceso a la información pública, la libertad personal, la inviolabilidad del domicilio, el derecho a la propiedad privada; y se ha recurrido al uso de tecnología de vigilancia para rastrear la propagación del coronavirus, y al almacenamiento de datos de forma masiva. (CIDH, 2020, p.4).

podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);”

En efecto, la llamada tecnología de vigilancia se ha materializado en aplicativos que tienen como principal intención informar sobre el virus y brindar un diagnóstico a partir de los datos ingresados en el aplicativo e identificar individuos contagiados, focos de contagio y permitir el rastreo del contagio (*tracking* y *tracing*). Asimismo, se han implementado herramientas tecnológicas que han permitido medición masiva de temperatura en espacios de uso público.

No existen dudas de que la implementación de nuevas tecnologías sustentadas en el tratamiento de datos personales, unido al uso de técnicas propias de la analítica de datos y la Inteligencia Artificial, comportan beneficios significativos y representan una importante oportunidad para detener la expansión del COVID-19, en tanto que permiten mejorar la capacidad de previsión y decisión de las autoridades sanitarias, contribuyen a fortalecer la eficacia de las medidas de distanciamiento social reduciendo con ello significativamente la propagación de la pandemia y minimizando el coste de vidas humanas (Domínguez, 2020, p. 610).

No obstante, como previamente se ha señalado, estas estrategias no siempre se configuran dentro de un régimen jurídico de protección de datos personales robusto y que garantice debidamente la protección de los datos personales y sus principios, lo que justifica identificar, para su prevención, los riesgos que se generan cuando se emplean herramientas tecnológicas que tratan datos personales y las posibles afectaciones al derecho fundamental a la protección de datos personales, máxime cuando su utilización ha hecho que los métodos de recopilación de datos personales sean cada vez más abundantes, complicados y se detecten con mayor dificultad (Cristea, 2018, p. 226).

Este contexto, plantea un necesario análisis de aquellas cuestiones que permitan alcanzar el difícil equilibrio entre el impulso de instrumentos tecnológicos que contribuyan a controlar los efectos del COVID-19 incrementando los recursos puestos a disposición de las autoridades sanitarias y la salvaguarda del derecho fundamental a la protección de datos personales.

3.1 INFORMACIÓN Y DIAGNÓSTICO DEL VIRUS

Contar con canales informativos que permanentemente sean actualizados sobre el COVID-19, sus síntomas, las medidas de prevención y diagnóstico es un asunto de interés para cualquier persona que tenga mínimamente algún síntoma o busque información que necesite compartir en su entorno familiar.

Ante el colapso de la atención telefónica para las consultas, los Estados, empresas privadas, organizaciones supranacionales desarrollaron apps, webs, chatbots, canales de Telegram, entre otros, a fin de que la ciudadanía obtenga información veraz y oficial o realice autoevaluaciones de forma sencilla, sin necesidad de hacer una llamada telefónica o acudir a la emergencia de un centro de salud pública o privada (Cascón-Katchadurian, 2020, p. 4).

En lo concerniente a las aplicaciones de autoevaluación, estás ofrecen recomendaciones sobre cómo actuar según los síntomas, llegando incluso a ponerse en contacto con los usuarios para realizarles test sobre el coronavirus o un seguimiento de la evolución de la enfermedad (Cascón-Katchadurian, 2020, p. 4). Todos estos datos se usan igualmente para hacer una representación aproximada del nivel posible de inmunidad de la población (Cascón-Katchadurian, 2020, p. 4).

En España, la Secretaría General de Administración Digital, dependiente de la Secretaría

de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, desarrolló el aplicativo móvil *Radar COVID*. Con su descarga, los usuarios de esta app reciben una notificación en caso de que en los catorce días anteriores a la misma hayan estado expuestos a un contacto epidemiológico con otro usuario que haya declarado en la aplicación haber dado un resultado positivo en la prueba de COVID-19, previa acreditación por parte de las autoridades sanitarias correspondientes (Domínguez, 2020).

En Corea del Sur se desarrolló la app *Self-quarantine safety protection* con el objetivo de evitar el descontrol de la enfermedad y el colapso de los hospitales, para lo cual registra los datos de los usuarios y sus respuestas a preguntas sobre el estado de salud y con los mismos los médicos ofrecen un diagnóstico en remoto lo cual ayuda a la descongestión de los teléfonos (Cascón-Katchadurian, 2020, p. 5). “De esta forma se consigue un diagnóstico masivo y con esos datos se decide a quién debe realizarse el test” (Ruiz, 2020 citado en Cascón-Katchadurian, 2020, p. 5).

En el caso peruano, la app que se ha hecho cargo de proveer información actualizada sobre las zonas de contagio y brindar a los ciudadanos un pronóstico sobre su posible condición de portador del COVID-19 fue la llamada “*El Perú en tus manos*”, la misma que “ofrece la opción «Mapa de zonas afectadas» (...) para acceder a un mapa de cercanías a él donde se marca la incidencia de contagios; así también, se dispone de la opción «Triage» (...) mediante el cual, de acuerdo con los síntomas que consigne, podrá determinar si es o no un posible portador del mencionado virus.” (Vásquez, 2020, p. 158).

Con respecto a los riesgos o posibles afectaciones al derecho a la protección de datos personales, que pueden derivarse de este tipo de apps deben considerarse aquellos vinculados al principio del consentimiento de las personas, puesto que existe el peligro que tanto los datos ingresados por las personas para recibir actualizaciones informativas sobre el virus como los datos ingresados para generar un autodiagnóstico de la app sean usados para una finalidad distinta a la que el usuario creía y consentía.

El análisis parte de considerar que cuando un usuario brinda sus datos identificativos y de salud para ser informado y/o autoevaluado por el aplicativo, su consentimiento girará en torno a la finalidad concreta del servicio; por tanto, el responsable del tratamiento que gestione la app no podría emplear los datos para una finalidad distinta a la de diagnosticar el virus con los datos del usuario.

Respecto a los aplicativos que son capaces de realizar un autodiagnóstico, se encuentran aquellos que lo logran en base a la grabación de voz de las personas. En España, por ejemplo, la empresa Biometric Vox viene desarrollando con ayuda de inteligencia artificial una app que será capaz de detectar un índice de contagio del COVID-19. Este sistema permitiría analizar - a distancia, sin contacto físico y en tiempo real - el estado del aparato fonador y, como consecuencia, poder aportar un índice de contagio y servir a las autoridades sanitarias como ayuda complementaria para el control de la propagación y cualquier otra gestión de datos (Biometric Vox, 2020, párr. 4).

En Brasil, SPIRA y SoundCov son dos aplicativos en los que los usuarios realizan una grabación de su voz que luego es analizada a través de algoritmos de aprendizaje automático dando lugar a un diagnóstico del COVID-19 (Almada & Maranhão, 2021, pp. 1-2).

The SPIRA project, currently under development at the University of São Paulo, seeks to detect severe respiratory insufficiency associated with the SARS-CoV-2

virus, to indicate whether the user of the app must seek hospitalization. To obtain this diagnosis, the SPIRA app records the patient's reading of a few pre-defined sentences. These recordings are analyzed by a machine learning model trained to distinguish the voices of healthy persons from those of people afflicted with respiratory insufficiencies (Almada & Maranhão, 2021, p. 2).

[El proyecto SPIRA, actualmente en desarrollo en la Universidad de São Paulo, pretende detectar la insuficiencia respiratoria grave asociada al virus SARS-CoV-2, para indicar si el usuario de la aplicación debe ser hospitalizado. Para obtener este diagnóstico, la aplicación SPIRA registra la lectura del paciente de unas frases predefinidas. Estas grabaciones son analizadas por un modelo de aprendizaje automático entrenado para distinguir las voces de personas sanas de las de personas afectadas por insuficiencias respiratorias].

SoundCov, an app developed by Fiocruz, Intel, and Instituto Butantan, trains a machine learning system to distinguish between the coughing sounds of a Covid-19-positive person and those of healthy people and people afflicted by other respiratory illnesses, such as pneumonia or tuberculosis. The application then combines the analysis of the coughing sounds with additional information about epidemiological variables and patient's health history, thus producing a final diagnosis (Almada & Maranhão, 2021, p. 2).

[SoundCov, una aplicación desarrollada por Fiocruz, Intel y el Instituto Butantan, entrena un sistema de aprendizaje automático para distinguir entre los sonidos de la tos de una persona que da positivo en el Covid-19 y los de personas sanas y los de personas afectadas por otras enfermedades respiratorias, como la neumonía o la tuberculosis. A continuación, la aplicación combina el análisis de los sonidos de la tos con información adicional sobre las variables epidemiológicas y el historial de salud del paciente, con lo que se obtiene un diagnóstico final].

Con este tipo de tecnología puede generarse una transgresión al principio de consentimiento ya que el mismo debe obtenerse brindando a los titulares de los datos de salud toda aquella información acerca de la forma y duración del tratamiento, de manera que, si ello no se produce, el consentimiento se considera inválido (Almada & Maranhão, 2021, p. 7). Vinculado a esto último, debe repararse en que las aplicaciones basadas en sistemas de aprendizaje automático son notoriamente opacas para los observadores externos, lo que plantea dificultades adicionales a la tarea de proporcionar a los usuarios la información que necesitan para dar su consentimiento informado (Almada & Maranhão, 2021, p. 7).

También se identifica la posibilidad de que se transgreda el principio de finalidad aplicable al tratamiento de los datos personales y, por tanto, se afecte al titular de los mismos, en razón a que

Almacenar datos de voz, hace posible que entidades no autorizadas utilicen los datos para identificar a las personas, obtener acceso de manera malintencionada a los sistemas que implementan el reconocimiento de voz, o simplemente procesar datos y construir artefactos de voz que podrían utilizarse para personalizar a los individuos creando escenarios que resultan problemáticos (Alva, 2020, p. 171).

Otra de las situaciones que pueden generar riesgos y afectaciones es la que se produce cuando los responsables de las apps mantienen datos de salud indefinidamente. Esto último está directamente relacionado con el principio de calidad e implica que los responsables del tratamiento de los datos de salud deben garantizar que la información

obtenida no será empleada a largo plazo con otros fines estatales o privados, sino que deben limitarse al tiempo de duración de la pandemia.

De esta forma, la exposición que puede tener el titular de los datos de salud que accedan a este tipo de app a que la utilización de su información sea destinada para finalidad distintas es alta, por lo que resulta indispensable identificar cuál es la empresa que pone a disposición el aplicativo y revisar sus políticas de privacidad, de forma previa a consignar datos personales con el objetivo de obtener información y/o efectuar un autodiagnóstico.

3.2 GEOLOCALIZACIÓN Y SEGUIMIENTO DE CONTAGIADOS

Sobre este punto, es necesario realizar una precisión conceptual previa debido a que el frente al uso de los teléfonos móviles para ayudar a controlar la pandemia, se presentan dos posibilidades principales: una basada en el geoposicionamiento (o *tracking*) y otra basada en el seguimiento automatizado de contactos (o *tracing*) (Buchland, 2020).

De acuerdo con la distinción mientras que el *tracking* consiste en que la app instalada en un teléfono móvil va guardando en todo momento la posición de la persona que lo utiliza, el *tracing* busca realizar un seguimiento automatizado de contactos, lo cual, involucra que haya una comunicación directa entre el teléfono móvil de una persona con el de todas aquellas personas con las que quiere estar en contacto cercano (Buchland, 2020).

Lo cierto es que, como se verá a continuación ni las herramientas enfocadas en *tracking* ni las apps destinadas al *tracing* se libran de los grandes peligros que surgen en cuanto a datos personales se refiere.

A. GEOPOSICIONAMIENTO (*TRACKING*)

Frente al avance del COVID-19 los Estados han implementado iniciativas tecnológicas destinadas a conocer los movimientos de la población para que a través de su estudio cuenten con patrones de la movilidad de las personas alrededor de una ciudad, región o país, con el objetivo de registrar la localización de las de personas contagiadas (o no contagiadas, para que no eviten el confinamiento) para asistirlas en caso sea necesario. Entonces, el conocimiento de estos datos resulta beneficioso para que los entes de la Administración a cargo de salud, seguridad e infraestructura, a la hora de articular y dimensionar las acciones que mitiguen el virus, puedan hacerlo de la manera más adecuada (AEPD, 2020a, p. 5).

La herramienta que permite conocer estos datos es la geolocalización o geoposicionamiento, es decir, una app que hace uso del *Global Position System* o más comúnmente conocido como GPS. Lo que debe considerarse, es que este tipo de herramientas tienen algunos problemas prácticos, como la falta de exactitud en la geolocalización (sobre todo en espacios interiores), o que los teléfonos móviles sólo informan que los usuarios han estado cerca de una persona, entre otros. (Buchland, 2020).

No obstante, si bien son conocidas las limitaciones que acompañan a la tecnología, lo cierto es que el contexto de la pandemia ha involucrado una proliferación de soluciones tecnológicas que han tenido la intención de apoyar en la lucha contra la pandemia (Andreu, 2020, p. 851). Es el caso de la app HaMagen, la cual ha sido un ejemplo de cómo el *tracking* puede ser una herramienta interesante para que un gobierno emprenda acciones eficientes para con su población. Las funcionalidades de este aplicativo han sido explicadas por el Ministerio de Salud de Israel:

HAMAGEN is an app that allows the identification of contacts between diagnosed patients and people who came in contact with them in the 14 days prior to the patient's diagnosis of the disease.

Cross-referencing your location data with the corona patients' location is done on your device and as soon as a match is identified, you will be directed to a link to the Ministry of Health to let you know what steps to take and to report the match to The Ministry (Israel National Cyber Directorate, 2020, p. 1).

[HAMAGEN es una app que permite identificar los contactos entre pacientes diagnosticados y las personas que estuvieron en contacto con ellos en los 14 días anteriores al diagnóstico de la enfermedad del paciente. El cruce de sus datos de localización (del usuario) con la ubicación de los pacientes de Corona se realiza en su dispositivo y, en cuanto se identifique una coincidencia, se le dirigirá a un enlace al Ministerio de Sanidad para informarle de los pasos que debe dar y para informar la coincidencia al Ministerio].

La geolocalización a través de dispositivos móviles puede operar de dos formas: por los operadores de telecomunicaciones y a partir de las redes sociales¹⁶. Sin embargo, ninguna de estas formas está privada de riesgos.

En el caso de la geolocalización realizada a través de los teléfonos móviles por los operadores de telecomunicaciones, esta consiste en que los operadores de telefonía móvil "proporcionen información anonimizada de la ubicación de sus usuarios en las celdas de telefonía que definen sus antenas" (AEPD, 2020a, p. 4). El riesgo que puede generarse es el de una anonimización incompleta, una subcontratación poco rigurosa o un ciberataque que ponga en manos de un tercero la localización de los teléfonos móviles de los usuarios.

Respecto a la geolocalización de los teléfonos móviles a partir de redes sociales, esta es una técnica utilizada antes de la pandemia ya que las direcciones IP de los usuarios pueden ser conocidas por los administradores de las páginas web y son utilizadas habitualmente con fines de publicidad. La información puede ser de ayuda para las autoridades sanitarias siempre que esté de acuerdo con un propósito y un fin previamente definido y sea aplicado a sus estrategias de prevención y control (AEPD, 2020a, p. 6).

La geolocalización puede brindar algunas tendencias y estadística de contagio a los operadores de los gobiernos para que haya más acción de su parte en las diferentes zonas. Sin embargo, como se ha visto en los anteriores párrafos, el geoposicionamiento hoy en día puede ser también una excusa para que se emprendan abusos contra el derecho fundamental a la protección de datos personales, incluso hay quienes consideran que "la inusitada expansión de la vigilancia y control estatal por medio de las tecnologías digitales para monitorear la posible transmisión del virus implica una importante regresión en materia de derechos humanos que será difícil de revertir en el escenario post-pandemia" (Bizberge y Segura, 2020, p. 71).

B. RASTREO Y SEGUIMIENTO DE CONTACTOS (TRACING)

El rastreo de contactos sigue la lógica de los servicios utilizada tradicionalmente por los servicios de salud: "se trata de cualquier registro de escrito que identifica a un paciente y sigue su historia clínica, la que es monitoreada por trabajadores de la salud, quienes a su vez pueden entregarle recomendaciones médicas personal o técnicamente" (Weidenslaufer, C. y Meza, M. 2020, p. 1).

16 Clasificación propuesta por la Agencia Española de Protección de datos.

Han surgido entonces en el medio nuevas formas para diseñar aplicativos, con la finalidad que los mismos colaboren más allá de una simple localización. Nos referimos a aquellos aplicativos que logran hacer una labor de *tracing* y no solo de *tracking*, previamente desarrollada. El objetivo al cual están orientadas, no sólo es el de hacer seguimiento de enfermos, sino también alertar a quienes hayan estado físicamente cerca de un paciente de COVID-19 adopten las medidas necesarias sanitarias pertinentes más adecuadas que permitan ayudar a contener la propagación del virus (Weidenslauer, C. y Meza, M. 2020, p. 1).

Es prácticamente imposible que un sujeto recuerde, y conozca, todos los contactos que haya podido tener a lo largo de un período de entre dos días o una semana desde que muestra síntomas. Lo importante es romper la cadena de transmisión de la infección de la forma más eficaz posible. Y esto lo pueden hacer las apps de rastreo de contactos (Arenas, M. 2020, p.3).

En las apps del tipo *tracing* cuya tecnología predominante es el *bluetooth*, lo que interesa no es tanto la localización exacta de la persona, sino registrar a las posibles personas con las que ha estado en contacto para que en el momento que alguien dé positivo se avise a todos los demás y de esa forma detectar a los asintomáticos (Cascón-Katchadurian, 2020, p. 10). Una de las ventajas de estos aplicativos que emplean el *bluetooth* es que son anónimas y descentralizadas por lo general, por lo que a los usuarios les indicaría que han estado en contacto con un paciente que ha dado positivo, pero no revelará la identidad de la persona (Cascón-Katchadurian, 2020, p. 15).

Se debe reparar en el hecho de que los Estados monitorean a su población por su geolocalización coadyuva a que la asistencia en puntos geográficos específicos se brinde de una manera más pronta y eficaz; sin embargo, no hay que considerar que ello esté exento de afectaciones al derecho fundamental a la protección de datos personales debido a las prácticas que pueden derivarse del objetivo antes descrito. Esto último lo ha identificado Access Now¹⁷, al señalar que “el rastreo de la ubicación geográfica de los teléfonos inteligentes proporciona información sobre el movimiento de los teléfonos de las personas y no del virus” (2020, p. 10), y que realizar seguimiento de cómo evoluciona el COVID – 19 mediante referencias cruzadas entre los datos geográficos de las personas con los casos de infección conlleva riesgos inherentes (2020, p. 10).

La referida organización refiere además que, si bien la información que se registra a través de la apps de rastreo y seguimiento es anónima dicha características puede revertirse de manera que las personas pueden ser reidentificadas fácilmente, y que la información puede resultar incompleta respecto del lugar en que la persona realiza sus actividades (Access Now, 2020, p. 10).

Los riesgos y la posible afectación al derecho a la protección de datos personales de este tipo de soluciones pueden producirse cuando se realizan mapas de relaciones entre personas, reidentificación por localización implícita de la fragilidad de los protocolos a la hora de configurar tarjetas casi anónimas, y al dispersarse las señales de los contagios de forma que no se identifique en ningún caso la identidad de los contagiados.

3.3 MEDICIÓN MASIVA DE TEMPERATURA EN ESPACIOS DE USO PÚBLICO

Al ser la fiebre el síntoma más recurrente en los infectados por el COVID-19, el escaneo de temperatura en las personas cumple una especial relevancia (Wilches-Visbal et al,

17 Access Now es una organización sin fines de lucro que viene funcionando desde el año 2009. Su misión es la defensa de los derechos digitales de los usuarios del mundo.

2021). Siendo así, una de las formas de medición masiva de temperatura en espacios de uso público ha sido a través de cámaras térmicas de reconocimiento facial.

Las cámaras térmicas son dispositivos que “detectan la radiación infrarroja emitida por cualquier cuerpo con temperatura superior al cero absoluto y la transforman en una señal eléctrica, que luego es procesada para obtener un valor o un mapa de temperaturas” (Wilches – Visbal et al, 2020, pp. 305-306). Como señala la AEPD, “(...) añaden la capacidad de tomar la temperatura a los individuos que cruzan un área, sin requerir en muchos casos ninguna acción por su parte” (2020a, p. 11).

Al respecto, si bien el uso de cámaras térmicas supone el empleo de una tecnología interesante para identificar el contagio, puede llegar a ser una práctica que comprometa los datos personales de las personas si es que va de la mano con el reconocimiento facial de las mismas, como lo ha sostenido Van Natta et al.: “In such exceptional times, one could argue that fever checks offer substantial population health benefits with limited long-term impacts on personal privacy. Yet, several private companies have integrated thermal imaging with facial recognition technology”. [En tiempos tan excepcionales, se podría argumentar que los controles de fiebre ofrecen importantes beneficios para la salud de la población con un impacto limitado a largo plazo en la privacidad personal. Sin embargo, varias empresas privadas han integrado la imagen térmica con la tecnología de reconocimiento facial] (2020, p. 5).

En el ámbito laboral y, en concreto en la normativa de seguridad y salud en el trabajo, la toma de temperatura puede ser de utilidad, pero situada en un marco de tratamiento de datos más extenso del que formen parte otras comprobaciones y garantías adicionales en las que se respeten los derechos y libertades previstos en la normativa de protección de datos personales (AEPD, 2020a, p. 12).

En el Perú, la Ley No. 29783, Ley de Seguridad y Salud en el Trabajo, señala en el literal c) de su artículo 49 que es una obligación del empleador: “identificar las modificaciones que puedan darse en las condiciones de trabajo y disponer lo necesario para la adopción de medidas de prevención de los riesgos laborales”. Esta obligación supone que el empleador preste particular atención a las medidas que toma para que sus trabajadores se encuentren en una situación de riesgo controlado en su centro de labores.

Respecto a los riesgos a la posible afectación al derecho a la protección de datos personales debe repararse en que la cámara térmica y la recopilación del dato solo puede entenderse como parte de un tratamiento mayor y no puede tomar un dato de salud a una persona y tratarlo espontáneamente por cualquier gestor de un lugar público simplemente porque crea que es lo mejor para sus clientes y usuarios (AEPD, 2020a, p. 12), lo que puede afectar directamente el principio de finalidad.

También resulta especialmente problemático no tener la posibilidad de conocer el alcance de la información que puede obtenerse utilizando los datos personales de salud recopilados mediante esta herramienta tecnológica, porque puede tratarse de información basada en la medición de temperatura que revele información reservada del estado de salud de la persona como puede ser el embarazo, la menopausia o el uso de fármacos, lo que supondría una afectación directa al principio de proporcionalidad en materia de protección de datos personales (Van Natta et al., 2020, p. 7).

En caso de no contar con una regulación adecuada, un monitoreo con tantas imprecisiones puede inadvertidamente generar un daño en los individuos que son etiquetados en un centro comercial, durante un viaje, sin que pueda tener una mínima posibilidad rectificación (Van Natta et al., 2020, p. 8), lo que supone una vulneración al principio

de calidad. Asimismo, se tendrá un riesgo de discriminación, estigmatización y tal vez difusión pública de datos de salud. Todo ello se puede agravar con el riesgo de fugas de información sensible si es que no se atiende al principio de seguridad en la protección de datos personales.

4. A MODO DE CONCLUSIÓN

Lo desarrollado en este trabajo conlleva una reflexión respecto del cuidado que los Estados y el sector privado deben tener al adoptar medidas para enfrentar la expansión del COVID-19, las cuales pueden tener consecuencias irreversibles en el derecho fundamental a la protección de datos personales y que pueden estar guiadas únicamente por la urgencia, el miedo y lo que es peor, por otros intereses.

Y es que, como consecuencia de la pandemia, los Estados y particulares han implementado distintas herramientas tecnológicas con la finalidad de proteger la salud pública y evitar la propagación de contagios. No obstante, en determinados casos, la implementación de estas herramientas conlleva a asumir riesgos y afectaciones al derecho a la protección de datos personales.

Comprobada la existencia de estos riesgos, resulta pertinente rescatar lo considerado por la antes citada Resolución de la CIDH, en tanto recomienda a los gobiernos de los Estados miembros que deben guiar su actuación de conformidad con dos obligaciones generales relacionadas a la protección de datos personales:

35. Proteger el derecho a la privacidad y los datos personales de la población, especialmente de la información personal sensible de los pacientes y personas sometidas a exámenes durante la pandemia. Los Estados, prestadores de salud, empresas y otros actores económicos involucrados en los esfuerzos de contención y tratamiento de la pandemia, deberán obtener el consentimiento al recabar y compartir datos sensibles de tales personas. Solo deben almacenar los datos personales recabados durante la emergencia con el fin limitado de combatir la pandemia, sin compartirlos con fines comerciales o de otra naturaleza. Las personas afectadas y pacientes conservarán el derecho a cancelación de sus datos sensibles.

36. Asegurar que, en caso de recurrir a herramientas de vigilancia digital para determinar, acompañar o contener la expansión de la epidemia y el seguimiento de personas afectadas, éstas deben ser estrictamente limitadas, tanto en términos de propósito como de tiempo, y proteger rigurosamente los derechos individuales, el principio de no discriminación y las libertades fundamentales. Los Estados deben transparentar las herramientas de vigilancia que están utilizando y su finalidad, así como poner en marcha mecanismos de supervisión independientes del uso de estas tecnologías de vigilancia, y los canales y mecanismos seguros para recepción de denuncias y reclamaciones.

Como se advierte, son diversos los riesgos asociados a los aplicativos que brindan información sobre el virus o facilitan al usuario un autodiagnóstico. No obstante, es responsabilidad de los Estados y de las empresas brindar gestión correcta de los datos personales de los usuarios de los aplicativos para lograr los objetivos de dar información y atención en la pandemia de forma eficiente y respetuosa de los principios del derecho fundamental a la protección de datos personales.

Es por esta razón que debe reforzarse la garantía del derecho fundamental a la protección de datos personales a través de un adecuado diseño de las herramientas tecnológicas y

de nuevos modelos de gestión de la información, lo que significa que en su desarrollo deben participar no solo expertos en sistemas de información, sino también científicos de datos, especialistas en inteligencia artificial, en bioética, bioderecho y en derechos humanos.

El tratamiento de datos personales en la actual emergencia sanitaria debe tener un objetivo general basado en evidencias científicas, en el que se haya evaluado su proporcionalidad en relación con su eficacia, eficiencia y teniendo en cuenta, de forma objetiva, los recursos organizativos que sean necesarios.

REFERENCIAS BIBLIOGRÁFICAS

- Arias, M. (2016). Definiciones a efectos del Reglamento General de Protección de Datos. En J.L. Piñar (Dir.) *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad* (115-134). Reus.
- Access Now. (2020). Recomendaciones para la protección de la privacidad y los datos en la lucha contra el COVID-19. 28. Disponible en: <https://www.accessnow.org/cms/assets/uploads/2020/04/Recomendaciones-para-la-protección-de-la-privacidad-y-los-datos-en-la-lucha-contra-el-COVID-19.pdf>
- Agencia Española de Protección de Datos (AEPD). (2020). Informe N/Ref. 0017-2020 sobre el tratamiento de datos personales en relación a la extensión del virus COVID-19.
- Agencia Española de Protección de Datos (AEPD). (2020a). Informe sobre el uso de las tecnologías en la lucha contra el COVID-19. Un análisis de costes y beneficios.
- Agencia Española de Protección de Datos (AEPD). (2018). *Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales sujetos al RGPD* [Guía].
- Almada, M., & Maranhão, J. (2021). Voice-based diagnosis of covid-19: Ethical and legal challenges. *International Data Privacy Law*, 11(1), 63-75. Fecha de consulta: 15 de abril de 2021. Disponible en: <https://doi.org/10.1093/idpl/ipab004>
- Alva, V. (2020). La pandemia COVID-19, distanciamiento social, el uso de tecnologías de la información y comunicación y la falta de la regulación internacional que proteja los datos personales. *Revista Académica de la Facultad de Derecho de la Universidad La Salle*. Fecha de consulta: 28 de junio de 2021. Disponible en: <https://repositorio.lasalle.mx/handle/lasalle/1695>
- Andreu Martínez, B. (2020). Privacidad, geolocalización y aplicaciones de rastreo de contactos en la estrategia de salud pública generada por la COVID-19. *Actualidad Jurídica Iberoamericana* 12, pp. 848-859
- Angarita, N. R. (2012). Aproximación constitucional de la protección de datos personales en Latinoamérica. *Revista Internacional de Protección de datos personales*, 13.
- Angarita, N. R. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo? *International Law: Revista Colombiana de Derecho Internacional*, 8(16).
- Arenas, M. (2020). ¿Testing, Tracing, Isolation? A propósito de las Directrices 04/2020 del Comité Europeo de Protección de Datos. *LA LEY Privacidad*, 4.

Arenas, M. (2020). ¿Rastrear o no rastrear? He ahí la cuestión. Las apps de rastreo de contactos y la protección de datos personales. *LA LEY Privacidad*, 5.

Autoridad Nacional de Protección de Datos Personales. (2019). Opinión Consultiva No. 07-2019-JUS/DGTAIPD-DPDP. Limitaciones al consentimiento cuando se de tratamiento a datos relacionados a la salud, de conformidad al artículo 14, numeral 6, de la Ley No. 29733. 06 de febrero.

Biometric Vox (2020). Biometric Vox inicia una investigación con inteligencia artificial para detectar COVID19 a través la voz. Disponible en: <https://biometricvox.com/blog/general/biometrivicvox-inicia-investigacion-inteligencia-artificial-detectar-covid19-por-voz/>

Bizberge, A. y Segura, M.S. (2020). Los derechos digitales durante la pandemia COVID-19 en Argentina, Brazil y México. *Revista de Comunicación*. 19 (2) pp. 61- 85.

Buchland Gidumal, J. (2020). ¿Son fiables las aplicaciones de geolocalización? *The Conversation*. Fecha de consulta: 23 de mayo de 2021. Disponible en: <https://theconversation.com/son-fiables-las-aplicaciones-de-geolocalizacion-y-seguimiento-de-contactos-141069>

Cascón-Katchadourian, Jesús-Daniel (2020). Tecnologías para luchar contra la pandemia Covid-19: geolocalización, rastreo, big data, SIG, inteligencia artificial y privacidad. *Profesional de la información*, v. 29, n. 4, e290429. <https://doi.org/10.3145/epi.2020.jul.29>

Cate, F. H., Cullen, P., & Mayer-Schonberger, V. (2013). Data protection principles for the 21st century.

Corredor, F. A., Suárez, J. C., & Patarroyo, L. J. (2020). Protección De Datos Personales en Sistemas De Monitorización y Vigilancia Masiva De Personas Ante La Pandemia De Covid-19.

Corte Interamericana de Derechos Humanos. (2020). Resolución 1/20: *Pandemia y Derechos Humanos en las Américas*.

Cristea, L. (2018). *La protección de datos de carácter sensible: Historia Clínica Digital y Big Data en Salud*. Bosch.

Cubillos Sánchez, M. C., y Restrepo Rojas, M. A. (2020, diciembre 7). La CoronAPP-Colombia y su política de tratamiento de datos. *Departamento de Derecho Informático*. <https://derinformatico.uexternado.edu.co/coroappcolombia/>

De', R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, 55, 102171. <https://doi.org/10.1016/j.ijinfomgt.2020.102171>

Domínguez, J. (2020). La necesaria protección de las categorías especiales de datos personales. Una reflexión sobre los datos relativos a la salud como axioma imprescindible para alcanzar el anhelado desarrollo tecnológico frente al COVID-19. *Revista de Comunicación y Salud*, 10(2), pp. 607-624.

European Data Protection Board (EDPB). (2020). Declaración sobre el tratamiento de datos personales en el contexto del brote de COVID-19. Adoptada el 19 de marzo de 2020. Fecha de consulta: 17 de mayo de 2021. Disponible en: <https://edpb.europa.eu>

europa.eu/sites/default/files/files/file1/edpb_statement_art_23gdpr_20200602_es_1.pdf

Gómez-Córdoba, A., Arévalo-Leal, S., Bernal-Camargo, D., Rosero de los Ríos, D., Gómez-Córdoba, A., Arévalo-Leal, S., Bernal-Camargo, D., & Rosero de los Ríos, D. (2020). El derecho a la protección de datos personales, tecnologías digitales y pandemia por COVID-19 en Colombia. *Revista de Bioética y Derecho*, 50, 271-294.

Herrera Bravo, R. (2011). Cloud computing y seguridad: Despejando nubes para proteger los datos personales. *Revista de derecho y ciencias penales: Ciencias Sociales y Políticas*, (17), 43-58.

Lopez, Luis Felipe (2016). *Protección de datos personales: adaptaciones necesarias al nuevo Reglamento europeo*. Francis Lefebvre.

Martinez, Ricard. (2020). A la muerte por protección de datos. Fecha de consulta: 20 de abril de 2021. Disponible en: <http://lopdyseguridad.es/a-la-muerte-por-proteccion-de-datos/>

Mendoza Enríquez, O. A. (2018). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. *Revista IUS*, 12(41), 267-291.

Naciones Unidas. Consejo de Derechos Humanos. (2020). Nota de prensa. COVID-19: los Estados no deben abusar de las medidas de emergencia para reprimir los DDHH. 16 de marzo. Fecha de consulta: 17 de mayo de 2021. Disponible en: <https://www.ohchr.org/SP/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=25722&LangID=S>

Oliver, N., Lepri, B., Sterly, H., Lambiotte, R., Deleatille, S., De Nadai, M., ... & Vinck, P. (2020). Mobile phone data for informing public health actions across the COVID-19 pandemic life cycle. *Sci Adv* 6 (23) Fecha de consulta: 24 de mayo de 2021. Disponible en: <https://advances.sciencemag.org/content/advances/6/23/eabc0764.full.pdf>

Piñar, José Luis. (2020). La protección de datos durante la crisis del coronavirus. Consejo General de Abogacía Española. Fecha de consulta: 20 de abril de 2021. Disponible en: <https://www.abogacia.es/actualidad/opinion-y-analisis/la-proteccion-de-datos-durante-la-crisis-del-coronavirus/>

Puyol, J. (2016) XI. Los principios del Derecho a la Protección de. En José Luis Piñar (Dir.), *Reglamento General de Protección de Datos*. Madrid, pp. 135-150

Razquín, M. (2019). El necesario equilibrio entre transparencia y protección de datos personales. En Diego Zegarra Valdivia (Coord.), *La proyección del derecho administrativo peruano: estudios por el centenario de la Facultad de Derecho de la PUCP*. Lima, Palestra, pp. 137-164.

Recuero Linares, M. (2020). La compartición internacional de datos personales relativos a la salud en tiempos de la COVID-19: Aspectos éticos y legales para el impulso de la necesaria cooperación. *Revista de Bioética y Derecho*, 50, 133-146.

Renda, A. (2020). Will privacy be one of the victims of COVID-19?. Centre for European Policy Studies. Publicado el 23 de marzo de 2020. Disponible en: <https://www.ceps.be/publications/will-privacy-be-one-victims-covid-19>

ceps.eu/will-privacy-be-one-of-the-victims-of-covid-19/

- Scheibner, J., lenca, M., Kechagia, S., Troncoso-Pastoriza, J.R., Raisaro, J.L., Hubaux, J.P.; Fellay, J., & Vayena E. (2020). Data protection and ethics requirements for multisite research with health data: a comparative examination of legislative governance frameworks and the role of data protection technologies. *Journal of Law and the Biosciences*, 1-30. <https://doi.org/10.1093/jlb/lcaa010>
- Van Natta, M., Chen, P., Herbek, S., Jain, R., Kastelic, N., Katz, E., Struble, M., Vanam, V., & Vattikonda, N. (2020). The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic. *Journal of Law and the Biosciences*, 7. <https://doi.org/10.1093/jlb/lcaa038>
- Vásquez Rodríguez, R. (2020). El consentimiento para tratamiento de datos personales de salud en tiempos del covid-19. *Yachaq Revista De Derecho*, (11), 145-164. <https://doi.org/10.51343/Yq.Vi11.366>
- Visbal, J. H. W., Pedraza, M. C. C., & Veliz, D. G. A. (2021). Procedimiento para el uso de pirómetros durante la pandemia por COVID-19: Procedure for the usage of pyrometers during the COVID-19 pandemic. *Archivos de Medicina (Manizales)*, 21(1), 305-308.
- Weidenslaufer, C. y Meza, M. (2020). COVID – 19: Uso de apps con rastreo de contactos y respeto de contactos y respecto a la privacidad. *Boletín 10 Biblioteca del Congreso Nacional de Chile / BCN*. Disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=documentos/10221.1/79593/1/boletin_coronavirus_10.1_FINAL.pdf
- Wilches-Visbal, Jorge-Homero, & Castillo-Pedraza, Midian-Clara, & Apaza-Veliz, Danny-Giancarlo (2021). Procedimiento para el uso de pirómetros durante la pandemia por COVID-19. *Archivos de Medicina (Col)*, 21(1), 305-309.
- Zegarra, D. (2014). Los principios de la protección de datos personales en el marco de la Ley No. 29733 y su Reglamento. En Jorge Danós Ordóñez y otros (Coords.), *Derecho Administrativo. Innovación, cambio y eficacia. Libro de ponencias del Sexto Congreso Nacional de Derecho Administrativo*. Lima, ECB Ediciones, pp. 623-635.
- Zegarra, D. (2019). La normativa peruana de protección de datos personales frente al reto de pasar de un modelo de gestión de datos al uso responsable de la información. En Diego Zegarra Valdivia (Coord.), *La proyección del derecho administrativo peruano: estudios por el centenario de la Facultad de Derecho de la PUCP*. Lima, Palestra, pp. 165-208.



EL USO DE ALGORITMOS Y SU IMPACTO EN LOS DATOS PERSONALES

THE USE OF ALGORITHMS AND THEIR IMPACT ON PERSONAL DATA

ALEJANDRO HUERGO LORA¹

RESUMEN

En el presente artículo se abordan las principales concepciones del término “algoritmo” y cómo el mismo es aplicado en el ámbito jurídico. Asimismo, se explica su relación con las predicciones basadas en datos y con los conceptos de inteligencia artificial digitalización y automatización, explicando sus principales características y diferencias. Posteriormente, se evalúa la aplicación de la inteligencia artificial en la creación y aplicación del Derecho. Después se analiza la injerencia de la regulación de datos personales en la utilización de algoritmos y el rol de la administración pública. Finalmente, se analizan los pormenores del proyecto del Reglamento sobre la Inteligencia Artificial.

PALABRAS CLAVE

Algoritmos | Predicción | Regulación |
Datos | Administración

CONTENIDO

1. Algoritmos: un concepto demasiado amplio; **2.** Cómo funcionan las predicciones basadas en datos; **3.** Inteligencia artificial; **4.** Parámetros jurídicos derivados de la protección de datos; **4.1** Pluralidad de perspectivas jurídicas sobre los algoritmos predictivos; **4.2** Los algoritmos funcionan, sobre todo, con datos anonimizados; **4.3** El consentimiento del interesado y sus debilidades; **4.4** Peculiaridades en el uso de datos por Administraciones Públicas; **4.5** Ambigüedad y casuismo; **4.6** Reglas concretas sobre el uso de algoritmos: decisiones automatizadas; **5.** El proyecto de Reglamento sobre la Inteligencia Artificial; **5.1.** Aplicaciones de la IA prohibidas; **5.2.** Aplicaciones de la IA

ABSTRACT

This article addresses the main conceptions of the term “algorithm” and how it is applied in the legal field. It also explains its relationship with data-driven predictions and with the concepts of artificial intelligence digitization and automation, explaining their main characteristics and differences. Subsequently, the application of artificial intelligence in the creation and application of the Law is evaluated. Then the interference of the regulation of personal data in the use of algorithms and the role of public administration is analyzed. Finally, the details of the draft Regulation on Artificial Intelligence are analyzed.

KEYWORDS

Algorithms | Prediction | Regulation |
Data | Administration

¹ Licenciado en Derecho por la Universidad de Oviedo y Doctor en Derecho por la Universidad de Bolonia. Ha sido investigador en la Universidad de Múnich tras ser el primer jurista español que obtuvo una beca postdoctoral del programa Marie Curie de la Unión Europea. Actualmente, se desempeña como catedrático de la Universidad de Oviedo desde 2010 y también imparte docencia en múltiples estudios de posgrado de diversas universidades españolas. Sus temas más habituales son las sanciones administrativas, los contratos públicos y el contencioso-administrativo. Ha dirigido el libro La regulación de los algoritmos (2020, con coordinación de Gustavo Manuel Díaz González). Contacto: ahuergo@uniovi.es

sometidas a autorización; **5.3.** Aplicaciones de la IA para las que se establecen reglas concretas de transparencia; **5.4.** Aplicaciones de la IA “de alto riesgo” y sus mecanismos de control; **5.5** Otras previsiones; **5.6.** Lo que regula y lo que no regula el proyecto de Reglamento.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 14 de junio de 2021 y aprobado para su publicación el 16 de agosto de 2021.

1. ALGORITMOS: UN CONCEPTO DEMASIADO AMPLIO

“Algoritmo” es una palabra de uso reciente en español, que parece muy ligada a los problemas y retos que plantea la inteligencia artificial o el *big data*. Sin embargo, no es exactamente así, y por ello creo que no es correcto hablar de un “régimen jurídico” o “naturaleza jurídica” de los algoritmos (o predicados similares), porque el término es demasiado impreciso.²

Aunque el uso de la palabra “algoritmo” en español es, como acabo de decir, reciente, y está ligado a la informática, en realidad tiene el mismo origen o raíz que la palabra “guarismo”, mucho más antigua y con un significado matemático, pero alejado del mundo de la inteligencia artificial o la informática. En realidad, parece que la palabra viene del nombre del matemático Mohamed ben Musa *al Juarismi* (que se supone que vivió entre 780 y 850, y trabajó fundamentalmente en Bagdad), y, de hecho, Juarismi sería la localidad de la que procedía, situada en el actual Uzbekistán (existe la palabra “Corasmia” para traducir ese topónimo). Al Juarismi ha tenido una gran influencia en la historia de las matemáticas y se le considera el creador del álgebra.³

En todo caso, el origen inmediato de la palabra “algoritmo” es la inglesa “algorithm”, que hace referencia a cualquier procedimiento formalizado en una serie de pasos para solucionar un problema o conseguir un resultado. Aunque puede haber (y hay) algoritmos al margen de los ordenadores, es decir, algoritmos no gestionados por ordenadores, lo cierto es que la palabra algoritmo se ha desarrollado (y ha llegado a la lengua castellana) en relación con la informática, pues los ordenadores necesitan ser programados y un programa de ordenador consiste, precisamente, en una sucesión ordenada de pasos que el ordenador ha de llevar a cabo. Los seres humanos pueden actuar mediante algoritmos o no; los ordenadores sólo pueden funcionar siguiendo un algoritmo.

Los “procedimientos” administrativos o judiciales son, al menos en cierto modo, algoritmos, en la medida en que se componen de pasos dotados de un contenido determinado, que han de seguirse para llegar a una solución (la resolución o acto final del procedimiento). La semejanza con los programas informáticos es, sin embargo, limitada, porque el tipo de vinculación que lleva al instructor o tramitador del procedimiento a seguir sus fases no tiene el mecanismo de un programa informático, sino que se trata de una vinculación jurídica. Al tramitar el procedimiento, el instructor sigue, voluntariamente, una norma jurídica. El programa no hace más que “obedecer” inconscientemente las órdenes que aparecen en el programa. Del mismo modo, mientras que en un programa es sencillamente imposible que se llegue al resultado final sin seguir todos los pasos o fases

2 De las cuestiones de que trata este artículo me he ocupado por extenso en “Una aproximación a los algoritmos desde el Derecho administrativo”, en HUERGO LORA, Alejandro (Dir.) / DÍAZ GONZÁLEZ, Gustavo Manuel (Coord.), *La regulación de los algoritmos*, Aranzadi, Cizur Menor, 2020, págs. 23-87, obra a la que remito a los lectores interesados.

3 BREZINA, C., *Al-Khwarizmi: The Inventor of Algebra*, Rosen Central, 2005.

(el programa “se colgaría” y no podría avanzar), en un procedimiento administrativo sí se puede dictar la resolución omitiendo (o ejecutando incorrectamente) alguna de las fases, y los efectos de esa omisión se determinarán con arreglo a una normas jurídicas (valorando, por ejemplo, la indefensión o los efectos de esa omisión sobre el contenido de la resolución final) y no en función de reglas mecánicas o puramente formales.

Si aplicamos este concepto al Derecho, existe una primera manifestación de los algoritmos jurídicos, que es la más sencilla y a la que estamos plenamente acostumbrados, aunque no se le haya dedicado una especial atención. Es frecuente que la Administración utilice programas o aplicaciones para llevar a cabo tareas concretas, es decir, para aplicar normas jurídicas o tramitar procedimientos. Un ejemplo sencillo, que en este caso manejan los ciudadanos y no la Administración, es el programa utilizado para elaborar la declaración del IRPF (durante bastantes años denominado “programa PADRE” y ahora “renta Web”). El contribuyente introduce los datos y el programa rellena las casillas de la declaración y establece el resultado, que el contribuyente firma, dotándolo así de efectos jurídicos. Las normas (en este caso, la Ley y el reglamento del IRPF, así como la legislación autonómica) han sido “volcadas” en un programa informático, algo que en este caso resulta en principio sencillo porque se trata de normas regladas. Las dudas que pueden surgir (por ejemplo, sobre la calificación jurídica de determinados ingresos, si son renta del trabajo o de actividades económicas, o están exentos) las resuelve, bajo su responsabilidad, el contribuyente al introducir los datos (aunque a veces el programa fuerza esas decisiones al admitir sólo una opción).

Este tipo de algoritmos no sustituyen a la norma, obviamente, sino que la traducen para facilitar su aplicación. Cuando un funcionario crea una hoja Excel en la que introduce los datos y efectúa los cálculos necesarios para, por ejemplo, liquidar los intereses de un justiprecio expropiatorio, está utilizando un algoritmo. En este caso, claramente no es necesario que la norma prevea o autorice la creación y aplicación del algoritmo. Por otro lado, sus posibles errores (es decir, la infidelidad en la traducción de la norma, por la eventual falta de incorporación al mismo de algunas de las opciones contempladas por ésta, o porque exista algún defecto que dé lugar a un resultado incorrecto o sesgado) darán lugar a la invalidez de sus resultados, porque lo único que importa y que tiene validez jurídica es la norma, no el algoritmo. Una liquidación tributaria preparada por un algoritmo pero que no se ajusta a la legislación aplicable es, obviamente, contraria a Derecho y así tendrá que declararse en cualquier procedimiento de impugnación, sin que tenga la menor relevancia que el error haya surgido al programar el algoritmo o al introducir los datos (en una operación manual de un funcionario).

En la práctica pueden surgir problemas, en la medida en que, por razones jerárquicas, los funcionarios se vean obligados a utilizar una aplicación que no se ajuste al marco jurídico. Ocurre a veces que el algoritmo está mal diseñado y calcula erróneamente el resultado o que no permite incorporar datos que son jurídicamente relevantes en la aplicación de la norma. Puede suceder que, de hecho, la comodidad del algoritmo induzca a sus usuarios a no comprobar la corrección del resultado, de forma que, aunque el algoritmo no prevalece sobre la norma, y los resultados que no se ajusten a la norma sean ilegales, en muchos casos prevalezca el algoritmo sobre la Ley. Todo indica que en estos casos el problema no es acceder al código del programa, sino conseguir que se aplique la norma por encima del error del algoritmo.

Este tipo de algoritmos se utilizan con frecuencia y a veces han llegado a los tribunales. Ya hace bastantes años se utilizaban programas informáticos para efectuar sorteos, por ejemplo, para determinar los tribunales que habían de juzgar los concursos de acceso a plazas de profesorado universitario. El programa permitía automatizar un proceso

(el sorteo) que es totalmente reglado pero que puede tener cierta complejidad porque los distintos miembros del tribunal proceden de conjuntos o colectivos diferentes. Algo así sucede en el programa utilizado para elegir, de entre los profesores solicitantes, a los miembros de los tribunales de las pruebas de acceso a la universidad, que en Cataluña ha dado lugar a una resolución de la autoridad de transparencia. (Comissió de Garantia del Dret D' Accéss a la Informació Pública [GAIP], 21 de setiembre de 2016). En esta misma línea, en Italia varias sentencias han anulado las resoluciones del concurso de trasladados de personal docente, que era decidido en aplicación de un algoritmo que "casaba" las diferentes solicitudes, supuestamente en aplicación de los criterios previstos en las normas.⁴ En España, un ejemplo reciente y muy polémico se ha producido en relación con el proceso de elección de plazas de formación como Médicos Internos Residentes (MIR). Estas plazas se asignan en función de la puntuación obtenida en un examen previo, por lo que se trata de un proceso perfectamente reglado. En 2020, se acordó, mediante Orden ministerial, que el proceso de elección no se haría de forma presencial (los aspirantes eligen por orden de puntuación), sino telemática (en años anteriores el aspirante podía optar entre la elección personal o telemática), lo que significa que los aspirantes presentarán una lista de peticiones y el programa hará la asignación en función de su puntuación. Aunque el sistema es, en principio, equivalente, otorga menos capacidad de elección a los aspirantes, que en la vía presencial pueden, por ejemplo, dejar pasar a otros aspirantes para poder elegir a la vez que una persona con quien quieran hacer la residencia, y tienen la garantía de conocer, en el momento de la elección, qué plazas están a su disposición, en lugar de formular al principio una serie de peticiones hipotéticas. Formulado recurso, el Tribunal Supremo concedió, en primer lugar, la suspensión cautelar (por lo que el sistema telemático no se aplicó) y después anuló la Orden, básicamente por razones formales (rango normativo), en sentencia de 13 de abril de 2021 (recurso 150/2020). Otro ejemplo es el programa "Euphemia", con el que, en el mercado eléctrico europeo, se casa la oferta y la demanda y se fijan los intercambios que deben producirse en cada momento entre los distintos sistemas nacionales para que el precio sea óptimo.⁵ También en relación con la electricidad, pero ahora no para determinar el precio en un mercado, sino para aplicar la norma que establece los requisitos para disfrutar del bono social, debe mencionarse el programa creado por el Ministerio competente, que en este momento es objeto de un recurso contencioso-administrativo en el que se solicita su difusión pública.⁶

A veces el algoritmo está en la propia norma, cuando ésta especifica la fórmula que debe aplicarse para llegar al resultado final: por ejemplo, en revisiones de precios (contratos), actualizaciones de tarifas (concesiones) o, con frecuencia, para la distribución de recursos escasos (ponderación de notas y otros méritos para la asignación de becas, por ejemplo). En estos casos se trata de algoritmos en el sentido de fórmulas o baremos que establecen la consecuencia jurídica a partir de un determinado supuesto de hecho, y es indiferente el modo técnico en que se aplique la fórmula (elaboración de una aplicación informática, aplicación de la fórmula a cada caso concreto por un funcionario, etc.).

4 Resoluciones del TAR de Lazio, de 10 de septiembre de 2018 (número 9227) y del Consejo de Estado decisión 2270/2019, publicada el 8 de abril de 2019). Serán analizadas *infra*.

5 Una descripción en <https://www.n-side.com/pcr-euphemia-algorithm-european-power-exchanges-price-coupling-electricity-market/>.

6 Se trata del procedimiento ordinario 18/2019, ante el Juzgado Central de lo Contencioso-Administrativo número 8.

2. CÓMO FUNCIONAN LAS PREDICIONES BASADAS EN DATOS (“MACHINE LEARNING”)

En realidad, el fenómeno realmente novedoso no son los algoritmos, sino las predicciones basadas en datos, que constituyen el producto o resultado de un tipo determinado de algoritmos que podemos denominar algoritmos predictivos.

Es imprescindible una visión, aunque sea sintética, de qué son y cómo funcionan las previsiones basadas en datos⁷. En esencia, se trata de analizar -con la utilización de algoritmos- grandes cantidades de datos relativos a un determinado fenómeno, para extraer correlaciones que nos lleven a producir, como resultado final, predicciones de hechos futuros.

Pensemos en el ejemplo del crédito, de la actividad de otorgamiento de préstamos. Toda entidad financiera intenta evitar la morosidad, porque cada préstamo no devuelto reduce sus beneficios. En el modelo tradicional, la decisión de conceder -o no- financiación se basa en múltiples criterios, algunos de los cuales están establecidos formalmente (por ejemplo, no estar incluido en una lista de morosos, o disponer de una garantía inmobiliaria o de un contrato de trabajo) mientras que otros son informales, puesto que la decisión final queda en manos de empleados que tendrán en cuenta todo tipo de “impresiones”. En definitiva, se trata de una mezcla entre criterios “razonados” (es decir, explicables racionalmente) y criterios subjetivos (el “ojo clínico” del empleado, que puede perder su prestigio dentro de la empresa si una operación importante resulta fallida).

El nuevo enfoque basado en los algoritmos parte de analizar una gran cantidad de datos (=big data) sobre operaciones anteriores (fallidas y exitosas). Datos relativos a los prestatarios (edad, profesión, titulación académica, domicilio, nivel de renta, hábitos de consumo, historial crediticio, etc.) y a las operaciones realizadas (capital, plazo, canal de comunicación con el cliente, tiempo dedicado a la negociación...). A veces los datos proceden del propio banco o son suministrados por el cliente al solicitar el préstamo, pero también pueden proceder de terceros (aseguradoras, empresas energéticas, de telecomunicaciones, redes sociales, etc.). Cada dato está “etiquetado”, es decir, sabemos qué personas han pagado sus créditos y cuáles otras no lo han hecho, de modo que cada dato personal (haber visitado determinada página, haber terminado el doctorado) se corresponde con haber demostrado solvencia o no haberlo hecho. Dicho de otro modo: tenemos miles de datos de las operaciones que han salido bien y de las que han salido mal. A partir de aquí, el algoritmo “remueve” esos datos, cruzándolos una y otra vez en todas las direcciones posibles, para establecer correlaciones. Algunas pueden ser más o menos obvias (a mayor nivel de renta del prestatario, más probabilidad de que se devuelva el préstamo), pero otras no tanto (por ejemplo, puede existir una correlación entre haber tenido muchos siniestros de tráfico comunicados a la aseguradora, y no pagar un crédito).

Otro ejemplo muy gráfico es el aprendizaje de idiomas. En el sistema tradicional, se aprenden las reglas de la gramática y de la pronunciación (previamente inducidas por expertos filólogos a partir del uso hablado y escrito del idioma), así como una cantidad suficiente de vocabulario, y de ese modo se aprende a formular frases correctas. Con

7 De entre los múltiples textos no jurídicos que pueden servir para obtener esa introducción, cabe citar MAYER-SCHÖNBERGER, V.; CUKIER, K., *Big data. La revolución de los datos masivos*, Turner, Madrid, 2013 (el libro original también se publicó en 2013) y LEE, K. F., *AI Superpowers. China, Silicon Valley and the New World Order*, Houghton Mifflin Harcourt, Boston-New York, 2018.

algoritmos predictivos se puede crear un traductor de un idioma a otro por una vía distinta. Se le proporciona al sistema un corpus enorme de textos escritos en los dos idiomas (por ejemplo, todos los textos normativos de la UE, que están publicados en todos los idiomas oficiales y se sabe que son equivalentes), de forma que, tras cruzar todos esos textos con la ayuda de algoritmos, el ordenador descubre, por ejemplo, a qué palabra inglesa equivale cada palabra española cuando aparece en un contexto determinado, y así puede ofrecer la correspondiente traducción. Como vemos, es el mismo método que permitió descifrar el lenguaje jeroglífico egipcio a partir de la piedra Rosetta, pero a una escala enorme, de modo que tanto la gran cantidad de datos utilizados como la entrada en juego de algoritmos nos permiten prescindir (hasta cierto punto) de Champollion.

Estos modelos son muy complejos y lo normal es que tengan en cuenta muchas variables, no sólo una. El resultado final es que, combinando todos los factores que se ha observado que tienen una correlación con la solvencia o, dicho de otro modo, que ayudan a predecir si el crédito será devuelto o no, y combinándolos entre sí en la proporción que resulta del modelo, obtenemos una "fórmula" que se puede aplicar a quien solicita un préstamo. Así, introduciendo los datos relevantes de esa persona (su titulación académica, su historial asegurador, etc.), obtendremos un resultado que nos indicará su propensión a ser buen o mal pagador, y ese dato podrá ser tenido en cuenta para conceder o denegar el crédito.

En unos casos, la decisión será automática (es decir, sin intervención humana) a la vista del resultado que proporciona el algoritmo, mientras que en otros ese resultado será una especie de "informe" que un humano (el encargado de tomar la decisión) tendrá en su mano y al que dará la importancia que considere adecuada.

Lógicamente, la predicción está sujeta a error, puesto que se basa en un modelo matemático que puede estar mal construido y que además depende de unos datos que pueden no predecir adecuadamente el futuro, como sucede, por ejemplo, si se producen cambios importantes desde el momento del que proceden los datos al momento en que hay que aplicar la predicción (por ejemplo, si intentamos predecir la evolución del PIB de 2020 con un modelo que funcionó en años anteriores pero que no tiene en cuenta el COVID-19). En el mundo real eso no es un problema: sencillamente, si las predicciones no funcionan dejan de ser usadas y se les hace el mismo caso que a los horóscopos publicados en los periódicos o a los sesudos gráficos que intentan predecir las cotizaciones bursátiles, que con frecuencia tienen el mismo grado de fiabilidad. El problema surge con las predicciones que no pueden ser verificadas. Por ejemplo: si el algoritmo recomienda otorgar un préstamo a una empresa y ésta no lo devuelve, queda claro que el algoritmo falla, y si los fallos abundan, dejará de utilizarse. Pero si el algoritmo recomienda no conceder un préstamo a una persona, y efectivamente no se le concede, es más difícil saber si el algoritmo ha fallado o no, porque no podemos saber si esa persona habría devuelto el crédito. Esto puede producir situaciones de indefensión (para quienes, por seguir el ejemplo, no reciben préstamos pese a que podrían haberlos devuelto). A la vez, como hay situaciones excepcionales que, precisamente por su excepcionalidad, no se tienen en cuenta en los cálculos, y con las que no se cuenta porque no suceden casi nunca y llegan a ser olvidadas, parece que el algoritmo es infalible y que se puede confiar ciegamente en él, lo que puede llevar a un exceso de confianza injustificada que a veces produce resultados catastróficos.⁸

8 En general, sobre la confianza en modelos matemáticos no comprobables que se utilizan para ganar seguridad en la toma de decisiones de riesgo, y los peligros a que puede llevar esa confianza (verificados, sin ir más lejos, en la crisis económica de 2008 y ahora en el caso del coronavirus), es fundamental la referencia a TALEB y su tetralogía *Incerto*, de entre la que

Podemos poner algunos ejemplos jurídicos. El programa COMPAS es uno de los más utilizados en Estados Unidos por los tribunales para determinar si se concede o no la libertad provisional (bien en la propia sentencia, o después). El programa analiza múltiples criterios que se supone que ayudan a predecir si un sujeto va a ser reincidente o no. No se trata de un “baremo” al uso, porque no son criterios establecidos en una norma, sino que han sido deducidos por un algoritmo a partir de experiencias anteriores, y están sujetos a modificación en función de los nuevos datos que se suministren. Una conocida sentencia del Tribunal Supremo de Wisconsin (asunto Loomis) acepta que los tribunales utilicen el informe suministrado por este programa para determinar sus sentencias, siempre que lo hagan junto con otros criterios. (Tribunal Supremo de Wisconsin, 13 de julio de 2016). En la Administración penitenciaria autonómica catalana se utiliza un programa muy parecido, denominado RISCANVI, para otorgar o denegar permisos penitenciarios, y existe una abundante jurisprudencia que, en sentido muy similar a la sentencia de Wisconsin, considera que se puede utilizar el resultado que arroja el programa RISCANVI para motivar la resolución (aunque no se conozca su contenido exacto), siempre que se puedan utilizar también otros factores y someter a crítica ese resultado.⁹ Es muy frecuente que las Administraciones encargadas de perseguir el fraude o el incumplimiento de normas, utilicen, incluso sin que una norma lo prevea o autorice, aplicaciones que, analizando datos, ayuden a descubrir casos en los que se pueda estar cometiendo un fraude y sea conveniente iniciar un procedimiento.¹⁰ No sólo eso, sino que hay Leyes que prevén la utilización de ese tipo de sistemas para detectar casos en los que pueda ser procedente la iniciación de un procedimiento.¹¹ Recientemente, el Tribunal de Distrito de

cabe destacar *El cisne negro* (el libro original es de 2007, la traducción española se publicó en Paidos, 2008) y la última parte, *Skin in the game*, Random House, New York, 2018.

- 9 Sobre el programa RISCANVI, FÉREZ-MANGAS, D.; ANDRÉS-PUEYO, A., “Eficacia predictiva en la valoración del riesgo del quebrantamiento de permisos penitenciarios”, *La Ley Penal*, 1342 (2018), así como la entrevista <http://www.fbg.ub.edu/es/actualidad/antonio-andres-pueyo-reto-riscanvi-detectar-que-interno-tiene-alto-riesgo-reincidencia/> (20 de enero de 2020). Como ejemplos de aplicación jurisprudencial pueden citarse los autos de la AP de Girona de 16 de noviembre de 2018 (recurso 890/2018) y 20 de diciembre de 2018 (recurso 974/2018). En ambas se lee: “ya hemos dicho en otras ocasiones que la forma que creemos más oportuna para valorar el RISCANVI no es la consistente en enmascarar los resultados ofrecidos por el algoritmo de manera automática tras la introducción de los datos de los que el test se compone, sino la de proporcionar posteriormente una explicación acerca de la fiabilidad de dichos datos, que creemos que se produce aludiendo a los meritados factores estáticos que no varían pese al transcurso del tiempo, por lo que las tendencias serán siempre medias o altas. Así ocurre en este caso por cuestiones relativas a los numerosos delitos cometidos de la misma tipología y por la existencia de una causa fundada en la drogadicción”.
- 10 De este tipo de aplicaciones nos enteramos con noticias como <https://www.lne.es/noticias-suscriptor/economia/2018/08/26/arsenal-algoritmos-fraude/2338570.html> (26 de agosto de 2018), https://blogs.elconfidencial.com/economia/big-data/2018-07-14/patrones-comportamiento-voracidad-fiscal_1592433/ (14 de julio de 2018), entre otras.
- 11 Un ejemplo es la Ley de la Comunidad Valenciana 22/2018, de 6 de noviembre, 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. Se regula un sistema de alertas (artículo 17) que básicamente analiza la información que tiene la propia Administración autonómica, y la que sus titulares hayan proporcionado libremente en internet (por ejemplo, mediante su participación en redes sociales), y suministra datos que pueden servir para la iniciación de una actuación de investigación (artículo 30). Sobre esta Ley, pronosticando su posible inconstitucionalidad a partir de la sentencia holandesa que se cita en la nota siguiente, COTINO, L., “«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*, Wolters Kluwer, 4 (2020).

La Haya ha decidido que un sistema similar (denominado SYRI) es contrario al derecho a la intimidad reconocido en el artículo 8 del CEDH.¹²

Veíamos antes cómo, en la forma “tradicional” de tomar decisiones, los criterios son, o bien racionales (es decir, criterios basados en algún razonamiento, algún principio) o bien irrationales, subjetivos (el “ojo crítico”, la “sana crítica”, etc.), a los que se recurre cuando se considera que hay factores imposibles de racionalizar, y que normalmente tienen como consecuencia que la decisión se encomienda a personas muy concretas que tienen la formación y/o la experiencia que supuestamente las convierte en idóneas para tomar esa clase de decisiones.¹³

En el mundo de los algoritmos predictivos y las predicciones basadas en datos, esto cambia por completo. Desaparecen las decisiones subjetivas o irrationales, siendo sustituidas por predicciones basadas en correlaciones descubiertas analizando gran cantidad de datos referidos a operaciones anteriores. Pero también son desplazados los criterios “racionales”, derivados de principios o argumentos, porque las predicciones algorítmicas sustituyen la causalidad por la correlación.¹⁴

Este es un punto fundamental al que es imprescindible prestar más atención. Estamos acostumbrados a que las decisiones se tomen en función de criterios razonados, aplicables, lo que nos remite a juicios de causalidad o de tipo normativo. Se opta por un determinado camino porque nos llevará al objetivo al ser el más coherente con los principios que se aplican en esa actividad, el recomendado por “la doctrina”, el que resulta de “la teoría”, etc. En cambio, los algoritmos predictivos suponen una nueva perspectiva. Simplemente se analiza el pasado (gran cantidad de datos referidos a experiencias anteriores, de las que sabemos qué resultado produjeron) y se extraen correlaciones, es decir, se identifica (automáticamente) qué características o grupos de características han llevado a los mejores resultados, y se toman esos criterios como base para las decisiones.¹⁵ Un ejemplo de aplicación de esta técnica es la creación de tests “baratos” o “sucios” para la detección de enfermedades o de otro tipo de situaciones, que, en lugar de identificar el patógeno o el hecho en sí que se está buscando (lo que puede ser caro), buscan otros datos que “normalmente” coinciden con aquel.¹⁶

-
- 12 Sentenciade5defebrero de 2020 del Tribunal de Distrito de La Haya (ECLI:NL:RBDHA:2020:1878). El texto, con enlace a la versión en inglés, es accesible en <https://uitspraken.rechtspraak.nl/iniendiendum? id=ECLI:NL:RBDHA:2020:865>.
- 13 Para una revisión crítica de esa confianza en “el sentido común”, el “ojo clínico” y otras expresiones con las que se proporciona cobertura o justificación a la confianza en la decisión no objetivable de los expertos, KAHNEMAN, D., *Thinking, fast and slow*, Penguin, 2012 (el libro se publicó originalmente en 2011; hay traducción española: *Pensar rápido, pensar despacio*, Debate, 2012), especialmente, capítulos 18 y 22.
- 14 Como explican en detalle MAYER-SCHÖNBERGER, V./CUKIER, K., *Big data*, cit., págs. 69-94.
- 15 Por lo demás, *nihil novum sub sole*. En cierto modo, triunfa la tesis del filósofo escocés David HUME (1711-1776), que consideraba que la causalidad no existe, sino que es una ilusión creada a partir de las correlaciones, que son lo único realmente observable. “Según él, la conexión causal no significa sino una relación de coexistencia y sucesión. Cuando un fenómeno coincide repetidas veces con otro o lo sucede en el tiempo, llamamos, en virtud de una asociación de ideas, al primero, causa, y al segundo, efecto, y decimos que este acontece porque se da el primero. La sucesión, por muchas veces que se repita, no nos da la seguridad de su indefinida reiteración, y no nos permite afirmar un vínculo de causalidad en el sentido de una conexión necesaria” (MARIAS, J., *Historia de la Filosofía*, Alianza, Madrid, 1993, 3^a ed., págs. 250-251).
- 16 Como se hizo por distintos grupos de investigación en relación con el Covid-19, sobre todo cuando los tests eran muy caros y escasos: <https://www.elcomercio.es/sociedad/disenan-modelos-que-convierten-los-pruebas-de-covid-en-sucios-08042020-0001.html>

Este nuevo camino puede llevar -y lleva- a que aparezcan nuevas opciones en las que nadie había pensado o en las que nadie habría pensado, porque las ocultaba inconscientemente el modo de pensar tradicional o el "marco" conceptual comúnmente aceptado. Un ejemplo frecuentemente mencionado es el algoritmo "AlphaGo" (creado por Deepmind, una compañía crucial en el desarrollo de los algoritmos predictivos que ahora pertenece a Google), que en 2017 venció al considerado mejor jugador de go del mundo (el go es un juego oriental, que hace algunos años se popularizó en occidente en una versión simplificada con el nombre comercial de Othello). A este programa no se le "enseñó" a jugar al go, al modo de los programas que juegan al ajedrez desde los años 80 (y que también han ganado a grandes jugadores). A "AlphaGo" se le suministraron millones de partidas (de las que se sabe, obviamente, quién ganó), para que, "revolviendo" esos datos con algoritmos, detectase cuáles eran o podían ser las opciones que llevan al triunfo con mayor probabilidad. El programa opera -no hace falta decirlo- sin prejuicios, y utilizaba jugadas por las que era muy poco probable que un jugador usual hubiese optado.¹⁷ Por eso se habla de "aprendizaje supervisado" (*supervised learning*) en el caso de los antiguos programas que jugaban al ajedrez (a los que no sólo se les programaban las reglas del juego, sino que se les indicaba cuáles eran las mejores jugadas ante los distintos escenarios posibles), frente al "aprendizaje no supervisado" (*unsupervised learning*) de los actuales algoritmos predictivos, porque (tomando una vez más el ejemplo de "AlphaGo") es "el ordenador" el que, aplicando el algoritmo, consigue, a partir del análisis de millones de partidas, identificar las mejores jugadas, es decir, aquellas que ofrecen más probabilidades de llevar a la victoria. De aquí la expresión *machine learning* (aprendizaje "mecánico", es decir, "no humano"), porque, una vez puesto en marcha el mecanismo, el sistema "aprende solo", sin necesidad de guía.¹⁸

inteligencia-artificial-coronavirus-rafiografia-torax-20200415135337-nt.html, <https://comunicacion.jcyl.es/web/jcyl/Comunicacion/es/Plantilla100Detalle/1284877983892/NotaPrensa/1284946083306/Comunicacion>. Un ejemplo reciente es la divulgación por la empresa Deep Mind de un "mapa" de las proteínas humanas (<https://elpais.com/ciencia/2021-07-22/la-forma-de-los-ladrillos-basicos-de-la-vida-abre-una-nueva-era-en-la-ciencia.html>) o la puesta a disposición de la comunidad científica, por un equipo liderado por Nuria López-Bigas, de la Universidad de Barcelona, de otro "mapa" de las mutaciones causantes de los distintos tipos de cáncer (<https://elpais.com/ciencia/2021-07-28/un-sistema-de-inteligencia-artificial-identifica-las-mutaciones-causantes-del-cancer-para-cada-tipo-de-tumor.html>). En ambos casos, la inteligencia artificial ha permitido llegar a esas conclusiones de forma mucho más rápida que por los procedimientos experimentales habituales.

- 17 En el mundo del deporte real también se producen cambios cualitativos de este tipo, que suponen una ruptura con la *lex artis* (aplicado este concepto con un significado diferente al habitual en responsabilidad civil médica). Como ocurrió, por ejemplo, cuando en los Juegos Olímpicos de México de 1968 Dick Fosbury saltó de espaldas en la prueba de salto de altura. Hasta ese momento todos los saltadores lo hacían hacia delante (utilizando la técnica del "rodillo ventral"), y se iban produciendo variantes o mejoras en el salto, pero siempre dentro del "marco conceptual" de hacerlo hacia delante. A quien comenzaba a practicar ese deporte se le enseñaba a saltar así. Una vez que Fosbury abrió ese nuevo camino, todos los siguieron porque se vio que permitía saltar más alto. Otro ejemplo (en este caso es un ejemplo de experimento innovador, aunque no es un cambio que se haya impuesto triunfalmente): en 2015, el tenista Roger Federer comenzó a restar a media pista, en lugar de hacerlo desde el fondo, que es lo habitual. No es algo que se haya universalizado (de hecho, el interés del movimiento radica en que se realiza por sorpresa, cuando el contrario está mirando hacia arriba para sacar), pero también es un ejemplo de movimiento que puede ser eficaz, pero en el que normalmente ni siquiera se pensaría porque se sale de lo usual.
- 18 En estos momentos existe una "nueva frontera" que es el *reinforcement learning*, que no deja de ser una aplicación del conductismo al *machine learning*, en el que se combina el "aprendizaje automático" a partir del análisis de un altísimo número de experiencias, con la introducción

Podría discutirse si este cambio (de causalidad a correlación) es tan radical. En la mayoría de actividades ya se opera de forma empírica o experimental. La medicina moderna, por ejemplo, no prescribe diagnósticos o remedios en función de una visión filosófica del cuerpo humano, sino en función de la observación de los síntomas, que ha llevado a identificar y describir enfermedades y sus correspondientes tratamientos (basados también en la observación de su eficacia).¹⁹ De todas formas, la aplicación de algoritmos predictivos introduce cambios importantes incluso en estos casos, porque se tiene en cuenta una cantidad de datos superior a la que puede procesar un analista humano y, además, el análisis de esos datos se realiza por un procedimiento “automático” (es decir, por un ordenador), lo que elimina los sesgos o prejuicios que podría tener un analista humano.²⁰

Precisamente en el Derecho son mayores las posibilidades de los algoritmos (o, dicho de otro modo, su aplicación supone un cambio mayor), en la medida en que las decisiones no suelen tomarse en función de criterios empíricos (derivados de correlaciones), sino normativos.²¹

3. INTELIGENCIA ARTIFICIAL

Inteligencia artificial, digitalización y automatización son etiquetas diferentes, aunque frecuentemente se confunden. A grandes rasgos, la digitalización supone la utilización de tecnologías de la información y las comunicaciones (TIC) para los procesos administrativos, sustituyendo al papel. Afecta, en primer lugar, a la comunicación entre la Administración

de incentivos para los resultados más acertados. Con ello se intenta reducir el tiempo de aprendizaje, es decir, evitar que el sistema tenga que probar todas las combinaciones posibles y se encamine con más rapidez al territorio en que se manifiestan resultados prometedores.

- 19 Con independencia de la inteligencia artificial, existe una tendencia conocida como “medicina basada en la evidencia” (*evidence-based medicine, EBM*), que supone, básicamente, que la prescripción de remedios o tratamientos se basa en un análisis estadístico de los resultados, que lleva a marginar algunos tratamientos o a privilegiar otros, con independencia de su mayor o menor justificación teórica o fisiológica, únicamente en función de su eficacia para la curación o mejora del paciente, medida con procedimientos estadísticos.
- 20 Se ha destacado que las predicciones basadas en *big data* suponen un cambio importante frente a los procedimientos estadísticos usuales porque éstos se basan en “muestras”, es decir, en una selección de entre los datos disponibles, debido a que con los métodos tradicionales era imposible manejar todos los datos. La superación del muestreo reduce las posibilidades de error o de distorsión de los resultados. Vid. MAYER-SCHÖNBERGER, V.; CUKIER; K., *Big data*, cit., págs. 49-68.
- 21 Pensemos en un ejemplo concreto: la acreditación de profesores universitarios. El sistema actual utiliza un baremo (como forma de reducir la discrecionalidad y sustituir los juicios de valor acerca de la “calidad” de los aspirantes), establecido en una norma (o, actualmente, en virtud de una norma, concretamente del Real Decreto 1312/2007, de 5 de octubre, por el que se establece la acreditación nacional para el acceso a los cuerpos docentes universitarios). El autor de la norma ha decidido (juicio de valor) cuáles son las características de un profesor ideal y puntuá a los aspirantes en función del grado en que las posean. Un algoritmo no predictivo sería una aplicación que calculase las puntuaciones a partir de los datos brutos curriculares (publicaciones, docencia, etc.). Ese algoritmo podría perfeccionarse de modo que pudiera importar los datos automáticamente de bases de datos sin necesidad de que el aspirante los introdujera en la aplicación. Un algoritmo predictivo creado para desarrollar esta misma función: (1) analizaría los datos de los profesores senior (es decir, los considerados mejores o más productivos de acuerdo con criterios previamente establecidos), (2) establecería qué características formativas o curriculares están asociadas a ese nivel de excelencia, y (3) identificaría, de entre los aspirantes, a los que reúnen esas características y por lo tanto es de prever que alcanzarán ese nivel.

y otros sujetos, pero también al archivo de los procedimientos. Provoca que quede un registro de toda la actuación administrativa en forma de datos estructurados que son la base para la posterior aplicación de inteligencia artificial. Anteriormente, ese registro quedaba en papel y no estaba estructurado, por lo que cualquier trabajo estadístico requería un esfuerzo adicional.

La automatización va más allá de la digitalización y sustituye al operador humano. Es un paso mucho menos frecuente, que de momento se limita, por razones comprensibles, a actos completamente reglados, que la Administración está obligada a dictar cuando se cumplan una serie de requisitos, y también, muy recientemente, a la iniciación de procedimientos sancionadores (Real Decreto-ley 2/2021, de 26 de enero, que modifica el texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre y texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, aprobado por Real Decreto Legislativo 5/2000, de 4 de agosto). La actuación administrativa automatizada requiere una previsión normativa previa, de conformidad con el artículo 41 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. No podría ser de otro modo, porque las Leyes atribuyen la potestad para dictar los distintos actos administrativos a órganos administrativos, cuyos titulares son personas físicas.

La inteligencia artificial suele entenderse, en este contexto, en el sentido de que las TIC llevan a cabo tareas que antes requerían la intervención humana, incluida la elaboración de todo o parte del contenido de una decisión administrativa. Normalmente se habla de inteligencia artificial cuando, a partir del análisis algorítmico de gran cantidad de datos, se puede ir más allá de la aplicación de las reglas que el programador ha fijado, y el programa crea nuevas reglas a partir de las correlaciones que descubre en los datos que se le suministran. Por ejemplo, los programas que, a partir del análisis de las infracciones detectadas en el pasado en un sector, predicen dónde es más probable que se estén produciendo infracciones, para que la Administración concentre allí el esfuerzo inspector.

La digitalización es condición necesaria de la automatización y la inteligencia artificial, pero no es condición suficiente. La “Administración electrónica”, tal como se regula en las Leyes 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y 40/2015, suele quedarse en digitalización. Por otro lado, automatización e inteligencia artificial son independientes entre sí: puede haber automatización sin inteligencia artificial (programas que realizan liquidaciones tributarias o que notifican denuncias por infracciones de tráfico detectadas con radar) e inteligencia artificial sin automatización (predicciones que sirven para que un inspector decida dónde acudir a inspeccionar, o que sirven para motivar la clasificación de un espacio como suelo no urbanizable debido a un riesgo de inundaciones establecido con un algoritmo).

Es obvio que el Derecho tiene que reaccionar ante la inteligencia artificial porque cambia algunos de sus presupuestos básicos, pero no es tan evidente cómo debe hacerlo.

La Administración y la jurisdicción, ahora o en el futuro próximo, tendrán diferentes relaciones con la inteligencia artificial: *utilizarla* en sistemas que faciliten sus procedimientos y la elaboración de sus decisiones (así como también el análisis de eficacia y eficiencia sobre las políticas públicas y las normas jurídicas), *controlar* su uso por la Administración (jurisdicción contencioso-administrativa) o por el sector privado (jurisdicción civil, autoridades de protección de datos), *contratarla* a través de distintas figuras de la legislación de contratos públicos (y con la importante discusión acerca del grado de transparencia que se exige a los productos que vaya a utilizar la Administración, que influye sobre los modelos de negocio) y *padecerla*, en la medida en que se utilizará

la IA para tratar de predecir el comportamiento de Administraciones y órganos judiciales y adelantarse a él, produciendo posibles distorsiones que obligarán a reformular los criterios o programas normativos de actuación administrativa o judicial.

A veces parece que los riesgos y los problemas sólo surgen cuando se sustituye al operador humano por una aplicación informática, y que la solución consiste en rechazar la sustitución y exigir la presencia humana. Pero la historia demuestra que la garantía para los ciudadanos nunca ha estado en la intervención de un humano, sino en el establecimiento de reglas que le vinculen. El Derecho ha servido siempre para controlar la actuación de los humanos, precisamente porque esa actuación humana es peligrosa. Lo más relevante no es quién actúe. Lo importante es cómo actúe y, sobre todo, que se pueda controlar esa actuación y garantizar que respete el programa normativo previamente establecido.

Tampoco podemos exigir a un algoritmo lo que no le pedimos a un humano. Por ejemplo, las decisiones de iniciación de procedimientos sancionadores, o, más aún, la decisión de inspeccionar (que para muchos ni siquiera supone iniciar un procedimiento administrativo), están sometidas a un control jurídico mínimo. El inicio de un procedimiento es un acto de trámite no recurrible, que puede basarse en causas muy variadas (empezando por la “propia iniciativa” del titular del órgano) y que, de hecho, no requiere ninguna justificación. En realidad, los tribunales relativizan el peso de los instrumentos que pretenden racionalizarlas (planes de inspección).²² No parece correcto que sólo se vean riesgos en ese tipo de decisiones cuando se utilizan algoritmos para intentar objetivarlas. El algoritmo puede tener sesgos (no por el propio algoritmo, sino por su programación o por los datos que se le suministran), pero al menos esos sesgos dejan huellas, mientras que los sesgos de los operadores humanos que deciden dónde inspeccionar o en qué casos iniciar un procedimiento, que también existen y son casi inevitables, no son tan fácilmente detectables o demostrables.

Como ya he explicado por extenso en otro lugar, el esquema básico para analizar jurídicamente el uso de la inteligencia artificial ha de ser detectar la función que cumple un determinado algoritmo o aplicación en el proceso de creación y aplicación del Derecho. Ese análisis sería similar a la “naturaleza jurídica” o a la calificación jurídica. Y en ese sentido (y dejando a un lado la aplicación ineludible de la normativa de protección de datos, en la que no puedo detenerme por falta de espacio), pueden avanzarse tres situaciones básicas:

- Algoritmos que traducen un régimen jurídico para facilitar la toma de decisiones por la Administración. Por ejemplo, programas que ayudan a liquidar un tributo, a calcular la subvención que le corresponde a una empresa en un determinado

22 Un buen ejemplo lo encontramos en la sentencia del Tribunal Supremo de 19 de febrero de 2020 (recurso de casación 240/2018). Un contribuyente impugnaba el resultado de una inspección tributaria alegando que el suyo no era uno de los supuestos en los que debía centrarse la actividad inspectora de la Administración según los programas oficiales aprobados y publicados: “La introducción de los planes de actuación, de Control, parciales, pueden tener la finalidad de facilitar a la Administración Tributaria su funcionamiento, especialmente mediante la aplicación de programas informáticos que permitan un tratamiento más ágil de la fiscalización de un determinado sector de contribuyentes, pero su previsión, quizás no muy acertada, en normas legales y reglamentarias, no puede traducirse sin más en un derecho subjetivo del contribuyente a no ser investigado si no se encuentra incluido en dichos planes y programas, pues ello supondría el incumplimiento por parte de la Administración del deber de fiscalización de que todos los ciudadanos cumplan con el deber de contribuir, previsto en el artículo 31.1 de nuestra norma constitucional”.

régimen de ayudas, la pensión de jubilación o la carga docente que tiene que asumir un profesor. Facilitan la actuación administrativa (ahorro de horas de trabajo humano, reducción de errores) pero no influyen en su contenido. Son programas que equivalen a una fórmula que traduce el contenido de la norma o de las bases que ha de aplicar la Administración (de hecho, algunas normas jurídicas o bases de licitaciones o de procedimientos selectivos ya describen su supuesto de hecho con una fórmula matemática). Lo más importante es que se puede (a efectos del control de lo que ha hecho la Administración) aplicar la norma “a mano”, *sin el algoritmo*, y comprobar si la aplicación algorítmica es correcta o no. El algoritmo no cambia el marco jurídico ni contribuye por sí mismo a determinar el contenido de la actuación administrativa, sino que es neutro. Si como consecuencia de un error en su configuración o aplicación, no lo es, el resultado será contrario a Derecho y será relativamente fácil detectarlo.

- Algoritmos que, como los anteriores, sirven para mecanizar o automatizar procesos reglados, sin cambiar su marco normativo, pero en los que el proceso es tan complejo que no se puede replicar sin el algoritmo, por lo que, en el momento de controlar la actuación administrativa, no se puede prescindir de él y es necesario verificar cómo ha funcionado. Es el caso de procesos complejos de asignación de recursos escasos (por ejemplo, concursos de trasladados con un alto número de funcionarios, como ocurrió en Italia, o la asignación de plazas MIR, que ya hemos visto que suspendida cautelarmente y después anulada por la Sala de lo Contencioso-Administrativo del Tribunal Supremo), en los que los resultados individuales están interconectados. El control jurídico de estas decisiones tomadas con ayuda de algoritmos no puede consistir en aplicar la norma “con lápiz y papel” para ver si coincide con la actuación realizada con ayuda algorítmica, sino que es necesario revisar el funcionamiento del algoritmo, lo que exigirá conocer todos los factores que contribuyen a determinar su resultado.
- Algoritmos de tipo predictivo, que contribuyen a orientar en una determinada dirección la actuación administrativa y que, a diferencia de los anteriores, aportan elementos decisionales propios. Esto sería inteligencia artificial en sentido estricto. Normalmente, su efecto es equiparable al de un baremo, que es una de las formas típicas de dirigir la acción administrativa, pero con la peculiaridad de que en este caso el baremo no lo fija una norma o una decisión administrativa de tipo no normativo (como un pliego de cláusulas administrativas particulares o las bases de un concurso), sino que lo determina el propio algoritmo a partir del análisis de casos precedentes. El algoritmo intenta conseguir un objetivo fijado por la norma (identificar a los estudiantes que se encuentren en riesgo de fracaso escolar, por ejemplo) y para ello crea una especie de retrato robot a partir del análisis de los datos de años anteriores. Las características concretas de ese retrato robot no las ha dibujado nadie, sino que las produce el modelo algorítmico. A día de hoy, ese tipo de modelos se aplican (sin habilitación normativa) como apoyo a decisiones de iniciación de procedimientos o, en un escalón inferior de formalización jurídica, para orientar el uso de los recursos públicos de bienestar o de inspección (por ejemplo, para identificar a personas a las que puede ser necesario seguir porque pueden estar en una situación de riesgo no detectada).²³ En la medida en que, en ausencia

23 El Ministerio de Trabajo ha adjudicado sucesivos contratos de servicios para dotarse de un servicio de “consultoría estratégica” que consiste, básicamente, en un modelo predictivo que apunte a empresas o supuestos en los que sea, en principio, más probable detectar infracciones

de algoritmo, esas decisiones carecerían, en la práctica, de control jurídico (no son actos administrativos discrecionales, sino actuaciones informales o actos de trámite), el peligro que se asume con la utilización de modelos algorítmicos es limitado, y también lo es la necesidad de regulación.

Una regulación es necesaria (y ya se está intentando a nivel europeo), y debería partir de las diferentes funciones jurídicas que puede desempeñar la inteligencia artificial.

4. PARÁMETROS JURÍDICOS DERIVADOS DE LA PROTECCIÓN DE DATOS

4.1 Pluralidad de perspectivas jurídicas sobre los algoritmos predictivos.

Los datos son uno de los tres elementos necesarios para la utilización de algoritmos predictivos, junto con los propios algoritmos y la capacidad de computación. No es sorprendente que las normas sobre protección de datos sean la primera respuesta jurídica al fenómeno.

No se trata, sin embargo, de la única. También existen otros títulos de intervención, que van desde el Derecho de la competencia (o de la competencia desleal), el del consumo o -por centrarnos en el uso que de estos algoritmos hacen las Administraciones Públicas- la regulación del procedimiento administrativo. El derecho fundamental a la protección de datos es sólo uno de los derechos del ciudadano que entran en juego en este campo, pero el particular también debe ser protegido en su condición de interesado en un procedimiento administrativo, lo que afecta a otros derechos (fundamentales o no) y a otros títulos de intervención del legislador, desde el derecho a la buena administración, el derecho a la tutela judicial efectiva y el mandato constitucional al legislador para la regulación del procedimiento administrativo (artículo 105).²⁴

En este sentido, es muy probable que se esté desplazando el centro de gravedad de algunas instituciones. Ciertas reglas o derechos pueden estar perdiendo importancia porque las nuevas técnicas de análisis de datos abren nuevas posibilidades de actuación para las Administraciones Públicas que les permiten eludir esas garantías. Pensemos en el derecho a no declarar contra uno mismo (o derecho a la no autoincriminación), recogido en el artículo 24.2 CE y aplicable tanto al proceso penal como a los procedimientos sancionadores, según una jurisprudencia constitucional y ordinaria bien conocida. La importancia práctica de esa regla disminuye a medida que aumenta la cantidad de datos libremente accesibles por la Administración que pueden servir para probar la comisión de infracciones o delitos. El “deber de colaboración” pierde relevancia cuando la Administración tiene a su disposición datos que no aporta el ciudadano en cumplimiento de ese deber, sino que voluntariamente va produciendo y “liberando” y que llegan a manos de la Administración.²⁵

(https://www.eldiario.es/economia/inspectores-trabajo-denuncian-externalizacion-empresa-privada-lucha-fraude_1_6304432.html).

- 24 En este sentido, CIVITARESE MATTEUCCI, S., “Umano troppo umano». Decisioni amministrative automatizzate e principio di legalità”, *Diritto pubblico*, 2019, págs. 5-41, pág. 23, que subraya que el RGPD sólo se ocupa del derecho a la protección de datos, pero no de otras perspectivas jurídicamente relevantes como el fundamento normativo necesario para que la Administración pueda actuar de forma automatizada.
- 25 Todo ello con independencia de los problemas prácticos que puedan surgir para que tales datos (por ejemplo, videos colocados por el presunto infractor -o por terceros- en redes sociales) produzcan efectos probatorios. Un análisis de estos problemas en la sentencia del Juzgado Central de lo Contencioso-Administrativo número 1 de 7 de julio de 2017 (recurso contencioso-administrativo 167/2016).

4.2 Los algoritmos funcionan, sobre todo, con datos anonimizados.

Otra advertencia importante, en la línea de relativizar la importancia del Derecho de protección de datos dentro del abordaje jurídico de los algoritmos, es que la normativa de protección de datos (fundamentalmente, el RGPD y la LO 3/2018) establece normas dirigidas a la utilización de datos personales, es decir, “información sobre una persona física identificada o identificable” (artículo 4), mientras que las predicciones algorítmicas se realizan, sobre todo, a partir de datos no personales.²⁶ Así, por ejemplo, para “entrenar” a un algoritmo que sirva para determinar la solvencia de potenciales solicitantes de préstamos sólo se necesita información sobre la ejecución de préstamos anteriores, pero se trata de información no personal porque no es necesario conocer el nombre y apellidos del prestatario, sólo aquellas notas de esa persona que puedan ser relevantes y, en particular, los datos relativos a si ha cumplido, o no, el contrato de préstamo. A partir de esos datos no personales (anonimizados) se hallarán correlaciones y se elaborarán perfiles que servirán para ayudar a decidir la concesión o denegación de una nueva petición de crédito. Por tanto, el peticionario de crédito sí aporta sus datos personales, que son analizados por la entidad financiera mediante un modelo algorítmico, pero esa aportación de datos no plantea problemas desde el punto de vista de la normativa de protección de datos, porque es una aportación consciente, consentida y legitimada por ese consentimiento y además por su necesidad para la celebración del contrato (artículo 6 RGPD). Pero el tratamiento de los datos anteriores queda al margen de la normativa de protección de datos porque no son datos personales. Es verdad que, como se ha observado reiteradamente, la anonimización puede fallar en casos concretos, en los que, por el escaso número de personas que se encuentren en una determinada situación, sea fácil identificar al sujeto que reúne esas condiciones. Pero se trata de excepciones y no podemos ignorar que la legislación de protección de datos acepta la anonimización como un procedimiento para eliminar el carácter personal de los datos y levantar algunas barreras a su tratamiento.²⁷

4.3 El consentimiento del interesado y sus debilidades.

En la práctica, la aplicación de las normas de protección de datos se ha traducido en la solicitud al interesado del consentimiento al tratamiento de sus datos, con carácter previo a la celebración de cualquier contrato o incluso a cualquier contacto comercial con una empresa, y, en especial, cuando se accede a cualquier página web o se utiliza cualquier aplicación. De hecho, también se exige ese consentimiento en los impresos de solicitud de participación en numerosos procedimientos administrativos, aunque se trata de un consentimiento “obligatorio” y, por tanto, no es un verdadero consentimiento.²⁸

-
- 26 Insiste en este argumento HOFFMANN-RIEM, W., *Big data. Desafíos también para el Derecho*, Civitas, Cizur Menor, 2018 (el original alemán también se publicó en 2018), pág. 107.
 - 27 Apartado 26 del preámbulo del RGPD: “los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo”.
 - 28 O se establece, en la convocatoria de que se trate, que la presentación de la solicitud “conlleva el consentimiento para la comunicación a otras administraciones públicas de los datos”, o “conlleva la autorización de la entidad solicitante para tratar dichos datos de manera automatizada y cederlos a los órganos de instrucción, evaluación, resolución, seguimiento y control competentes (...)” (artículo 15.13 de la Resolución de la Secretaría de Estado de Universidades, Investigación, Desarrollo e Innovación y de la Presidencia de la Agencia Estatal de Investigación de 13 de agosto de 2018, por la que se aprueba la convocatoria de tramitación anticipada para el año 2018 del procedimiento de concesión de ayudas a Proyectos de I+D+i «Retos investigación»

Las cláusulas de prestación del consentimiento (política de privacidad y protección de datos), no se leen por casi nadie, entre otras cosas porque se plantean como un paso previo a la utilización de una aplicación o a la obtención de una información en una página web, que son procesos a los que es inherente la celeridad. Dicho de otro modo: si los consumidores no siempre leen todas las cláusulas de los contratos que firman (a veces ni siquiera en el caso de los contratos firmados ante notario), aunque se les suministren con días de antelación a la firma, es ilusorio pensar que vayan a leer las cláusulas que actúan como paso previo al acceso a una página web o a la utilización de una aplicación, cuando la razón por la que se acude a la página o a la aplicación es precisamente por la rapidez con que pueden ser utilizadas, desde cualquier soporte (especialmente, el teléfono móvil) y sin más dilación. No digamos cuando se trata de aplicaciones que se descargan para solucionar una necesidad inmediata (pagar el aparcamiento, buscar rápidamente un hotel o restaurante, etc.).

Esta legislación de protección de datos que resulta desactivada por el consentimiento del interesado (es decir, que sólo obliga a pedir y obtener el consentimiento), además de resultar poco útil, utiliza una técnica que, en sectores similares como el Derecho de consumo, fue superada hace décadas. Tanto en el Derecho de los consumidores como en la protección de datos se parte del presupuesto de que existe una parte débil, que en el primer caso es el consumidor y en el segundo es el titular de los datos cuando se enfrenta a peticiones de consentimiento que son difíciles de gestionar (por su prolijidad) y que, si se le plantean como una condición necesaria para utilizar aplicaciones, pueden llegar a ser casi obligatorias, si la negativa le conduce a una especie de aislamiento o de renuncia a la tecnología. La respuesta del Derecho de consumo a esta situación ha sido, como es sabido, prescindir del dogma del consentimiento, es decir, afirmar que el hecho de que el consumidor haya firmado un contrato no es suficiente para que el mismo le vincule en su integridad, porque, si hay cláusulas abusivas, éstas son nulas a pesar del consentimiento del consumidor. Por eso, los *disclaimers* y los consentimientos que se aceptan antes de cualquier contrato electrónico tienen una importancia muy limitada *en lo relativo a las cláusulas contractuales* (dejamos a un lado en este momento la protección de datos, donde el consentimiento sí tiene una importancia decisiva) porque se aplica un control material, que expulsa las cláusulas abusivas.

El Derecho de la protección de datos camina en esta dirección, pero todavía lo hace muy lentamente. No existen apenas normas imperativas que prohíban determinados tratamientos de los datos a pesar del consentimiento del interesado. Y, aunque existen reglas para la prestación del consentimiento, que intentan evitar cesiones en blanco o una prestación del consentimiento que sea sólo una apariencia, la realidad muestra que ese consentimiento se sigue prestando de forma irreflexiva y en un contexto (el acceso a páginas o a aplicaciones) en el que priman la urgencia o la celeridad. Por lo tanto, en la práctica, buena parte de los límites legales se superan con facilidad gracias al consentimiento de los afectados.

Por otro lado, la tecnología ha facilitado a los usuarios la posibilidad de registrar todas sus actividades, lo que tiene muchas ventajas (pensemos en las pulseras de actividad que registran la práctica deportiva o la actividad física en general, las tarjetas y en general los pagos electrónicos, que permiten el control del gasto y evitan tener que archivar miles de documentos en papel, o la geolocalización y sus múltiples utilidades, etc.). Salvo excepciones, el ciudadano colabora voluntariamente y crea grandes cantidades de datos. Y se ha asentado un modelo económico en el que esos datos no tienen utilidad sólo para

correspondientes al Programa Estatal de I+D+i Orientada a los Retos de la Sociedad, en el marco del Plan Estatal de Investigación Científica y Técnica y de Innovación 2017-2020).

el ciudadano, sino también para las empresas, y con frecuencia es el potencial de esos datos lo que ha llevado a empresas a crear las aplicaciones que utilizan los usuarios.²⁹ La evolución de la tecnología no ayuda a la restricción en los consentimientos al tratamiento de datos, sino al revés.

4.4 Peculiaridades en el uso de datos por Administraciones Públicas.

Ya hemos visto, como un ejemplo de la aplicación de la normativa de protección de datos por las Administraciones, que hay convocatorias (por ejemplo, de becas o subvenciones) en las que se exige al peticionario que acepte expresamente el tratamiento de sus datos (sin opción de no hacerlo) o se establece en la propia convocatoria que la presentación de la solicitud conlleva la autorización o consentimiento para dicho tratamiento. El consentimiento del interesado es necesario para que la solicitud sea tramitada y se convierte, por tanto, en uno de los requisitos necesarios para obtener una resolución favorable. Esta técnica es inadecuada porque un consentimiento "obligatorio" es una contradicción. El consentimiento es innecesario porque el tratamiento de los datos se justifica en virtud de otros títulos jurídicos [una misión realizada en interés público por la Administración, artículo 6.1.e) RGPD].

Más allá de este ejemplo, es necesario tener en cuenta las peculiaridades del tratamiento de los datos cuando quien pone en marcha una aplicación es una Administración Pública o, en general, un ente que opera en régimen de Derecho administrativo (lo que incluye a los concesionarios y contratistas cuando lo hagan para gestionar una actividad pública que les haya sido encomendada). Incluso en el caso de que estemos hablando de actividades prestacionales y no de policía, y se trate de prestaciones de recepción voluntaria por el interesado, no podemos considerar libre el consentimiento cuando la negativa a prestarlo impide al ciudadano acceder a una prestación o supone renunciar a las ventajas derivadas de utilizar una aplicación en línea, y condonarse a utilizar formas de relación no electrónica. Por eso, en estos casos el tratamiento de datos que lleva a cabo la Administración ha de justificarse en normas que legitimen ese tratamiento en algún título distinto del consentimiento, y no (o no sólo) en el consentimiento de los afectados, y han de cumplirse, además, los límites y garantías específico (empezando por el principio de proporcionalidad).

4.5 Ambigüedad y casuismo.

La normativa sobre protección de datos tiene, por otro lado, debilidades evidentes. Una de ellas es la constante utilización de conceptos legales indeterminados, entre los que destacan los de "proporcionalidad" y "adecuación": en numerosos supuestos, la norma

29 Como explica ZUBOFF, S., *The age of surveillance capitalism*, Profile Books, London, 2019, pág. 5, la aparición de esta economía de los datos no era previsible (o al menos no fue prevista) cuando, hacia el año 2000, y ya en pleno auge de internet, comenzó a avanzarse en lo que sería el internet de las cosas, es decir, la domótica y demás posibilidades de manejar aparatos online. Los primeros proyectos suponían el control centralizado a distancia de múltiples mecanismos, pero sin que los datos fueran manejados o aprovechados por alguien distinto de su titular. Es lo mismo que sigue sucediendo, por ejemplo, con el control de grandes instalaciones (centrales energéticas, etc.), que también son manejadas por medios electrónicos y digitales, pero bajo el control del titular de la instalación. El gran cambio vino cuando, debido en buena medida a los avances de los algoritmos, se vio la utilidad económica de los datos agregados generados por millones de usuarios, y eso impulsó a muchas empresas a invertir y a generar aplicaciones gratuitas que han ganado el interés de los usuarios y son masivamente utilizadas por ellos, a cambio del "único" precio (que en buena medida es invisible o percibido como inocuo) de entregar sus datos.

permite una determinada conducta, siempre que sea proporcional y se apliquen garantías adecuadas (o bien, la prohíbe, salvo que concurra uno de los presupuestos habilitantes y se cumplan esos conceptos indeterminados). Esa forma de legislar produce inseguridad jurídica y supone que el autor de la norma abdica parcialmente de su labor, porque deja en manos del aplicador la tarea de ponderar distintos intereses o principios en juego, en lugar de tomar la decisión y establecer preferencias dentro de ciertos ámbitos o cuando se respeten algunos requisitos. El resultado final es, como he dicho, inseguridad jurídica y dificultad para predecir las decisiones que se tomen en los casos concretos.³⁰

Todo ello se une a los déficits de aplicación que se producen en esta materia, derivados de que con frecuencia el tratamiento de datos resulta invisible. Podemos discutir si las cláusulas con las que se solicita el tratamiento de los datos son adecuadas o no³¹, pero es mucho más difícil reaccionar cuando se produce una cesión de datos no autorizada, entre otras cosas porque muchas veces no es detectable: el ciudadano que resulta destinatario de una decisión tomada a partir de esa cesión de datos (con resultados favorables o desfavorables para él, según los casos), puede no enterarse de que la decisión ha sido tomada sobre la base de un previo análisis de datos.

Por otro lado, en éste como en otros sectores, parece bastante claro que las autoridades de protección de datos no tienen medios suficientes para imponer la aplicación de las normas por vía sancionadora, sobre todo en un contexto de innovación tecnológica.

30 Un ejemplo reciente lo encontramos en la sentencia del TJUE de 11 de diciembre de 2019 (asunto C-708/18, TK), que resuelve una cuestión prejudicial en un pleito iniciado por un vecino de un bloque de viviendas que se oponía a que la comunidad de propietarios instalara cámaras en el portal como medida de seguridad ante los robos que se habían producido. La sentencia rechaza la aplicación de algunas reglas que podrían haber resuelto con claridad el caso (por ejemplo, normas nacionales que prohíben sin excepciones el tratamiento de ciertos tipos de datos, o, en sentido contrario, que consideran que la comunidad, como gestora de las zonas comunes, pueda disponer sobre la instalación de cámaras), y opta por un modelo de ponderación en cuya virtud la conformidad a derecho de la decisión va a depender en cada caso de conceptos cuya aplicación última corresponde al juez, como la proporcionalidad, o de si existen otros medios menos invasivos para la intimidad que puedan conseguir la misma finalidad (algo similar al favor *libertatis*). El resultado es que se produce un brusco salto entre la enunciación de esos principios generales y la decisión concreta (que podía haber sido ésa u otra diferente, a partir de los mismos principios) y que ésta ni siquiera la toma el TJUE, sino que se remite al órgano que había planteado la cuestión: "Habida cuenta de las consideraciones anteriores, procede responder a las cuestiones prejudiciales planteadas que los artículos 6, apartado 1, letra c), y 7, letra f), de la Directiva 95/46, deben interpretarse, a la luz de los artículos 7 y 8 de la Carta, en el sentido de que no se oponen a disposiciones nacionales que autorizan la instalación de un sistema de videovigilancia como el controvertido en el litigio principal, colocado en las zonas comunes de un edificio de uso residencial sin el consentimiento de los interesados, con el fin de satisfacer intereses legítimos consistentes en garantizar el cuidado y la protección de las personas y de los bienes, si el tratamiento de datos personales mediante el sistema de videovigilancia de que se trata reúne los requisitos impuestos en dicho artículo 7, letra f) [es decir, "interés legítimo" perseguido por el responsable del tratamiento, que prevalezca sobre "el interés o los derechos y libertades fundamentales del interesado"], circunstancia que corresponde verificar al órgano jurisdiccional remitente".

31 La discusión sobre la conformidad a la normativa de protección de datos de las cláusulas de solicitud del consentimiento sí está presente en la jurisprudencia del TJUE. Un ejemplo reciente en la sentencia de 1 de octubre de 2019 en el asunto C-673/17 (Planet 49): "el consentimiento (...) 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".

Seguramente serán necesarios más mecanismos de aplicación de las normas, incluido el de contar con la colaboración de otros agentes, privados, que se especialicen en la detección de conductas infractoras y que las denuncien o ayuden a los perjudicados a ejercitarse en acciones civiles.³²

4.6 Reglas concretas sobre el uso de algoritmos: decisiones automatizadas.

A la luz de estas consideraciones, que ayudan a relativizar la importancia de la legislación de protección de datos en este contexto, vamos a analizar brevemente algunas de las normas más relevantes para la utilización de predicciones algorítmicas. Ya se ha indicado que lo más habitual es que se utilicen datos anonimizados para “entrenar” algoritmos, es decir, para poder elaborar perfiles o modelos y que, posteriormente, esos modelos se utilicen con los datos personales (éstos sí son personales, no están anonimizados) del interesado, para realizar alguna predicción respecto a él. En otros casos, los datos anonimizados con los que trabaja el algoritmo elaboran predicciones generales que no están dirigidas a ningún interesado en concreto, sino que sirven a la Administración para tomar medidas de organización (como ocurre con los datos generales anonimizados sobre movilidad de la población, que la Administración compra para poder obtener conclusiones que le sirvan para planificar sus políticas).

Como los datos con los que se elabora el modelo algorítmico están anonimizados, las previsiones de la legislación de protección de datos no les afectan o sólo de manera muy ligera. En cuanto a los datos del interesado respecto al que se va a tomar una decisión con apoyo en las conclusiones del modelo algorítmico, tampoco plantea demasiados problemas su tratamiento, porque los suministra él mismo y la legitimidad del tratamiento deriva de la función pública que desempeña la Administración [letras e), y, en su caso, c) y f) del artículo 6.1 del RGPD]. Por tanto, los problemas o los límites se van a plantear desde otros sectores del ordenamiento jurídico, más que desde el flanco de la protección de datos. Concretamente, una vez que el modelo algorítmico descubre una serie de correlaciones que permiten predecir un determinado resultado con cierta probabilidad, el problema es saber qué relevancia jurídica puede darse a esa predicción, y también si determinados factores, por mucho que se muestren relevantes en la práctica (es decir, aunque puedan ser indicativos de una correlación), pueden ser tenidos en cuenta o están vetados por ser discriminatorios. Pero son problemas distintos de la protección de datos, que se abordarán más adelante.

Mención aparte merece la regulación de las decisiones individuales automatizadas en el artículo 22 RGPD.³³ Comencemos por el ámbito de aplicación. La norma sólo se aplica a “una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles”. Ya sabemos que las predicciones algorítmicas son eso,

32 Sobre esta cuestión, HUERGO, A., “Las sanciones administrativas en el marco del *law enforcement*”, en ZEGARRA VALDIVIA, D. (Coord.), *La proyección del Derecho Administrativo Peruano. Estudios por el Centenario de la Facultad de Derecho de la PUCP*, Palestra, Lima 2019, págs. 515-539 (esp., págs. 532-538).

33 El artículo 22 (“Decisiones individuales automatizadas, incluida la elaboración de perfiles”) dispone:

“1. Todo 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.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

predicciones, que pueden ser seguidas o no por quien ha de tomar la decisión. Por tanto, esta regulación no afecta a todas las predicciones algorítmicas, sino que sólo opera en aquellos casos en que la predicción se integra en un sistema automatizado de toma de decisiones.³⁴ En la práctica, lo normal es que, si la decisión tiene una entidad económica suficiente, no se tome de modo puramente automático, sino que la predicción se integre como un elemento más de juicio. Pierde relevancia, por consiguiente, el artículo 22. Éste no aborda la esencia de los algoritmos predictivos, sino una de sus posibles formas de utilización.

En segundo lugar, el artículo 22 sólo se refiere a una decisión “que produzca efectos jurídicos en él [el interesado] o le afecte significativamente de modo similar”. De nuevo se restringe el ámbito de aplicación, porque lo normal (lo veremos más adelante) es que las predicciones algorítmicas sirvan para seleccionar objetivos a la Administración, para indicarle dónde puede ser necesario actuar (tanto en caso de actuaciones de gravamen, por ejemplo, sancionadoras, como favorables, por ejemplo, en servicios sociales), más que para determinar el contenido de la decisión. Es dudoso que esta clase de decisiones (que a veces ni siquiera se refieren a personas concretas, sino a grupos o a zonas), produzcan “efectos jurídicos en el interesado” en el sentido del artículo 22.³⁵ Sin embargo, la conocida sentencia SYRI del Tribunal de Distrito de La Haya, de 5 de febrero

-
- b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
 - c) se basa en el consentimiento explícito del interesado.
3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.
4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado”.
- 34 Sobre la relación entre decisiones automatizadas y uso de algoritmos, VAN ECK, M., “Algorithms in Public Administration”, entrada de blog publicada el 31 de enero de 2017 (<https://marliesvaneck.wordpress.com/2017/01/31/algorithms-in-public-administration/>).
- 35 Un documento relevante para la interpretación de este concepto podrían ser las “Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2017/679” adoptadas por el “Grupo de Trabajo sobre Protección de Datos del artículo 29” el 3 de octubre de 2017 y revisadas por última vez y adoptadas el 6 de febrero de 2018 (https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053). Aunque se analiza expresamente este concepto legal (páginas 23-25), parece claro que una decisión de inicio de un procedimiento no es una decisión “que produzca efectos jurídicos” para el afectado, y, en su caso, podrá entrar en la categoría de una decisión que “le afecte significativamente de modo similar”, aunque los ejemplos que se analizan se refieren todos al tráfico privado (publicidad online, aplicación de condiciones contractuales diferentes, denegación de crédito). Se detiene en esta cuestión HERNÁNDEZ, J. C., “Decisiones algorítmicas de perfilado: régimen y garantías jurídicas”, REDA, 203 (2020), págs. 281-322, esp. págs. 293-295. Los ejemplos que menciona, basándose en el documento que se acaba de citar, parecen corresponder a resoluciones, no a actos de trámite (ni “preparatorios de actos de trámite”): “la cancelación de un contrato, la denegación de entrada a un país, o la concesión o denegación de una prestación por una administración pública”. Parece considerar las circunstancias personales del destinatario de la decisión como un criterio para determinar si la decisión afecta a los derechos o no, lo que puede introducir una importante dosis de inseguridad.

de 2020, se basa, para declarar que dicho sistema de selección de posibles casos de fraude es ilegal, justamente en que los informes de riesgo "afectan significativamente" a los ciudadanos "de modo similar" a una decisión que produzca efectos jurídicos.³⁶

Al margen de estos problemas y dudas sobre el ámbito de aplicación, el artículo 22 constituye una buena muestra de las limitaciones de las normas de protección de datos. Establece, en resumen, una prohibición con excepciones. De las tres excepciones, dos tienen escaso desarrollo en Derecho público: el consentimiento (por lo que ya he dicho, es decir, porque aquí no debería considerarse suficiente en la mayoría de los casos) y el supuesto de que la decisión automatizada "es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento", pensado más para el Derecho privado (y este supuesto plantea, además, muchas dudas, porque no está claro cuándo "es necesaria" una decisión de este tipo para la celebración o ejecución de un contrato, pues normalmente es la conveniencia de una de las partes, no la necesidad, lo que impulsa la utilización de algoritmos). La otra excepción es una autorización normativa. Es decir: hace falta una habilitación normativa (no necesariamente legal) para que puedan adoptarse decisiones "basadas únicamente en el tratamiento automatizado" de datos personales, si se quiere que la decisión "produzca efectos jurídicos en él [el interesado] o le afecte significativamente de modo similar". A su vez, y como se adelantó hace un momento, no basta la habilitación normativa, sino que es preciso que se cumpla un requisito adicional que consiste en la adopción de "las medidas adecuadas para salvaguardar los derechos y libertades y los derechos y los intereses legítimos del interesado". Aunque esas "medidas adecuadas" son indeterminadas, su mínimo queda, sin embargo, perfectamente explicitado: "el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión".³⁷

Además, se establecen dos precisiones. La primera, que la decisión automatizada no puede basarse en las categorías de datos especialmente protegidos del artículo 9.1, de nuevo salvo excepciones entre las que se incluyen "razones de un interés público esencial".

La segunda, que, mediante Ley, se pueden establecer excepciones en los supuestos del artículo 23, que son muy amplios, y que incluyen algunos que parecen muy relacionados con algunas actividades típicamente administrativas, como "objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbito fiscal, presupuestario y monetario, la sanidad pública y la seguridad social", "la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas

36 Sentencia de 5 de febrero de 2020, apartado 6.59: "El hecho de un informe de riesgo no necesariamente lleve a posteriores investigaciones, ni a una sanción administrativa o penal, y que no puede ser utilizado como único fundamento jurídico de una decisión dirigida a hacer cumplir una norma [*enforcement decision*] no significa que no produzca efectos significativos en la vida privada del titular de los datos". Sobre esta sentencia, vid. el comentario muy favorable de COTINO, L., «*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*, Wolters Kluwer, 4 (2020).

37 Se trata de la "reserva de humanidad" que ha destacado la doctrina, pudiendo citarse, por todos, PONCE, J., "Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico", *Revista General de Derecho Administrativo*, 50 (2019). Desde otra perspectiva, OSWALD, M., "Algorithm-assisted decision-making in the public sector: framing the issues using administrative law rules governing discretionary power", *Philosophical Transactions of the Royal Society*, A, 2018, 376:20170359 (17).

deontológicas en las profesiones reguladas”, o “una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública (...).”.

El RGPD establece, así, que la actuación administrativa automatizada requiere una habilitación normativa, algo que el artículo 41 LRJSP no expresa con la misma claridad.³⁸ En Alemania, se exige una habilitación normativa para que puedan adoptarse actos administrativos de forma automatizada, con independencia de que se basen, o no, en predicciones basadas en datos.³⁹ En cambio, en Francia se exige que, cuando una decisión administrativa se tome sobre el fundamento de un “tratamiento algorítmico”, se informe de ello al ciudadano.⁴⁰ No importa si la decisión se adopta de forma automática o no; lo que es relevante es el uso de un “tratamiento algorítmico”. Y no se exige una base normativa para dicho tratamiento, pero sí se exige que se informe al ciudadano. Me parece una opción normativa más adaptada a la realidad.

5. EL PROYECTO DE REGLAMENTO SOBRE LA INTELIGENCIA ARTIFICIAL

Después de una consulta previa, un Libro Blanco y peticiones de otras instituciones como el Parlamento o el Consejo, la Comisión acaba de ejercer su competencia de iniciativa legislativa y ha formulado proyecto de Reglamento sobre “un enfoque europeo de la inteligencia artificial”.⁴¹

El proyecto define la IA como un software que, a partir del uso de técnicas matemáticas y de programación que se enumeran en el Anexo I (y que son lo que vulgarmente se entiende por “algoritmos”, aunque esta palabra tenga un significado más amplio, como ya sabemos), produce resultados que sirven para realizar predicciones, recomendaciones de decisiones futuras, etc.

El punto de partida de este futuro Reglamento es ya conocido: la IA es una oportunidad a la que no se puede renunciar porque permite ganar en eficiencia y porque *si no lo hacemos nosotros, lo harán otros*, y a la vez supone riesgos importantes, que van desde la posibilidad de que un sistema “inteligente” que controle una central energética o una máquina de tratamiento médico comience a funcionar mal y cause daños graves, a

-
- 38 Una cuestión en la que CIVITARESE MATEUCCI, S., «*«Umano troppo umano»*», cit., págs. 34 y sigs., es partidario de exigir no sólo habilitación normativa, sino una habilitación normativa específica para la adopción de un tipo concreto de decisiones automatizadas, no una habilitación general para la toma de decisiones automatizadas.
- 39 Mediante una Ley de 18 de julio de 2016, de modernización de los procedimientos tributarios, se introdujeron reformas en distintas Leyes y, concretamente, en la Ley de Procedimiento Administrativo (*Verwaltungsverfahrensgesetz -VwVfG-*) se introdujo un nuevo parágrafo, el 35 a, que dispone: “Se puede dictar un acto administrativo por medios totalmente automáticos, siempre que haya sido admitido por una norma y no exista discrecionalidad ni margen de apreciación”. Cuando el precepto habla de norma jurídica (*Rechtsvorschrift*), emplea una expresión técnica que incluye leyes y reglamentos, pero excluye lo que en Alemania se llaman reglamentos administrativos (*Verwaltungsvorschrift*), similares a circulares o instrucciones.
- 40 La norma se encuentra en la Ley de República Digital (Ley 2016-1321, de 7 de octubre), en su artículo 4 (que modifica el Código relaciones con la Administración, artículo L311-3-1): “Sous réserve de l’application du 2° de l’article L. 311-5, une décision individuelle prise sur le fondement d’un traitement algorithmique comporte une mention explicite en informant l’intéressé. Les règles définissant ce traitement ainsi que les principales caractéristiques de sa mise en œuvre sont communiquées par l’administration à l’intéressé s’il en fait la demande”.
- 41 <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206>

que se discrimine a personas en función de los "informes" que produzca un sistema de análisis inteligente de datos, o que se establezcan sistemas de vigilancia omnipresente de tipo "Gran Hermano". El riesgo consiste, en definitiva, en la posibilidad de que se causen daños que pueden afectar a la integridad o vida de las personas, daños materiales, impactos graves para la sociedad en su conjunto, o para actividades económicas de gran importancia, o distorsión en la prestación de servicios esenciales, o impactos negativos en los derechos fundamentales (incluido el derecho a no ser discriminado o el derecho a la intimidad). La utilización de IA supone un riesgo de que se vulneren derechos o bienes jurídicos que ya están protegidos a nivel legal y, en algunos casos, constitucional.

Este punto de partida (necesidad de minimizar los riesgos que produce una actividad a la que no se puede o quiere renunciar) es el mismo de casi cualquier otra regulación de actividades de riesgo, por ejemplo, las industriales.

A partir de aquí, se pueden utilizar varios instrumentos o técnicas de intervención: la prohibición total o parcial de ciertas actividades para evitar los riesgos (siguiendo el principio de precaución), un régimen autorizatorio (control preventivo), otras formas de control preventivo (declaraciones responsables, por ejemplo), un control exclusivamente posterior (responsabilidad civil y, en su caso, penal de quien causa daños utilizando esa técnica creadora de riesgos), todo ello acompañado de un aparato inspector, que actúa, normalmente, a instancia de los perjudicados, y que ayuda a éstos y a los tribunales a descubrir y acreditar las conductas infractoras.

En este proyecto de Reglamento se combinan esos enfoques, que además se adaptan a la especialidad y complejidad del objeto de regulación.

5.1 Aplicaciones de la IA prohibidas

De entrada, se prohíben algunos usos de la IA (artículo 5): cualquier sistema "que se sirva de técnicas subliminales que trasciendan la conciencia de una persona para alterar de manera sustancial su comportamiento de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra", o que "aproveche alguna de las vulnerabilidades de un grupo específico de personas debido a su edad o discapacidad física o mental para alterar de manera sustancial el comportamiento de una persona que pertenezca a dicho grupo de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra", o bien el uso de "sistemas de IA por parte de las autoridades públicas [significativa restricción] o en su representación con el fin de evaluar o clasificar la fiabilidad de personas físicas durante un período determinado de tiempo atendiendo a su conducta social o a características personales o de su personalidad conocidas o predichas, de forma que la clasificación social resultante" produzca resultados perjudiciales "en contextos sociales que no guarden relación con los contextos donde se generaron o recabaron los datos originalmente" o bien provoque un trato perjudicial o desfavorable "que es injustificado o desproporcionado con respecto a su comportamiento social o la gravedad de este". También se prohíben los sistemas de vigilancia indiscriminada y general ("gran hermano").

La verdad es que los tres primeros son supuestos que representan versiones extremas de algunos usos habituales de la IA y, precisamente por estar descritos en términos tan extremos y con tal acumulación de adjetivos, es muy difícil que se apliquen, por lo que la prohibición tiene una utilidad pequeña.

Decir que una aplicación de IA manipula el comportamiento humano, provocando que una persona se comporte, asuma una opinión o tome una decisión en su propio perjuicio, es decir todo y nada. Gran parte de la publicidad podría entrar en esa definición, pero a

la vez el comportamiento humano sigue siendo voluntario (esa es al menos la creencia que sustenta todo el ordenamiento jurídico), por lo que difícilmente podemos decir que una aplicación tiene esa fuerza “obligatoria” que “fuerce” a los ciudadanos a comportarse de una determinada manera. Por lo demás, no hace falta usar la IA para manipular ni para intentar llevar a las personas a tomar decisiones que son más favorables al interés de quienes les mueven en esa dirección que al interés de quienes las toman.

Lo mismo podemos decir de las aplicaciones que explotan información o predicciones sobre una persona o grupo de personas para atacar sus debilidades o circunstancias especiales, llevando a una persona a comportarse, formar una opinión o tomar una decisión en su propio perjuicio.

En cuanto a las aplicaciones que “clasifican” a las personas en función de datos obtenidos a partir de su comportamiento o de sus características personales (o de predicciones acerca de ellas), y que llevan a tratar de forma discriminatoria a determinadas personas o grupos, en contextos que nada tienen que ver con los datos en los que se basa la clasificación, o de forma desproporcionada, es uno de los escenarios de mal uso de la IA más frecuentemente descritos. Por ejemplo, un sistema que calcule la prima del seguro de automóvil en función de distintas circunstancias que puedan “predecir” la mayor o menor probabilidad de que un conductor provoque un accidente, y que acabe encareciendo la prima, por ejemplo, a quienes tengan menos estudios, o carezcan de un empleo indefinido, o se vean obligados a recorrer largas distancias en coche para ir a trabajar todos los días. Sólo se restringe su uso por poderes públicos. No se está eliminando completamente la posibilidad de utilizar el análisis de datos para que las empresas adapten su esfuerzo publicitario, sus ofertas o sus condiciones contractuales a las características de distintos clientes, que es una de las utilizaciones más habituales de la IA.

Alguna de estas conductas prohibidas (la vigilancia biométrica en tiempo real) puede ser llevada a cabo, de forma excepcional, por una autoridad pública cuando lo autorice una norma y para fines de seguridad pública.

5.2 Aplicaciones de la IA sometidas a autorización.

La identificación biométrica remota en lugares públicos (videovigilancia en calles, por ejemplo) se somete a autorización administrativa, que sólo se concederá cuando exista una norma habilitante, para la lucha contra delitos graves (incluido el terrorismo) y sometida a límites y garantías (artículo 5.3). Como es sabido, no se trata de la instalación de cámaras que simplemente graben lo que pasa en la calle, y ayuden posteriormente a saber qué pasó y a buscar a posibles responsables, sino de sistemas que comparan las imágenes percibidas con bases de datos, lo que les permite identificar automáticamente a una persona (el proyecto no dice que esta exigencia de autorización se aplique sólo a las aplicaciones en las que la identificación es inmediata o en tiempo real).

5.3 Aplicaciones de la IA para las que se establecen reglas concretas de transparencia.

En el artículo 52.1 se obliga a que, cuando se utilice un *chatbot* u otro mecanismo automatizado que interactúe con los usuarios, se advierta a éstos de que no están hablando o mensajeándose con una persona real, sino con una aplicación, salvo que esto sea obvio en vista de las circunstancias.

Otra regla importante (artículo 52.3) es que la obliga a que los sistemas conocidos como *deep fake*, que generan imágenes y/o sonido que pueden engañar y hacer creer que son imágenes reales de personas concretas (por ejemplo, personajes famosos o políticos, que pueden verse comprometidos por vídeos en los que parece que hacen o dicen cosas totalmente contrarias a sus ideas o imagen público) adviertan de que se trata de una ficción, aunque se admiten excepciones basadas, por ejemplo, en la libertad de expresión (lo que puede legitimar el uso de estas técnicas en obras de ficción como películas o series).

Menos clara me parece la obligación de advertir de la utilización de sistemas de reconocimiento de emociones a partir de datos, aunque parece hacer referencia a supuestos en que el reconocimiento se produce “en directo”, es decir, a partir de datos obtenidos en ese momento (artículo 52.2).

5.4 Aplicaciones de la IA “de alto riesgo” y sus mecanismos de control.

Pero el núcleo del proyecto de Reglamento no son las aplicaciones prohibidas o las que se someten a autorización o a reglas concretas, sino el régimen de las aplicaciones “de alto riesgo”, que se enumeran en el Anexo III y se regulan en los artículos 6-51.

Un primer grupo de aplicaciones de alto riesgo (para las que se exige, como veremos, su verificación previa por un tercero independiente) son las que se utilizan en productos que, por los riesgos que producen, están sometidos a alguna de las normas europeas enumeradas en el Anexo II, y ésta exige que el producto en cuestión se someta a una evaluación de conformidad realizada por un organismo independiente. La explicación es clara: si el sistema de IA se inserta en un producto sometido a un determinado mecanismo de control dirigido a reducir riesgos, el propio sistema de IA deberá someterse a ese mismo control.

El otro grupo (que no requiere esa verificación independiente, sino que estará sometido a una especie de declaración responsable) incluye las aplicaciones típicas de la IA “predictiva”, como las que sirven para determinar la admisión (o no) de estudiantes a centros educativos, la contratación de trabajadores o su promoción dentro de la empresa, la concesión -o denegación- de créditos, la concesión de prestaciones sociales (y la vigilancia sobre el cumplimiento de sus condiciones), la “policía predictiva” y la evaluación de riesgos que se utiliza para distribuir los recursos policiales o, en fin, las aplicaciones de IA dirigidas a su uso por jueces y tribunales. Puede comprobarse que la creación de perfiles o la utilización de IA para determinar las condiciones contractuales o el trato a un sujeto no están completamente prohibidas por el artículo 5, sino que, salvo casos extremos, son simplemente “aplicaciones de IA de alto riesgo”.

Para este tipo de aplicaciones entra en juego otra forma de tratamiento jurídico, que no es la prohibición sino el establecimiento de unos requisitos que deben cumplir. A diferencia de lo que sucede en otros ámbitos tradicionalmente considerados “de riesgo”, como el industrial, donde la regulación acaba, a nivel reglamentario, con la aprobación de normas que establecen condiciones concretas de seguridad, aquí se enuncian unos requisitos tan generales que recuerdan al artículo 6 de la Constitución de 1812 (“El amor a la Patria es una de las principales obligaciones de todos los españoles, y asimismo el ser justos y benéficos”). Así, las aplicaciones de alto riesgo deben estar basadas en datos “pertinentes y representativos, [que] carecerán de errores y estarán completos” (artículo 10.3). Es preciso documentar y archivar los datos generados en la creación y utilización de la aplicación (artículo 11). Los registros “garantizarán un nivel de trazabilidad del funcionamiento del sistema de IA durante su ciclo de vida que resulte adecuado para la

finalidad prevista del sistema” (artículo 12.2). Además, los sistemas de IA de alto riesgo “se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de una herramienta de interfaz humano-máquina adecuada” (artículo 14.1).

No se exige una transparencia total, sino “suficiente para que los usuarios interpreten y usen correctamente su información de salida” (artículo 13.1). El artículo 70.1.a) dice que las obligaciones de información serán compatibles con “los derechos de propiedad intelectual y la información empresarial confidencial o los secretos comerciales de una persona física o jurídica, incluido el código fuente, salvo en los casos contemplados en el artículo 5 de la Directiva 2016/943 relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas”.

Estos requisitos son, en cierto modo, “objetivos” máximos a los que se debe tender, pero que pueden conseguirse de muchas maneras y también con niveles de intensidad diferentes. Pensemos en la transparencia, la solidez o la documentación o archivo de los datos generados en el funcionamiento de la aplicación: habrá que buscar en cada caso concreto cuál es el modo de cumplir esos objetivos, y no hay una única forma de hacerlo, puesto que, entre otras cosas, se puede aspirar a un nivel máximo, medio o mínimo de calidad o de seguridad. Podemos decir, por ejemplo, que los coches deben ser “seguros”, pero no hay una única forma de conseguirlo y, por otro lado, no todos los modelos y marcas aspiran al mismo nivel de seguridad. Queda, por tanto, mucho que concretar.

En las aplicaciones de alto riesgo, y dejando a un lado las de identificación biométrica, las de manejo de infraestructuras críticas, así como aquellas que se instalan en productos que están sujetos a una regulación de seguridad (maquinaria industrial, juguetes, ascensores, explosivos, etc.) es el propio “proveedor” o “fabricante” quien controla el cumplimiento de esos requisitos de forma responsable (artículo 43). Por eso digo que el mecanismo es similar al de una declaración responsable (Anexo II, apartado 3).

Esto supone aplicar la técnica del compliance o “cumplimiento normativo”. Cada fabricante o diseñador tendrá que establecer, en cada producto de IA y en su proceso de creación y aplicación, una serie de medidas dirigidas a cumplir suficientemente los requisitos establecidos en los artículos 10-14 del proyecto de Reglamento, y documentarlo. Esas medidas no serán las mismas en todos los casos, sino que tendrán que ser proporcionales al tipo de aplicación, a su complejidad, a los daños que pueda causar, al riesgo de que tales daños se produzcan, etc.

Hay algunos casos en los que sí se establecen normas que traducen los requisitos generales en estándares concretos, y el proyecto hace referencia a ellas. Esto sucede cuando la IA se aplique en productos que tienen normas de seguridad que se extiendan también a aquélla (por ejemplo, vehículos de transporte, sujetos a una normativa de seguridad estricta) o cuando la UE apruebe estándares técnicos sobre algún aspecto de la IA.

Para aquellos supuestos en que el proyecto exige que la conformidad sea certificada por un tercero (que son, fundamentalmente, las aplicaciones de IA que se utilizan en productos sujetos a normativa de seguridad, así como también las de identificación biométrica y las de manejo y control de infraestructuras críticas), se regulan las entidades de verificación en términos similares a otros sectores (como la auditoría o la inspección técnica de vehículos, por mencionar sólo dos campos muy diferentes entre sí): entidades que son independientes de las empresas cuyos productos verifican, y que están sujetas

a regulación administrativa, además de tener un seguro de responsabilidad y disponer de competencias técnicas suficientes. Sus decisiones deberán estar sujetas a recurso (artículo 37).

5.5 Otras previsiones.

Las aplicaciones que no estén calificadas como "de alto riesgo" (lo que significa que las probabilidades de que con ellas se causen daños a derechos o bienes protegidos son menores) podrán asumir códigos de conducta voluntarios para dar cumplimiento a los requisitos establecidos para las aplicaciones de alto riesgo (artículo 69).

Los Estados miembros deben establecer mecanismos de supervisión y también de sanción. Las multas tendrán un tope máximo de 30 millones de euros o del 6% de la cifra de negocios mundial (si es superior a aquella cantidad), para infracciones que consistan en la utilización de las aplicaciones prohibidas de la IA, el suministro de información falsa a las entidades de verificación o el incumplimiento de los requerimientos de las autoridades (artículo 71).

También se regulan cuestiones como el establecimiento de sandboxes o espacios controlados de pruebas (artículo 53).

5.6 Lo que regula y lo que no regula el proyecto de Reglamento.

Este proyecto de Reglamento establece unos requisitos para que se puedan utilizar aplicaciones de IA tanto por operadores públicos como privados. Son requisitos generales y adicionales, porque ahora no existen expresamente, con los que se quiere prevenir daños a bienes y derechos dotados de protección al máximo nivel jurídico. Dicho de otro modo: no es que el Reglamento prohíba cosas que ahora están permitidas, sino que intenta prevenir que se produzcan esos resultados lesivos o dañinos.

El cumplimiento de los requisitos establecidos por el Reglamento (que es un cumplimiento relativo, como estamos viendo, sobre todo en el caso de las aplicaciones de alto riesgo, porque los requisitos son más bien objetivos máximos más que reglas concretas) no agota los problemas jurídicos de la IA. Queda en pie, de entrada, el control posterior que veíamos al principio. Si se producen daños a pesar de, por ejemplo, las medidas preventivas especificadas en el documento de compliance elaborado por el productor de la aplicación de IA o aprobado por la entidad certificadora, podrá haber responsabilidad civil o, en su caso, penal, aunque será necesario valorar en qué medida la responsabilidad queda excluida como consecuencia de la aplicación de esas medidas, que en principio suponen una actuación diligente dirigida a minimizar los riesgos. Es lo mismo que sucede con la ITV, que es un sistema dirigido a reducir los riesgos en la circulación de vehículos a motor, pero el hecho haber superado la ITV no excluye que se produzcan daños ni que el conductor y/o propietario del vehículo sean responsables de ellos.

Por otro lado, el cumplimiento de los requisitos establecidos en el Reglamento no significa que las aplicaciones de IA se puedan utilizar sin más y para cualquier cosa. Es necesario también cumplir la normativa sobre protección de datos y, además, habrá que estar atentos a la normativa aplicable, en su caso, al concreto sector en el que se aplique la IA. Así, por ejemplo, en su uso por Administraciones Públicas habrá que tener en cuenta qué se quiere hacer con esa aplicación: no es lo mismo utilizarla para automatizar procesos, de forma puramente instrumental (como en las aplicaciones que facilitan las declaraciones tributarias, que son jurídicamente irrelevantes), que usarlas como una ayuda para decidir cuándo se inicia un procedimiento administrativo (un paso más) o para determinar el contenido de una resolución administrativa, lo que exigirá

normalmente una habilitación normativa y no sólo el cumplimiento de los requisitos generales que establece este proyecto de Reglamento.

REFERENCIAS BIBLIOGRÁFICAS

- Brezina, C. (2005). *Al-Khwarizmi: The Inventor of Algebra*. Rosen Central.
- Civitarese, S. (2019). "Umano troppo umano". Decisioni amministrative automatizzate e principio di legalità". *Diritto pubblico*, 1, 5-41.
- Díaz, G. (Coord.) (2020). *La regulación de los algoritmos*. Aranzadi.
- Hernández, J. (2020). Decisiones algorítmicas de perfilado: régimen y garantías jurídicas. *REDA*, (203), 281-322.
- Hoffman-Riem, W. (2018). *Big data. Desafíos también para el Derecho*. Civitas.
- Huergo, A. (2019). Las sanciones administrativas en el marco del law enforcement. En D. Zegarra, (Coord.), *La proyección del Derecho Administrativo Peruano. Estudios por el Centenario de la Facultad de Derecho de la PUCP*, (pp. 515-539). Palestra.
- Kahneman, D. (2012). *Thinking, fast and slow*. Penguin.
- Lee, K. F. (2018). *AI Superpowers. China, Silicon Valley and the New World Order*. Houghton Mifflin Harcourt.
- Mayer-Schönberger, V. y Cukier, K. (2013). *Big data. The massive data revolution*.
- Resolución de estimación de las reclamaciones 123/2016 y 124/2016. (2016, 21 de septiembre). Comissió de Garantia del Dret d'Accés a la Informació Pública (Oriol Mir Puigpelat). <http://www.gaip.cat/es/inici/>
- Sentencia 2015AP157-CR. (2016, 13 de julio). *Tribunal Supremo de Wisconsin, State v. Loomis* (Ann Walsh Bradley, J.). <https://casetext.com/case/state-v-loomis-22>
- Van Eck, M. (31 de enero de 2017). Algorithms in Public Administration. *Marlies van Eck*.<https://marliesvaneck.wordpress.com/2017/01/31/algorithms-in-public-administration/>.
- Zuboff, S. (2019). *The age of surveillance capitalism*. Profile Books.



DERECHO ADMINISTRATIVO, BIG DATA Y PROTECCIÓN DE DATOS PERSONALES

ADMINISTRATIVE LAW, BIG DATA AND PERSONAL DATA PROTECTION

FELIPE ROTONDO TORNARÍA¹

RESUMEN

La Administración estatal debe servir al público, lo que legitima el ejercicio de poderes que el ordenamiento jurídico establece. Para ello utiliza herramientas, entre ellas las que hoy día provienen de las nuevas tecnologías de la información y la comunicación.

En todo caso y como en toda materia procede el respeto de los derechos humanos, entre ellos el de protección de los datos personales.

PALABRAS CLAVE

Administración | Su carácter servicial | Instrumentos tecnológicos y derechos humanos.

CONTENIDO

1. Derecho Administrativo, 1.1 Su objeto. Carácter servicial de la Administración, 1.2 Sujeción al derecho. Enfoque ético; 2. Big data, 2.1 Noción Básica, 2.2 Tipos y fuentes de datos, 2.3 Valor de los datos, 2.4 Inteligencia artificial: referencia; 3. La Administración y las TIC, 3.1 Utilización de las nuevas tecnologías, 3.2 Incidencia en la organización, 3.3 Incidencia en el procedimiento, 3.4 Continuación, 3.5 Relación con el Open Data, 3.6 Utilidad del Big Data; 4. Derecho a la Protección de Datos Personales, 4.1 Naturaleza. Sujetos, 4.2 Configuración, 4.3 Principios; 5. Anotaciones Finales; 6. Bibliografía.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 29 de abril de 2021 y aprobado para su publicación el 19 de agosto de 2021.

1. DERECHO ADMINISTRATIVO

1.1. Su objeto. Carácter servicial de la Administración

El Derecho Administrativo trata básicamente de la organización y actividad de la

1 Profesor de Derecho Administrativo, Universidad de Montevideo. Integrante de la Unidad Reguladora y de Control de Datos Personales cuyo Consejo Ejecutivo preside por períodos anuales en alternancia con otro miembro, y de la Comisión Nacional de Servicio Civil de la República Oriental del Uruguay.

Administración, la cual es el conjunto de órganos estatales que ejercen función administrativa.

La Administración forma parte, pues, del Estado y como tal, en un Estado constitucional de Derecho, su centro radica en la persona humana, titular de una dignidad que es atributo de su esencia y vale con independencia de la dignidad moral individual².

La Administración debe servir al interés general, el cual justifica el ejercicio del poder público y, a la vez, lo configura como instrumento para cumplir las competencias que establece el ordenamiento jurídico y ello de manera transparente, razonable y motivada. Así podrá hacer efectiva una “buena administración”, la cual se concibe hoy como un principio de derecho y, por tanto, un deber de la organización administrativa³.

El referido interés general “es la dimensión pública de los intereses individuales, o sea de los intereses de cada individuo en cuanto partípice de la sociedad (jurídicamente organizada en el Estado) (Bandeira de Mello, 2010, p. 18)⁴; en términos de la legislación uruguaya, este interés:

...se expresa, entre otras manifestaciones, en la satisfacción de necesidades colectivas, de manera regular y continua, en la buena fe en el ejercicio del poder, en la imparcialidad de las decisiones adoptadas, en el desempeño de las atribuciones y obligaciones funcionales, en la rectitud de su ejercicio y en la idónea administración de los recursos públicos. La satisfacción de necesidades colectivas debe ser compatible con la protección de los derechos individuales, los inherentes a la personalidad humana o los que se deriven de la forma republicana de gobierno⁵.

1.2. Sujeción al Derecho. Enfoque ético

Las reglas que constituyen este Derecho se dirigen, pues, a atender el bienestar colectivo, el cual se configura con el goce de los derechos de las personas.

Tienden a su protección y la de los diversos grupos sociales en relación al ejercicio del poder público; mejor, a asegurar que este cumpla con su misión servicial. Si la esfera pública es la “de los intereses de todos”, su forma más acabada se genera:

-
- 2 Conf. Arda, Arturo. El hombre en cuanto objeto axiológico, en “El hombre y su conducta. Ensayos filosóficos en honor de Risieri Frondizi”. Puerto Rico 1980, Ed. Universitaria, pp. 73-74, cit. por Héctor Gros Espiell, La dignidad humana en los instrumentos internacionales sobre Derechos Humanos. Anuario de Derechos Humanos. Nueva época Vol. 4. Instituto de Derechos Humanos. Facultad de Derecho. Universidad Complutense. Madrid 2003, p. 193.
 - 3 Sobre la buena administración, la Carta Iberoamericana de los Derechos y Deberes del Ciudadano en relación con la Administración (CLAD, Caracas 2013) expresa que es la que actúa según los principios de eficacia, con procedimientos que remuevan de oficio obstáculos formales y dilaciones “buscando la compatibilidad con la equidad y el servicio objetivo al interés general”; eficiencia, que exige “optimizar los resultados alcanzados en relación con los recursos (...)” y economía en cuanto al “uso racional de los recursos públicos disponibles. El gasto público se realizará atendiendo a criterios de equidad, economía, eficiencia y transparencia”.
 - 4 Bandeira de Mello, Celso Antonio. Grandes temas de Direito Administrativo. 1^a ed. 2^º tiragem. Malheiro Ed. S. Paulo 2010, A noção jurídica de interesse público, p. 181.
 - 5 Leyes N° 17.060 de 23-XII-1998, art. 20 y N° 19.823 de 19-IX-2019 sobre Normas de Conducta en la Función Pública.

...por la constitucionalización de esos intereses de todos que son los derechos universales y, por ello, fundamentales. Dígase lo mismo 'del pueblo', aquí definido como el sujeto jurídico colectivo cuyos componentes son unificados por la igual titularidad de expectativas constituidas, como son precisamente los derechos fundamentales. (Ferrajoli, 2011, p. 52-53)⁶.

Por otra parte, el Estado y su Administración se sujeta a las reglas de Derecho, tanto a los principios como a la normativa constitucional, legal, reglamentaria y, por cierto, a la internacional, en especial la concerniente a los Derechos Humanos.

El Derecho Administrativo no se enfoca, entonces, en la potestad pública, sino en el administrado, mejor dicho, la persona. Sus normas:

...se dirigen a atender el bienestar colectivo, el cual se configura con el goce de los derechos de las personas. Tienden a su protección y la de los diversos grupos sociales en relación al ejercicio debido del poder público; a asegurar que este cumpla con su misión servicial" (Rotondo, 2015, p. 87)⁷.

Es un Derecho Administrativo personalizado y garantista que supera: "concepciones meramente técnicas para asumir la prevalencia del enfoque ético, en que se reconoce la supremacía de los derechos fundamentales y la consagración de los procedimientos democráticos de formación y manifestación de la voluntad estatal" (Justen Filho, 2006, p. 47-48)⁸.

2. BIG DATA

2.1. Noción básica

El big data dice relación con las tecnologías de la información y la comunicación (TIC), e implica el tratamiento de grandes cantidades de datos procedentes de diversas fuentes con el fin de hallar interrelaciones, encontrar patrones repetitivos e inferir información; al efecto la dinámica de las nuevas tecnologías usa algoritmos. Sus características van más allá de la capacidad de las herramientas habituales del software.

El concepto de 'datos masivos' implica la búsqueda, recolección y almacenamiento de enormes cantidades de datos, así como los procedimientos seguidos para su análisis y obtención de tendencias; el análisis puede configurarse, entre otras modalidades, mediante asociaciones que habilitan hallar relaciones entre variables y minería de datos para ubicar comportamientos predictivos, combinando métodos estadísticos y de machine learning con almacenamiento en bases.

6 Ferrajoli, Luigi. Principia iuris. Teoría del derecho y de la democracia. 2. Teoría de la democracia. Ed. Trotta. Madrid 2011, pp. 52-53: "Las instituciones públicas son las que están dirigidas al ejercicio de funciones públicas y/o la garantía de situaciones universales, las primeras de todos los derechos fundamentales".

7 Rotondo, Felipe. Derechos fundamentales y Derecho administrativo. Revista de Derecho Público, Año 24. Nº 47. Mdeo. 2015, p. 87.

8 Justen Filho, Margal. Curso de Direito Administrativo. 2^a ed. Ed. Saraiva 2006, pp. 47-48. Carlos F. Balbín. Curso de Derecho Administrativo. La Ley T. I. 1^a ed. 1^a reimpresión Bs.As. 2008, pp. 95-98 refiere al "(...) equilibrio del poder, entendido como el conjunto de prerrogativas que persiguen el reconocimiento de derechos vs. otros derechos. Ese equilibrio entre derechos con intermediación del poder estatal y sus prerrogativas es el paradigma (...) del Derecho Administrativo actual".

El valor del Big data no radica (solo) en la cantidad (*volumen*) de datos procesados sino en la capacidad de inferencia que deriva de su *variedad y velocidad* (de crecimiento), y se vincula a las notas de veracidad, calidad, confiabilidad y a las cuestiones de su tratamiento en virtud, precisamente, del enorme volumen y complejidad.

2.2. Tipos y fuentes de datos

Los datos pueden ser estructurados, con formato y longitud definidos, (ejemplo, datos fiscales de los contribuyentes); no estructurados, dispersos (ejemplos, los e-mails o datos que surgen de expedientes administrativos) o semiestructurados, que con sus propios metadatos refieren a los objetos y sus relaciones (caso del HTML).

Por otra parte, pueden ser estáticos, concretos en el tiempo (renta de una persona en cierto período) o dinámicos, obtenidos de modo continuo, los cuales permiten mayor análisis hacia el futuro (ejemplo, sobre el tráfico de la ciudad o los lapsos de acceso a servicios públicos).

En cuanto a sus fuentes, los datos pueden generarse por las personas, así al enviar mensajes de whatsapp, correos electrónicos, tuitear contenidos, utilizar motores de búsqueda, etc.;emerger de cruzamientos de datos, automáticamente o no; producirse entre máquinas con diversos dispositivos, caso de los sensores, geo-localizadores, etc. y generarse por lectores biométricos de huella, retina, etc.

En este sentido el Big Data se vincula con el Internet de las Cosas (IoT), estructura de red por la cual los dispositivos físicos se interconectan de modo de recabar, transmitir, almacenar y analizar datos como tablets con pantallas más grandes, electrodomésticos inteligentes, wearables.

El volumen y velocidad con que los datos se generan exigen un adecuado almacenamiento, procesamiento y análisis, incluso para que no queden obsoletos, sean veraces y contribuyan a la finalidad del titular de la base y, si corresponde, se supriman, actualicen o archiven.

A los efectos indicados existe hoy la disciplina llamada Ciencia de Datos.

2.3. Valor de los datos

Los datos como información tienen un valor incommensurable en todo sentido y ámbito (social, económico, científico, administrativo, etc.) dados los resultados que pueden alcanzarse con el trío que forman con la tecnología y el análisis.

Pero si bien esto da lugar o habilita beneficios implica, a la vez, riesgos, entre otros a la vulneración de la privacidad y de los datos personales.

En ese sentido, cabe citar el documento “*Seizing opportunities, preserving values*” derivado del mandato del entonces Presidente de Estados Unidos de Norteamérica Barack Obama, quien se comprometió entonces (enero 2014) a ajustar el programa de vigilancia sobre datos telefónicos. Expresa que las tecnologías de Big Data, como toda tecnología, no son, per se, buenas o malas, que pueden utilizarse para el bien de la sociedad o para dañar y que en su perspectiva positiva contribuyen a fortalecer la democracia, generar crecimiento económico y mejorar la calidad de vida de los ciudadanos en diversas áreas.

Afirmó, también, que en cuanto a los derechos de los ciudadanos el tratamiento de datos habilita a las autoridades públicas a realizar prácticas discriminatorias y que los valores en peligro se relacionan directamente con la privacidad, por lo que es necesaria la protección

de toda información personal con adecuadas leyes de protección a consumidores y a los ciudadanos en general, garantizando que la información recolectada sea utilizada para fines permitidos y previamente establecidos.

2.4. Inteligencia Artificial: referencia

El Big data y la capacidad de aprendizaje autónomo “hacen posible que las computadoras perciban, aprendan, razonen y colaboren en el proceso de toma de decisiones para la resolución de problemas en formas que resultan similares a lo que hace la gente” (Smith y Shum, 2018)⁹.

He ahí la Inteligencia Artificial, sobre la cual no existe una única definición:

...podría afirmarse que, en su concepción amplia, se trata de un término ‘sombrilla’ que incluye una variedad de técnicas computacionales y de procesos enfocados a mejorar la capacidad de las máquinas para realizar muchas actividades, los que comprenden desde modelos algorítmicos, pasando por los sistemas de machine learning, hasta llegar a las técnicas de deep learning” (Red Iberoamericana de Protección de Datos, 2019)¹⁰.

Hoy día la Inteligencia Artificial se aplica cada vez más: “asistentes virtuales en nuestros celulares, algoritmos en las redes sociales que nos muestran de una u otra forma la información, autos sin conductor, programas que aprenden de nuestras acciones para recomendarnos música, películas o artículos de consumo en tienda online, traductores en tiempo real, sistemas que detectan de forma temprana enfermedades o riesgos sanitarios, entre otros” (AGESIC, 2019)¹¹.

Pero, también, sirven para alterar o falsificar videos y hacer aparecer personas ausentes en una reunión o hacerles decir lo que no han dicho, con incidencia en múltiples ámbitos, incluso en la actividad política y el voto del ciudadano y otras múltiples situaciones, lo cual puede darse, incluso, sin mala fe por defecto de los diseños de sistemas.

Todo ello plantea cuestiones éticas y jurídicas, propias de la esencia de la persona humana, ser social y responsable, que debe asumir lo que debe hacer o no hacer y cómo hacerlo y las consecuencias de su conducta¹².

9 El futuro computarizado. La Inteligencia Artificial y su rol en la sociedad, por Microsoft. Prólogo de Brad Smith y Harry Shum. Washington. EE.UU. 2018. En el Capítulo 1 señala que las tecnologías abarcan capacidad de diversa índole de las computadoras: visión ('ver' mediante el reconocimiento de lo que figura en una imagen o video); voz ('escuchar' mediante la comprensión de las palabras que las personas dicen y transcribirlas a texto); lenguaje ('comprender' el significado de las palabras según los diversos matices y complejidades del lenguaje) y conocimiento ('razonar' mediante la comprensión de la relación entre personas, cosas, lugares, eventos y conceptos similares).

10 Cf. Recomendaciones generales para el Tratamiento de Datos en la Inteligencia Artificial aprobadas por la Red Iberoamericana de Protección de Datos. XVII Encuentro, Naucalpan de Juárez-México 2019.

11 Estrategia de Inteligencia Artificial para el Gobierno Digital. Agencia para el Desarrollo del Gobierno de Gestión Electrónico y la Sociedad de la Información. (AGESIC) Uruguay. <http://www.fic.edu.uy/sites/default/files/2019-10/estrategia%20de%20inteligencia%20artificial.pdf>

12 Las diversas cuestiones involucradas han determinado la Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 21-IV-2021, por el que se establece normas armonizadas en materia de Inteligencia Artificial (Ley de Inteligencia Artificial) y modifican determinados actos legislativos de la Unión. Contiene una clasificación en base a riesgos según la función del sistema de Inteligencia Artificial; plantea como no admisibles, entre

Procede tener en cuenta, por otra parte, que: "El cúmulo abrumador de información que nos inunda no significa más sabiduría. La sabiduría no se fabrica con búsquedas ansiosas por Internet, ni es una sumatoria de información cuya veracidad no está asegurada (...)" (Francisco, 2020, p. 37)¹³.

3. LA ADMINISTRACIÓN Y LAS TIC

3.1. Utilización de las nuevas tecnologías

La Administración, en su organización y en su actividad, debe mirar hacia el futuro y replantearse, efectuar el tránsito de la Galaxia Gutenberg a la Galaxia Internet¹⁴.

Las TIC, "por sí solas no transforman los roles, la estructura y las funciones, pero en un sistema democrático, abren importantes posibilidades para que los agentes transformadores impulsen genuinas reformas" (Prats y Catalá Joan, 2015, p. 21)¹⁵.

Ellas contribuyen a la interrelación de la Administración con el entorno, a que sea abierta a la participación ciudadana, transparente y a que preste los servicios de la mejor manera, con procedimientos más simples y de menor duración, que sean idóneos en cuanto a resultado, tiempo y costos, a que se reduzcan las molestias del administrado, por ejemplo, al no exigirse su desplazamiento a la oficina para recabar informaciones.

3.2. Incidencia en la organización

Desde esta perspectiva, las nuevas tecnologías habilitan a la Administración a reducir el número de cargos de supervisión; a ampliar el ámbito físico de las tareas y hasta independizarlo mediante el correo electrónico, la videoconferencia, el teletrabajo, etc., de modo que contribuyen a la flexibilidad de la estructura, a redefinir sus fronteras e implicar un nuevo gerenciamiento, a la transversalidad interna de cada entidad y entre las entidades que integran la Administración de modo que operen como unidad, con mayor servicialidad hacia el administrado.

No se eliminan las modalidades organizativas clásicas (desconcentración, delegación, descentralización, etc.) pero se requiere una mayor coordinación y una estructuración

otros, los que presentan gran potencial para manipular personas con técnicas subliminales que van más allá de sus conciencias o explotan vulnerabilidades de grupos como menores de edad o personas con discapacidad, y pueden distorsionar su conducta hasta generar, en ellos o terceros, un daño físico o psíquico. También los sistemas gubernamentales de puntuación social o los de identificación biométrica remota en tiempo real en lugares públicos como el reconocimiento facial, salvo caso de extrema gravedad; entre los sistemas de alto riesgo están los de filtrado de perfiles profesionales en procesos de selección- susceptibles de replicar sesgos-, o los de calificación crediticia, entre otros. En cuanto al uso de algoritmos, complementa la normativa con requerimientos específicos para minimizar el riesgo de discriminación, en especial la referida al diseño y calidad de los sets de datos utilizados, lo que se complementaría con obligaciones de gestión de riesgos, testeos y supervisión humana a lo largo de todo el ciclo vital de los sistemas.

13 SS Francisco. Carta Encíclica Fratelli Tutti. Sobre la fraternidad y la amistad social. Paulinas. Bs.As. 2020, p. 37.

14 El primero, título del libro de Marshall Mc Luhan de 1962, el segundo de Manuel Castells. Barcelona. Aretà 2001.

15 Prats y Catalá Joan. De la Burocracia al Management, del Management a la Gobernanza. Las transformaciones de las Administraciones Públicas de nuestro tiempo. Estudios Goberna. INAP. Madrid, 2005, p. 21.

que promueva y asegure el uso adecuado de las tecnologías y permita una articulación más fuerte, nexos basados en la disposición de información estratégica confiable en una actividad mancomunada, incluso en el ámbito de la llamada “descentralización por colaboración”, que comprende la actuación del sector privado.

Hoy la gobernanza se inserta en la Sociedad de Redes porque además de implicar una conexión entre la Administración, prestadores privados de servicios, usuarios, unidades de investigación, etc., ellos son interdependientes y dan lugar a un grupo determinante en el proceso de elaboración de políticas.

“En la Sociedad de Redes moderna, (...) estamos dependiendo cada más del acceso a las redes y a la información que contienen y los servicios que ofrecen. Podemos hablar de un entorno digital (...)” (Saarenpää, 2019, p. 105)^{16/17}.

3.3. Incidencia en el procedimiento

La despapelización de los expedientes, ahora digitales, determina por su parte la necesaria adecuación de los procesos y, en su caso de las normas jurídicas, “para continuar otorgando a las personas los mismos derechos y garantías que en el ámbito material”(Viega, 2013)¹⁸, garantías que corresponden al principio de seguridad, expresión específica del de juridicidad.

Dada la innegable importancia del soporte, se ha llegado a identificar procedimiento y expediente, si bien este es el resultado documental del procedimiento.

Así se ha dicho que el soporte papel se convirtió “en una de las herramientas básicas de la Administración” y recordado que uno de los principios de dominación legal de Max Weber es el “atenerse al expediente”, lo que debería mantenerse en la era de la Administración Electrónica, “convenientemente puesto al día”, porque es “una herramienta básica del principio de legalidad, en tanto forma esencial de expresión de la voluntad administrativa. La escritura es garantía de una Administración más cerebral que pasional, menos caprichosa y mejor informada, con más criterio sobre las decisiones a tomar, más objetiva en suma”(Ortega, 2008, p. 52-55)¹⁹.

La despapelización habilita enlaces de diversa documentación a modo de hiperexpediente

-
- 16 Saarenpää, Atthi. “Protección de datos: lo excepcional llega a ser lo natural”. Revista de Derecho y Nuevas Tecnologías N° 1-2019. La Ley Uruguay, pp. 105 y ss. Expresa: “en el gobierno de la información actual dependemos de un entorno operativo digital y los enlaces electrónicos del ciudadano promedio con el gobierno son más interactivos y se realizan en tiempo más real que antes”; “en la Sociedad de Redes, dependemos críticamente de las redes de información y su uso en el gobierno y en otros lugares. Su utilización toma diversas formas, desde la creación de documentos, hasta la comunicación y desde iniciar asuntos de manera electrónica hasta la utilización de una gran variedad de cuentas electrónicas (canales seguros de hecho) que establecen los individuos y las organizaciones”.
 - 17 “(...) en un mundo donde las funciones públicas esenciales, la comunicación social y la información personal migran a plataformas digitales, los gobiernos en colaboración con la sociedad civil y las empresas, necesitan crear las reglas, los controles y los equilibrios necesarios para mantener la justicia, la competitividad, la equidad e incluso la propiedad intelectual, la seguridad y la fiabilidad”, Klaus Schwab. La Cuarta Revolución Industrial. World Economic Forum. Ed. Debate, España 2016.
 - 18 Conf. Viega, María José. Procedimiento administrativo electrónico. Presentación realizada en las VIII Jornadas del Tribunal de lo Contencioso Administrativo. Mdeo, 2013.
 - 19 Rivero Ortega, Ricardo. El Expediente Administrativo. De los Legajos a los Soportes Electrónicos. Thomson Aranzadi. Pamplona 2008, pp.52-55.

y un mejor manejo simultáneo de expedientes, lo que es especialmente útil en la actividad de control o en el funcionamiento de órganos colegiados²⁰.

3.4. Continuación

En el aspecto del procedimiento administrativo, como secuencia de etapas conformadas por actos jurídicos y operaciones materiales dirigidas a cierto objetivo, de los cuales el más usual es el dictado de un acto jurídico principal (resolución de un asunto), la cuestión se proyecta en el *procedimiento electrónico*, el cual implica actuaciones de esta índole, incluso actos administrativos que se forman por medio del computador o este los “crea”.

En el segundo caso se trata de actos automatizados, especie del electrónico, en los que no intervienen personas físicas, sino que el sistema produce la decisión (Delpiazzo, 2010, p. 79)²¹.

Por ello, para que no se “traslade” la autoridad de las personas a los algoritmos y acorde con principios como los de objetividad y transparencia, procede establecer “previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, indicarse ‘el órgano que debe ser considerado responsable a efectos de impugnación (Ley española N° 40/2015)’”^{22/23}.

En cuanto al objeto de los referidos actos, las innovaciones tecnológicas como la Inteligencia Artificial habilitan a la Administración a tomar decisiones derivadas de algoritmos con base en análisis predictivos y sistemas con capacidad de aprendizaje. Pero esos algoritmos pueden contener un parámetro con un supuesto erróneo o que sea irrelevante para adoptar una medida jurídicamente válida; también pueden tener una falla de programación, así; por ejemplo, parámetros vinculados en términos ilógicos entre sí o con relación a la regla a aplicar.

De ahí que “la confianza ciega en la tecnología puede traducirse en situaciones de profunda injusticia de nula o tardía solución si no se cuenta con mecanismos de contingencia y

-
- 20 En ese sentido el decreto uruguayo N° 276/013 de 9-IX-2013 sobre procedimiento electrónico en la Administración Central, art.11, establece que “Cuando un expediente electrónico esté a consideración de un órgano colegiado será puesto en conocimiento simultáneo a todos sus integrantes a efectos de ser estudiado y resuelto dentro del mismo plazo” y el art. 12, que si se requiere la actuación de otro órgano u organismo, “esta se producirá a través de medios electrónicos de comunicación, salvo que causas justificadas lo impidan, dejándose constancia explicativa de ello”.
 - 21 Delpiazzo, Carlos E. Noción y regulación del procedimiento y del acto administrativo electrónico, en Estudios de Derecho Administrativo. La Ley, Mdeo. 2010 N° 1, p. 79 y ss. Expresa que es viable en la actividad reglada y en la discrecional, en esta última “mediante la implementación de sistemas expertos capaces de emular la conducta de un experto humano dentro de un dominio limitado a partir del llamado ‘razonamiento cibernético’ (...”).
 - 22 Ley española N° 40/2015, 1º de octubre, de Régimen Jurídico del Sector Público, art. 41.2. Condice con el Reglamento (UE) 2016 del Parlamento Europeo y del Consejo, de 27-IV-2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la circulación de estos datos, art. 22.
 - 23 En ese sentido, Valero Torrijos, Julián. Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración. Revista Catalana de Dret Public N° 58-2019, pp. 82 y ss.

acción con recursos humanos calificados para responder” (Pezzuti, 2020).²⁴

Otro aspecto de incidencia de las nuevas tecnologías es el de posibilitar una mayor participación ciudadana, habilitando que los habitantes sean informados y consultados en los asuntos que les atañen.

Al efecto se les reconoce el derecho a relacionarse electrónicamente con la Administración, sin excluir los medios tradicionales, por lo cual el uso y desarrollo de las TIC no es una facultad discrecional de los organismos públicos sino su obligación²⁵, “lo que supone que las Administraciones estén interrelacionadas entre sí a fin de simplificar los procedimientos” (2007)²⁶.

La interoperabilidad es un supuesto imprescindible para la actuación administrativa electrónica; se la entiende como la capacidad de los sistemas de información, y por ende de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos. Se trata de una cuestión instrumental que tiene como sustrato la viabilidad de la circulación de la información pública entre las Administraciones como cuestión sustancial (Delpiazzo, 2020, p. 17-36)^{27/28}.

3.5. Relación con el Open Data

Las TIC interesan, también, en relación al open data que refiere a los datos abiertos por parte de la Administración, accesibles a cualquier persona de manera gratuita o a un costo mínimo, y por medios de publicidad que deben resultar amigables, con contenido veraz y lenguaje entendible, en tiempo real.

-
- 24 Conf. Pezzuti, Miguel. Los actos administrativos electrónicos. Mdeo. 2020 inédito. Ejemplifica con la actual pandemia del coronavirus y los esfuerzos por suministrar vacunas: “La implementación de sistemas que distribuyan agendas solo mediante acceso remoto, resulta idónea para garantizar la inexistencia de privilegios indebidos en el acceso, por lo que parece contar con sólidos fundamentos en los principios de igualdad y eficacia. Pero si existe una base de datos con errores (ejemplo de supuesto inválido en el algoritmo por errores en las fechas de nacimiento) que impidan a cierto sector de la población vulnerable (mayores de 80 años, por ejemplo) acceder a la vacuna, podrían verificarse contagios con efectos graves que podían prevenirse o bien el agotamiento de partidas con la definitiva imposibilidad de acceso en una campaña, puesto que la eficiencia en el reparto conspira contra los indebidamente excluidos”.
- 25 Así en el Uruguay este derecho se prevé por la ley N° 19.355 de 18-XII-2015, art. 74.
- 26 Carta Iberoamericana de Gobierno Electrónico aprobada por la IX Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado, Pucón, Chile, 31-V y 1-VI- 2007; se adoptó por la XVII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, Sgo. de Chile, 10-XI- 2007.
- 27 Delpiazzo, Carlos E. Impacto de las TIC en el Derecho Administrativo en Impacto de las Nuevas Tecnologías en el Derecho Administrativo. Instituto de Derecho Administrativo, Facultad de Derecho. Universidad de la República. FCU. Mdeo. 2020, pp. 17-36.
- 28 La ley uruguaya N° 18.719 de 27-XII-2010, arts. 157 a 161, establece que las entidades públicas, estatales o no, deberán adoptar las medidas necesarias e incorporar en sus respectivos ámbitos tecnologías para promover el intercambio de información pública o privada autorizada por su titular, disponible en medios electrónicos; que deben cumplir con las obligaciones de secreto, reserva o confidencialidad y las medidas necesarias para garantizar niveles de seguridad y confidencialidad adecuados; que recabarán el consentimiento cuando corresponda según la ley de Protección de Datos Personales y que responderán por la veracidad de la información al momento de producirse el intercambio. El art. 159 nomina como principios rectores los de cooperación e integralidad; finalidad; confianza y seguridad; previo consentimiento informado de los titulares de los datos personales; eficiencia y eficacia.

En la sociedad de la información y el conocimiento cobra vigor el derecho al acceso a la información como modo de llegar a la verdad, propio de la naturaleza racional de la persona y del principio de transparencia, esencial en un sistema democrático; en este sentido la regla es la transparencia activa y pasiva de lo que es, precisamente, de naturaleza “pública”.

Así se tiene el derecho al acceso a la información pública el cual, por otro lado, permite un mejor proceso de toma de decisiones al implicar mayor visibilidad, contribuir a la participación ciudadana y a que la Administración sirva realmente al interés general, evitando la corrupción²⁹.

Al efecto procede una ponderación de derechos en base a criterios generales cuya aplicación, obviamente, exige atender la especificidad de cada caso.

El open data debe darse, además, de manera global en el ámbito de la Administración, lo que exige cooperación entre las entidades que la conforman y la sujeción a buenas prácticas.

De todos modos, hay información en poder de la Administración Pública que al referir a personas identificadas o identificables no es pública y está tutelada por la normativa de protección de datos personales.

3.6. Utilidad del Big Data

En cuanto al uso de las tecnologías de Big Data por la Administración, los tratamientos contribuyen al cumplimiento de sus cometidos y el ejercicio de los respectivos poderes instrumentales.

Por ejemplo, en áreas como las de la salud, para prevenir riesgos sanitarios, establecer los caracteres de enfermedades y su atención médica, ordenar los tiempos hospitalarios o controlar beneficios por licencia por enfermedad; en la materia energética, a fin de gestionar la eficiencia en el uso del alumbrado público o controlar el consumo particular; en la recaudación tributaria, para mejorar la actividad inspectiva y verificar las declaraciones de los contribuyentes; en la educativa, para prevenir la deserción escolar o encarar programas de estudio adecuados; en la seguridad pública, para prevención de delitos, determinar tendencias por zonas, en lo cual es especialmente relevante la protección de la identidad de las personas y evitar “sesgos incrustados” de cualquier índole (de género, etnia, posición económica, etc.).

La utilización en las ciudades inteligentes (smart cities) es un ejemplo del aporte coordinado de información de diverso tipo (tratamiento de información sobre energía, tránsito vehicular, ambiental, etc.) con un objetivo de desarrollo sostenible basado en inversiones variadas, más allá de la tecnológica.

29 En el Uruguay rige la ley 18.381 de 17-X-2008, que define como información pública “la que emane o esté en posesión de cualquier organismo público, estatal o no estatal” y reconoce el derecho al acceso a esa información sin necesidad de justificarse las razones por las que se la solicita. Los lineamientos esenciales son los de divulgación máxima de la información; presunción juris tantum a favor de la publicidad; proporcionalidad y legalidad (formal, no por reglamento) de las restricciones a la información, para las cuales deben existir razones objetivas y explícitas que revelen el daño para un bien jurídico protegido, sea un interés público o una información privada cuya tutela sea de interés público. Ninguna razón es admisible si la información refiere a violaciones de derechos humanos o es relevante para investigar, prevenir o evitar estas violaciones.

De manera general, el Big data contribuye al diseño, implementación, evaluación y monitoreo de políticas públicas y a la prestación de servicios públicos, lo cual debe insertarse en una gobernanza digital que respete y haga respetar los derechos de las personas, entre ellos a la protección de los datos personales, dado el enorme cúmulo de datos recabados y almacenados por la organización administrativa, con creación de perfiles de quien se relaciona con la Administración como usuario, consumidor, etc.

Por lo mismo, el uso del Big data ha de configurarse sobre un principio de transparencia reforzado porque muchos datos pueden proceder de terceros, de cruzamiento de información entre las entidades, etc. sin el conocimiento del afectado y, además, en interconexión con dispositivos digitales, lo que hace que el uso de los datos sea más complejo y opaco.

También sobre el principio de igualdad que por esencia es relacional y no admite ninguna discriminación o sesgo arbitrarios; este principio puede encararse incluso como de inocuidad en el sentido de que de ningún modo se lesionen valores humanos, individuales o sociales.

Estos principios se interrelacionan con los aplicables en materia de protección de datos personales que se indican en el apartado siguiente.

De otra manera la innovación tecnológica llevará a ilegitimidad de los tratamientos y a que no se logre la confianza social que la respalde.

4. DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

4.1. Naturaleza. Sujetos

Existe el derecho a la *intimidad*, a lo reservado de cada persona, el derecho a “ser dejado solo” (a la soledad, de Warren y Brandeis, ‘The Right to Privacy’, 1890), “prerrequisito para la construcción de la autonomía individual que a su vez constituye el rasgo esencial del sujeto democráticamente activo” (Tribunal Constitucional de Colombia, 2010)³⁰.

También, en visión usualmente seguida, el más amplio de privacidad respecto a un ámbito que se comparte con los más cercanos; corresponde al respeto de una esfera privada de cada persona y su entorno, exento de la invasión de terceros y de la autoridad de los magistrados.

En ese enfoque se hace referencia a generaciones de derechos, si bien en todos ellos, de un modo u otro, se configuran nuevas facetas por la incidencia de la sociedad tecnológica.

Dada la fuerza expansiva de los derechos y con base en el de la intimidad y el más amplio de la privacidad, se desarrolló el relativo a la protección de los datos personales en un entorno en que el obligado es tanto público como privado, constituyendo un derecho de tercera generación, fundamental y propio de un sistema democrático.

Muchas normativas, entre ellas la ley uruguaya N° 18.331 de 11-VIII-2008, art. 1º, lo

30 Términos de la sentencia del Tribunal Constitucional de Colombia, sentencia C-640/10 de 18-VIII-2010.

reconocen como derecho “inherente a la personalidad humana”^{31/32}.

El reconocimiento o declaración, con finalidad tuitiva, procede por esa inherencia; el art. 6º inciso 2º de la citada ley establece, por otra parte, que: “Las bases de datos no pueden tener finalidades violatorias de derechos humanos” o “contrarias a las leyes o a la moral pública”.

4.2. Configuración

El derecho a la protección de los datos personales tiene una configuración compleja ya que comprende varios poderes de disposición y control de esos datos: “la facultad de saber en todo momento quién dispone de ellos y a qué uso los está sometiendo”; “el poder oponerse a esa posesión y usos (...)”, el “consentir sobre la recogida y uso de los datos personales y a saber de los mismos”; el de requerir a quien corresponda que ponga fin a su posesión y empleo, o “en su caso, requerirle para que los rectifique o los cancele” (Tribunal Constitucional español 292/000)³³.

Asimismo, comprende el derecho a impugnar valoraciones personales efectuadas en base a un tratamiento automatizado de datos, lo que es relevante ante la utilización del Big data.

Por cierto, el derecho de la protección de datos personales no es absoluto; la Suprema Corte de Justicia de Uruguay suele expresar en sus fallos que los derechos no son ilimitados, salvo la vida, “un derecho ilimitado sería antisocial por ello su necesidad de hacerlo compatible con el derecho de los demás dentro de la comunidad y con los intereses superiores de esta última” (2016)³⁴.

El titular es una persona física determinada o determinable aunque alguna legislación, como la uruguaya, lo extiende a la persona jurídica “en cuanto corresponda”, lo que se fundamenta en que ella cuenta con una imagen propia en el sector de su actividad, con un valor que se proyecta sobre sus actividades y sus propios bienes o, que en su caso, se le reconoce la titularidad de derechos que sirven instrumentalmente a la intimidad de sus

31 Esa disposición legal agrega que “está comprendido en el art. 72 de la Constitución”, el cual recibe la esencia humanista del jusnaturalismo liberal a través de los principios generales de derecho, los cuales configuran un bloque de juridicidad con la normativa constitucional y el Derecho internacional de los Derechos Humanos.

32 El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo cit., en su Primer “Considerando” expresa que “La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental”; tiene en cuenta textos jurídicos como la Carta de los Derechos fundamentales, art. 8 ap. 1 y el Tratado de Funcionamiento de la UE, art. 16 ap. 1

33 Sentencia del Tribunal Constitucional español 292/000, de 30-XI. Expresa que el derecho alcanza “a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros puede afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual (...), sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que, por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos (...)”.

34 Entre otras, sentencias Nº 312/995, 220/002, 54/004, 564/012, 697/014, 79/016, esta última de 5-IV-2016. En igual sentido, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo cit., en su Cuarto “Considerando” afirma que este derecho “debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos, con arreglo al principio de proporcionalidad (...)”.

integrantes o que están directamente conectados con esta³⁵.

El sujeto obligado, “responsable de la base de datos o del tratamiento” puede ser una persona física o jurídica, pública o privada “propietaria de la base o quien decida sobre finalidad, contenido y uso del tratamiento” (ley citada, art. 4 “K”), por lo que está comprendida la Administración a través de las diversas personas jurídicas estatales que ejercen función administrativa.

El ámbito subjetivo no tiene, pues, exclusiones en lo que atañe al titular de la información, al responsable ni al encargado del tratamiento.

Por su parte, el tratamiento de los datos personales se define como “operaciones y procedimientos sistemáticos, de carácter automatizado o no, que permiten el procesamiento de datos personales, así como también su cesión a terceros mediante comunicaciones, consultas, interconexiones o transferencias” (ley citada, art. 4 “M”).

4.3. Principios

A continuación, se mencionan algunos de los que rigen en la materia, reglas que explicitan valores superiores y contribuyen a dar coherencia y permanencia al ordenamiento, sobre todo ante los incessantes cambios tecnológicos. Los principios están interrelacionados, se sustentan en el de juridicidad y contribuyen para la interpretación e integración de la normativa:

- A. Veracidad, según el cual los datos deben ser veraces, adecuados, ecuánimes y no excesivos en relación con la finalidad (“minimización”); además no podrán obtenerse por medios desleales, fraudulentos, abusivos o, extorsivos.

Este principio pone en juego criterios de proporcionalidad y, por tanto, juicios de idoneidad, necesidad y ponderación.

- B. Finalidad, que impone fines precisos y la coherencia en el tratamiento de datos con relación a los que dan mérito a su obtención; asimismo su eliminación cuando no sean necesarios o pertinentes a los fines para los cuales hubieren sido recolectados, por lo que abarca la regla de la limitación temporal sin perjuicio de casos de excepción por razones históricas, estadísticas o científicas y, en la medida de lo posible, disociados.

Impone, pues la especificación relativa a los fines de los tratamientos, lo que se relaciona con el principio especialidad que delimita las competencias de los órganos públicos ya que ellos no se rigen por el principio de libertad, solo pueden desarrollar los cometidos que el ordenamiento les asigna.

En cuanto a la disociación, es clave que impida vincular a persona determinada o determinable, sin posible reidentificación; puede efectuarse mediante anonimización. Y en todo caso exige controles periódicos determinados por el responsable de la respectiva base, ante la aparición de nuevas tecnologías y de métodos para prevenir y evitar los posibles riesgos de reidentificación.

- C. Consentimiento informado: previo a todo tratamiento de datos o a su comunicación,

35 La ley uruguaya N° 18.331 vigente (arts. 3 ‘A’, 9 ‘A’ y 22) contiene normas que no se aplican a la persona jurídica, así respecto al límite del registro por un plazo determinado de datos relativos a obligaciones de carácter comercial; se las excluye de la titularidad de bases destinadas a exclusivo uso personal o doméstico y de la exigencia del previo consentimiento informado respecto del tratamiento del dato de su teléfono.

que exige una declaración o acción afirmativa clara del titular del dato (Reglamento (UE) 2016/679 del Parlamento)³⁶.

Debe ser informado para que este titular conozca inequívocamente la finalidad a la que se destinarán los datos y el tipo de actividad del responsable, mediante un medio sencillo y claro; esto es especialmente relevante en el caso de datos sensibles como los de salud, de origen racial o étnico, opiniones políticas, biométricos, etc.

El vínculo entre los principios es evidente, así entre el de finalidad y el del consentimiento; y ellos cobran vigor en el Big Data.

En efecto:

“Una de las características de algunos tratamientos masivos de datos consiste, en la reutilización de datos que inicialmente habían sido recogidos para otra finalidad, o bien con una legitimación diferente. Pensemos en los casos en que se tratan datos personales que son necesarios para la ejecución de un contrato, en sentido estricto, y luego son reutilizados por el responsable de tratamiento para otros fines como, por ejemplo, en el caso de los pagos efectuados mediante tarjeta de crédito. En el caso de que el emisor de la tarjeta considerase efectuar un tratamiento adicional para, digamos, ofrecer a sus clientes sus propios productos financieros, puede entenderse que se trata de una finalidad conexa y compatible con la original. Sin embargo, una reutilización consistente en cruzar la información detallada de las compras efectuadas, con el fin de elaborar perfiles de consumo para luego ser ofertados a terceros resulta ajena a la relación contractual inicial. Esto constituye una desviación de la finalidad, para la cual se necesitaría una nueva legitimación en base al consentimiento” (González, 2017)³⁷.

Es posible un fundamento diverso al consentimiento para el tratamiento de datos, así si este tiene como base el interés legítimo o razones de interés general autorizadas por ley, o si el organismo solicitante tiene mandato legal para hacerlo^{38/39}.

-
- 36 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo cit., art. 4 numeral 11 y Estándares de la Red Iberoamericana de Protección de Datos Personales de 20-VI-2017, art. 12.1.
 - 37 González, Pedro Alberto. Responsabilidad proactiva en los tratamientos masivos de datos. Revista Internacional de Éticas aplicadas. Nº 24-2017, pp. 115 y ss. <https://www.dilemata.net/revista/index.php/dilemata/article/view/412000103>
 - 38 La ley uruguaya prevé excepciones al consentimiento, así para el ejercicio de funciones propias de los Poderes públicos, cumplir una obligación legal y comunicar datos personales relativos a la salud, si esto es necesario “por razones sanitarias, de emergencia o para la realización de estudios epidemiológicos, preservando la identidad de los titulares mediante mecanismos de disociación adecuados, cuando ello sea pertinente”, ley Nº 18.331, art. 17 inc. 3º ‘C’, texto dado por ley Nº 18.719 de 27-XII-2010, art. 153. El art. 19 prevé que “Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional, la normativa específica y lo establecido en la presente ley”.
 - 39 También hay situaciones, “particularmente en el contexto de la acción humanitaria”, en las que “obtener el consentimiento puede ser muy difícil, y, por ende, puede ser necesario y legítimo recurrir a otro fundamento jurídico, como el interés público o los intereses vitales del titular de datos. La posibilidad de basarse en motivos de interés público es particularmente

- D. Seguridad que comprende aspectos físicos, lógicos y jurídicos lo que se relaciona con la gestión de la información, determinación de los activos de que se dispone y de los niveles de riesgos, así como la formación del personal de la organización. En caso de violación a la seguridad de la base, su responsable debe comunicarlo a quienes pueden verse afectados y al órgano garante en cierto plazo⁴⁰.
- E. Reserva, de acuerdo con el cual “las personas físicas o jurídicas que obtuvieren legítimamente información proveniente de una base de datos que les brinde tratamiento”, deben utilizarla “en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad”.

Prohíbe toda difusión de la información a terceros, y quienes trabajen para el responsable en cualquier relación jurídica, están sujetos a secreto profesional.

- F. Responsabilidad, por toda violación de la normativa lo que es propio de un Estado de Derecho y se proyecta en diversas áreas, básicamente administrativa, civil y penal.

En interrelación con otros principios, se enfatiza una responsabilidad proactiva que configura la accountability. Ella se dirige a asegurar el debido cumplimiento de la normativa y a implementar medidas para acreditarlo: registro de actividades, auditorías, evaluaciones de impacto, adopción de la privacidad por diseño desde el inicio del sistema de información, sin que disminuya su funcionalidad.

La referida privacidad impone que sea por defecto en el sentido de configurar a los sistemas de modo que, por defecto, brinden mayor protección a la privacidad a fin de no compartir información del usuario, salvo acción de este que altere la configuración; la funcionalidad que integra y garantiza seguridad y privacidad; la protección durante todo el ciclo de vida de los datos, incluyendo su supresión o eliminación, sin perjuicio de los lapsos de retención lícitos.

Se añade la transparencia en tanto el responsable de la base debe informar los términos de uso desde un principio y no modificarlos sin el previo consentimiento del titular de los datos, así como someterse a una verificación adecuada⁴¹.

relevante para organizaciones humanitarias que, debido a la naturaleza de sus actividades y las situaciones de emergencia en la que generalmente operan, tienen mayores dificultades para obtener consentimiento (...) Esto puede ser el caso, por ejemplo, cuando el tratamiento de datos personales es un prerequisito para recibir asistencia, o cuando se requieran recopilar los datos de una persona desaparecida”, Informe del Comité Jurídico Interamericano Principios Actualizados sobre la Privacidad y la Protección de Datos Personales con Anotaciones. 98º Período Ordinario de Sesiones 5-9 abril de 2021 (OEA/Ser.Q CJL/doc. 638/21- 8abril2021). Principio Dos: Transparencia y Consentimiento.

- 40 En el Uruguay, por ley N° 19.670 de 15-X-2018 art. 38 y decreto N° 64/020, arts. 3 y 4, la comunicación referida debe hacerse en plazo máximo de 72 horas de conocida la vulneración. Se dispone también que “Constatada la existencia de incidentes de seguridad que occasionen, entre otras, la divulgación, destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos, los responsables o encargados de tratamiento deberán iniciar los procedimientos previstos necesarios para minimizar el impacto de dichos incidentes dentro de las primeras 24 horas de constatados”.
- 41 V. Brian Nougrères, Ana. La protección inteligente de los datos personales: privacy by design (PbD). Revista Internacional de Protección de Datos Personales. N° 1 - Universidad de los Andes. Bogotá 2012. Concluye que “El concepto de Privacy by Design constituye una teoría para implementar los principios de la protección de datos personales de una forma integral, con una visión holística, que los incorpora con la concepción del negocio y de los sistemas de información” .

Se ha agregado la actualización o rediseño, basado en “repensar, rediseñar y revivir”, o sea rever las estrategias de mitigación de riesgos y sistemas para una mayor protección a la privacidad, minimizando los datos recabados, reexaminando y limitando sus períodos de retención y siempre que sean estrictamente necesarios para la respectiva finalidad, reforzando la seguridad, etc.

En cuanto a la evaluación de impacto, se impone si el tratamiento refiere a un importante número de datos personales, lo que ha sido establecido por diversa normativa, entre ella el Reglamento Europeo ya citado⁴² y reciente legislación uruguaya^{43/44}.

5. ANOTACIONES FINALES

- i) La Administración debe ser instrumento del interés general y, para ello, cumplir las reglas de Derecho, siendo idónea en cuanto al resultado debido (eficaz) y propiamente eficiente respecto a la actividad y medios utilizados, que estos sean adecuados cualitativa y cuantitativamente. Ello en la sustancia de las medidas y en su motivación o justificación.
- ii) Las TIC contribuyen a la “eficacia eficiente”⁴⁵ e inciden en la configuración de un Derecho administrativo de la información, aggiornado, centrado en la persona y sus derechos fundamentales.

42 Art. 35 apartado 1: “Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares de los datos vinculados a la comisión de infracciones penales, civiles o administrativas”.

43 La evaluación de impacto se incluye como una medida de la responsabilidad proactiva según ley N° 19.670 ya citada, art. 39 y decreto 64/020; el art. 6 de este dispone que “En forma previa al inicio del tratamiento, el responsable y el encargado del tratamiento en su caso, deberán realizar una evaluación de impacto en la protección de datos personales, cuando en las operaciones de tratamiento pueda: a) Utilizarse datos sensibles como negocio principal. b) Proyectarse un tratamiento permanente o estable de los datos especialmente protegidos (...) o de los datos vinculados a la comisión de infracciones penales, civiles o administrativas; c) Implicar una evaluación de aspectos personales de los titulares con el fin de crear o utilizar perfiles personales, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad de comportamiento y solvencia financiera y localización. d) Llevarse a cabo el tratamiento de datos de grupos de personas en situación de especial vulnerabilidad y, en particular, de menores de edad o personas con discapacidad. e) Producirse un tratamiento de grandes volúmenes de datos personales. f) Transferirse datos personales a otros Estados u organizaciones internacionales respecto de los que no exista nivel adecuado de protección) Otros que determine la Unidad Reguladora y de Control de Datos Personales”.

44 La Unidad Reguladora y de Control de Datos de Uruguay conjuntamente con la Agencia de Acceso a la Información Pública de la Argentina emitieron un Guía de Evaluación de Impacto en Protección de datos. V. <https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos>.

45 Parejo Alfonso, Luciano. Perspectivas del Derecho Administrativo para el próximo mileno. Parte IV La eficacia administrativa y la calidad total de los servicios públicos. Ed. Jurídicas Gustavo Ibáñez. Bogotá 1998, p. 89 y ss. Expresa que “(...) la eficacia engloba necesariamente la eficiencia y economía en la ejecución del gasto encomendado a la administración”, “la eficacia reclamada por la Constitución” (española), es una eficacia eficiente”.

Los datos que posee la Administración son un activo en la medida que sean exactos, oportunos, auditables y trazables.

Tanto en su creación como en su aplicación, los procedimientos deben brindar confianza a los habitantes, enfatizando en la seguridad del procesamiento y análisis de los datos masivos y, en general, en el respeto de los derechos, entre ellos el de protección de los datos personales.

Solo así las herramientas tecnológicas contribuyen realmente a crear valor público.

- iii) El referido uso responsable involucra dimensiones de índole ética, jurídica, técnica y social que permitan una transformación digital que habilite, legítimamente, anticiparse a las necesidades de las personas y prevenir situaciones problemáticas.

Para ello son aplicables los principios de responsabilidad proactiva, con "responsable" claramente identificable; transparencia, que lleve a poner a disposición los datos utilizados y los algoritmos, siendo estos neutrales y auditables; seguridad, para la cual se enfatiza en controles permanentes y en la privacidad por diseño.

- iv) Las personas no son un (mero) conjunto de enorme cantidad de datos y, por otro lado, importa que sean ellas quienes ejerzan efectivamente la autoridad pública necesaria en la comunidad y no que las decisiones provengan de algoritmos, en una especie de gobierno desarrollado por los datos.

"El marco regulatorio debe adaptarse igualmente a los nuevos apremios. Además de confianza, los ciudadanos reclaman seguridad en la utilización de las nuevas tecnologías. Las soluciones jurídicas deben ser integrales, contemplando todos los elementos afectados, y garantizando la regularidad y la eficacia de los procesos". (Sánchez Bravo, 2007, p.83).

6. BIBLIOGRAFÍA

Agencia para el Desarrollo del Gobierno de Gestión Electrónico y la Sociedad de la Información (AGESIC). (2019). *Estrategia de Inteligencia Artificial para el Gobierno Digital*. <http://www.fic.edu.uy/sites/default/files/2019-10/estrategia%20de%20inteligencia%20artificial.pdf>

Balbín, C. (2008). *Curso de Derecho Administrativo*.

Bandeira de Mello, C. (2010). *Grandes temas de Direito Administrativo*. Malheiro.

Brian, A. (2012). La protección inteligente de los datos personales: privacy by design (PbD). *Revista Internacional de Protección de Datos Personales y Acceso a la información*, (1), 4-15.

Centro Latinoamericano de Administración para el Desarrollo. (2007). *Carta Iberoamericana de Gobierno Electrónico*.

Delpiazzo, C. (2010). Noción y regulación del procedimiento y del acto administrativo electrónico. *Estudios de Derecho Administrativo*, (1).

Delpiazzo, C. (2020). Impacto de las TIC en el Derecho Administrativo. En C. Vásquez, *Impacto de las Nuevas Tecnologías en el Derecho Administrativo* (pp. 17-36).

- Montevideo: Fundación de Cultura Universitaria.
- Ferrajoli, L. (2011). *Principia iuris. Teoría del derecho y de la democracia*. Trotta.
- González, P. (2017). Responsabilidad proactiva en los tratamientos masivos de datos. *Revista Internacional de Éticas aplicadas*, (24), 115- 129. <https://www.dilemata.net/revista/index.php/dilemata/article/view/412000103>
- Justen Filho, M. (2006). *Curso de Direito Administrativo*. 2^a edición. Saraiva.
- Parejo, L. (1998). *Perspectivas del Derecho Administrativo para el próximo milenio*. Ed. Jurídicas Gustavo Ibáñez.
- Parlamento y Consejo Europeo. (27 de abril de 2016). Reglamento UE 2016/679.
- Pezzuti, M. (2020). Los actos administrativos electrónicos. MDEO.
- Prats, J. (2005). *De la Burocracia al “management”, del “management” a la gobernanza. Las transformaciones de las Administraciones Públicas de nuestro tiempo*. INAP.
- Red Iberoamericana de Protección de Datos. (2019). *Recomendaciones generales para el Tratamiento de Datos en la Inteligencia Artificial aprobadas por la Red Iberoamericana de Protección de Datos. XVII Encuentro*.
- Rivero, R. (2008). *El Expediente Administrativo. De los Legajos a los Soportes Electrónicos*. Thomson Aranzadi.
- Rotondo, F. (2015). Derechos fundamentales y Derecho administrativo. *Revista de Derecho Público*, Año 24, (47), 87-102.
- Saarenpää, A. (2019). Protección de datos: lo excepcional llega a ser lo natural. *Revista de Derecho y Nuevas Tecnologías*, (1), 105-140.
- Sánchez, A. (2007). *La Administración Electrónica en España*. *Revista do direito*, (28), 83-111.
- Smith, B. y Shum, H. (2018). Prólogo. En Microsoft, *El futuro computarizado. La Inteligencia Artificial y su rol en la sociedad*.
- Tribunal Constitucional de Colombia. (18 de agosto de 2010). Sentencia C-640/10.
- Viega, M. (2013). Procedimiento administrativo electrónico. Presentación realizada en las VIII Jornadas del Tribunal de lo Contencioso Administrativo. MDEO.



ELEMENTOS PARA LA CONFIGURACIÓN DE LA ADMINISTRACIÓN DIGITAL

ELEMENTS FOR THE CONFIGURATION OF THE DIGITAL ADMINISTRATION

RUBÉN MARTÍNEZ GUTIÉRREZ¹

RESUMEN

La transformación digital de las Administraciones Públicas requiere unas sólidas bases conceptuales y normativas. Este artículo profundiza en dichas cuestiones y en los principales elementos que deben ser considerados como estructurales en el modelo de e-Administración. Con este objetivo, se prestará especial atención a los principios estructurales como la interoperabilidad y la seguridad, a los derechos y, también, a los instrumentos necesarios para configurar la Administración digital: sede electrónica, registros, gestión documental electrónica, notificación electrónica e identificación y firma. Finalmente, se realizará una propuesta de modelo de regulación legal adecuada y se analizarán los aspectos metodológicos básicos.

PALABRAS CLAVE

E-Administración | Interoperabilidad | Seguridad | Derechos | Instrumentos | Tramitación electrónica | Marco normativo

CONTENIDO.

1. Planteamiento general. Concepto y regulación actual en España y Perú; **1.1.** Concepto de Administración Digital; **1.2.** La regulación en España; **1.3.** La regulación en Perú; **2.** Elementos estructurales del modelo de e-Administración; **2.1.** Interoperabilidad; **2.2.** Seguridad; **2.3.** Otros principios: accesibilidad – usabilidad, neutralidad y proporcionalidad; **3.** Garantías y derechos de las personas. En especial, el derecho a no aportar datos y documentos; **3.1.** Los derechos en el modelo de e-Administración en la legislación española; **3.2.** El derecho clave a no aportar datos y documentos

ABSTRACT

The digital transformation of public administrations requires solid conceptual and regulatory foundations. In this article we are going to delve deeper into these issues and into the main elements that should be considered as structural in the e-Administration model. With this objective in mind, special attention will be paid to structural principles such as interoperability and security, the rights, and also to the instruments necessary to configure the digital Administration: webs, registers, electronic document management, electronic notification and electronic signature. Finally, the paper analyses a proposal will be made for an appropriate legal regulation model and the basic methodological aspects.

KEYWORDS

E-Government | Interoperability | Security | Rights | Tools | E-processing | Regulatory framework

¹ Profesor Titular de Derecho Administrativo, Universidad de Alicante. Actualmente es Investigador Principal del Proyecto de Retos del Ministerio, convocatoria 2019, titulado "Datos abiertos y reutilización de la información del sector público en el contexto de su transformación digital: la adaptación al nuevo marco normativo de la Unión Europea". Más información de su CV en: <https://cvnet.cpd.ua.es/curriculum-breve/es/martinez-gutierrez-ruben/2556>. Contacto: ruben.martinez@ua.es

por las personas interesadas. El acceso al dato mínimo necesario para la tramitación. Su regulación en España; **4.** Instrumentos básicos para la tramitación electrónica de procedimientos; **4.1.** Sede electrónica; **4.2.** Oficinas de asistencia en materia de registros y registros electrónicos; **4.3.** Expediente electrónico, gestión documental avanzada y archivo; **4.4.** Comunicaciones y notificaciones; **4.5.** Identificación y firma electrónica; **5.** El modelo de regulación legal adecuado. Propuestas; **6.** Aspectos metodológicos del proceso de implantación de la e-Administración. Propuestas y retos. Referencias bibliográficas.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 29 de abril de 2021 y aprobado para su publicación el 15 de agosto de 2021.

1. PLANTEAMIENTO GENERAL. CONCEPTO Y REGULACIÓN ACTUAL EN ESPAÑA Y PERÚ

1.1. Concepto de Administración Digital

Antes de comenzar a profundizar en los elementos estructurales y normativos del modelo de Administración Digital, resulta interesante establecer su concepto. Cuando hablamos de Administración Digital nos referimos al concepto clásico de Administración Pública Electrónica, que es un concepto mucho más acotado que el de Gobierno Digital, ya que este último incluye también la regulación de la actividad por medios electrónicos que desarrollan los órganos de carácter político o de gobierno. Los conceptos jurídicos deben formularse teniendo en cuenta su potencial utilidad para la configuración del régimen jurídico del ámbito concreto de que se trate. Con esta premisa, y en relación al concepto de Administración Digital (equivalente al de Administración Pública Electrónica), debo remitirme al concepto que procedí a formular en 2007², en primer término, y en 2009, ya con más profundidad analítica. Conforme a este último concepto, la Administración electrónica se define como:

Un nuevo modelo de administrar basado en la aplicación de las tecnologías de la información y la comunicación en el desarrollo de las actividades administrativas con dos dimensiones diferenciadas: de un lado, la dimensión interna, que comprende la aplicación de las TIC en el trabajo administrativo interno y en las relaciones interadministrativas; y, de otro lado, la dimensión externa, referida a la aplicación de las TIC con el objetivo de ofrecer servicios públicos y procedimientos administrativos en sede electrónica a los administrados (pp. 202 y ss.)

En base a esta definición, podemos formular una serie de consideraciones. En primer lugar, que la e-Administración debe entenderse como un nuevo modelo de administrar basado en la utilización de las TIC, razón por la cual deberán establecerse los mecanismos jurídicos y técnicos que puedan garantizar la necesaria seguridad jurídica de las personas en sus relaciones con las Administraciones públicas. En segundo lugar, el modelo de Administración electrónica tiene dos dimensiones, la interna y la externa, y las obligaciones y exigencias en cada una de ellas deben adaptarse a sus potenciales destinatarios, ya que no es lo mismo establecer obligaciones para los empleados públicos que para las personas que se relacionan con las Administraciones. En este sentido, la normativa que regule este modelo de administrar deberá observar las garantías necesarias de la dimensión *ad intra* de las Administraciones, y también de las relaciones

² En Administración electrónica: origen, definición institucional y contexto actual. Revista Aranzadi de Derecho y Nuevas Tecnologías.

ad extra o de contacto con las personas en sus relaciones con las Administraciones y en el procedimiento. Por último, en tercer lugar, la aplicación de la TIC en estas dos vertientes debe subdividirse en cuatro actividades características: (1) el trabajo administrativo interno, (2) las relaciones interadministrativas, (3) el desarrollo de servicios públicos y (4) la implantación, desarrollo y realización de procedimientos administrativos electrónicos. Todos estos elementos deberían encontrarse presentes en la regulación normativa de la e-Administración.

1.2. La regulación en España

La regulación del modelo de Administración electrónica en España tiene como base las dos leyes administrativas que estructuran el Derecho Administrativo español, de forma que el procedimiento electrónico se inserta plenamente en el corazón y ADN del ordenamiento jurídico – administrativo de carácter básico en España. De un lado, la Ley 39/2015, de Procedimiento Administrativo Común, que regula la vertiente externa de la actuación administrativa, ha integrado en su articulado la regulación legal del procedimiento administrativo electrónico. De otro lado, la Ley 40/2015, de Régimen Jurídico del Sector Público, regula la dimensión interna del obrar de las Administraciones, incorporando las cuestiones relativas al funcionamiento electrónico del sector público³. Con estas dos leyes, se derogaron la Ley 30/1992, que se ocupaba del régimen jurídico de las Administraciones públicas y el procedimiento administrativo común por medios presenciales y en papel, y la Ley 11/2007, que regulaba la e-Administración y el procedimiento administrativo electrónico. Ahora bien, las Leyes 39 y 40 de 2015 han regulado de forma separada en dos Leyes los aspectos *ad intra* y *ad extra* del modelo de e-Administración. Se trata de una separación que resulta un tanto polémica y artificial, ya que se han regulado en normas diferentes cuestiones íntimamente relacionadas como la sede y el registro electrónico, por no hablar de que algunos de los instrumentos tienen una ubicación sistemática cuestionable como, por ejemplo, la sede electrónica en la Ley que regula la vertiente interna, la separación de la regulación de la firma e identificación electrónicas, o la reduplicada regulación legal del archivo, además de otras cuestiones que deberían disponer de un mejor tratamiento legal.

Pocos días antes de la plena eficacia del régimen legal de la e-Administración en España previsto para 2 de abril de 2021 (después de una serie de aplazamientos legales de la fecha inicialmente prevista de 2 de octubre de 2018), se promulgó el 31 de marzo de 2021 el Real Decreto 203/2021, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

Sobre ello, he señalado en publicaciones anteriores que:

La propia estructura de la norma reglamentaria tiene una mejor sistematica que la regulación legal de estos aspectos divididos en las Leyes 39 y 40 de 2015 sobre una idea, las cuestiones de la dimensión externa en la LPAC, y las cuestiones de la dimensión interna en la Ley 40/2015, de Régimen Jurídico del Sector Público (LRJSP). Esta distinción legal que se efectuó en las denominadas “leyes siamesas”, que desde luego son uno de los pilares básicos de nuestro sistema jurídico – administrativo, siempre planteó incertidumbres, que se

3 Para un estudio sistemático e integrado de ambas normas, me remito más ampliamente a tres de mis trabajos más recientes: *El Régimen Jurídico del Nuevo Procedimiento Administrativo Común*, del año 2016; *El procedimiento electrónico en las Administraciones Locales. Aspectos metodológicos y normativos del proceso de implantación*, del año 2018 y *El procedimiento administrativo y el régimen jurídico de la Administración Pública desde la perspectiva de la innovación tecnológica*”, del año 2020.

apreciaban especialmente en algunos aspectos como la ubicación sistemática de la Disposición Adicional Segunda de la LPAC (que tenía mejor encaje en la LRJSP), la regulación de los portales web, puntos de acceso general electrónico y sedes electrónicas que se ubicaron en la LRJSP siendo instrumentos de la vertiente *ad extra*, o la división de las cuestiones de e-firma en las 2 normas que ciertamente suponían una dificultad interpretativa adicional, entre otras muchas cuestiones. A priori, la sistemática del Reglamento también merece una valoración positiva al establecer el desarrollo de las Leyes con una visión integral y de conjunto en el que se regulan todos los instrumentos del modelo de Administración electrónica en una sola norma, lo que clarifica y simplifica el régimen jurídico y la certeza regulatoria en este ámbito (2021^a, p. 2).

Así, este reglamento culmina el marco normativo de la e-Administración en España.

1.3. La regulación en Perú

La regulación de la e-Administración en Perú ha variado de forma considerable desde el estudio comparativo del procedimiento administrativo electrónico titulado “El procedimiento administrativo electrónico en los ordenamientos peruano y español”, en Revista de Derecho Administrativo, CDA, número 9, año 5. En aquel momento sugerí, ante la inexistente regulación del modelo de Administración electrónica en la Ley de Procedimiento Administrativo General o en alguna Ley específica y unitaria, que:

El legislador peruano (...) deberá acometer una reforma del régimen jurídico de la Administración electrónica en Perú que ordene de manera sistemática y coherente los principios rectores, los derechos de los ciudadanos, las garantías de la tramitación electrónica, los elementos estructurales de la e-Administración y los cuatro instrumentos necesarios para desarrollar procedimientos administrativos electrónicos. Para realizar esta labor tendrá dos posibilidades igualmente válidas: de un lado, reformar de manera integral la vigente Ley de Procedimiento Administrativo General para incorporar la regulación del procedimiento administrativo electrónico; o, de otro lado, promulgar una Ley que regule de manera integral y específica la Administración electrónica y el procedimiento administrativo electrónico (2010, p. 113).

Con la promulgación en 2018 del Decreto Legislativo N° 1412 por el que se aprueba la Ley de Gobierno Digital, entiendo que el legislador peruano optó por la regulación de las cuestiones de e-Administración en una Ley específica. No obstante, aunque se trata de una Ley que ha abordado los diferentes elementos o instrumentos de tramitación electrónica, la regulación legal es aún muy sucinta y limitada en cuanto a la regulación de algunos instrumentos clave como la sede electrónica o los registros, además de que no ha incluido la notificación electrónica, el expediente electrónico y otras cuestiones que se mantienen en el texto actual de la Ley N° 27444 del Procedimiento Administrativo General. Realmente, y desde luego no es una cuestión menor ni desacertada, la Ley de Gobierno Digital de 2018 se centra fundamentalmente en tres aspectos: (1) la identidad y firma electrónica, (2) la interoperabilidad y (3) la seguridad. Sin embargo, no puede decirse que esta ley específica regula de manera integral, unitaria y coherente el modelo de e-Administración y el procedimiento administrativo electrónico en el sentido que manifesté en el trabajo citado supra. Lamentablemente, a nivel legal, sigue existiendo dispersión normativa e insuficiencia regulatoria legal en algunos instrumentos del modelo de Administración pública electrónica.

Ahora bien, en la misma línea que ha sucedido en España, el reglamento de desarrollo

de la Ley de Gobierno Digital, aprobado por Decreto Supremo N° 029-2021-PCM que aprueba el Reglamento del Decreto Legislativo N° 1412, el cual aprueba la Ley de Gobierno Digital y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, enmienda las disfunciones legales que hemos señalado con una regulación amplia, detallada y unitaria del modelo de Administración electrónica. De hecho, la norma dispone de algunos preceptos y capítulos interesantes y de impacto como los relativos a la interoperabilidad y la seguridad, que sitúa a la normativa peruana en muy buen lugar en la regulación de estas materias. Sin embargo, muchos de los aspectos regulatorios del reglamento deberían a mi juicio incorporarse en un texto de naturaleza legal con mayor precisión que la que actualmente establece la Ley de Gobierno Digital por razones de seguridad jurídica. Incluso, quizá el reglamento de 2021 podría ser el espaldarazo definitivo para una nueva regulación legal del procedimiento administrativo general en Perú que integre plenamente en su articulado los instrumentos de tramitación electrónica de procedimientos, dejando la Ley de Gobierno Digital como un texto legal centrado en los importantísimos principios de interoperabilidad y seguridad garantizados plenamente por Ley. Con estas modificaciones legislativas, Perú podría situarse claramente a la vanguardia de la regulación de la e-Administración y el procedimiento administrativo electrónico.

2. ELEMENTOS ESTRUCTURALES DEL MODELO DE E-ADMINISTRACIÓN

2.1. Interoperabilidad

El concepto de interoperabilidad no es nuevo en el ámbito de la aplicación de las Tecnologías de la Información y la Comunicación en la actividad de las Administraciones públicas, e incluso en sentido más general se trata de un concepto que aparece en la normativa de ferrocarriles europea de la primera mitad del S.- XX con el objetivo de conseguir estandarizar los anchos de vía para que las máquinas de ferrocarril pudieran circular de una región o Estado a otro. En términos generales, la interoperabilidad tiene como objetivo garantizar la correcta conexión o conectividad de dos equipos o instrumentos que deseen o necesiten comunicarse entre sí, de modo que sea posible la fluida comunicación entre distintos aplicativos o plataformas de tramitación electrónica, lo que constituye la base necesaria para posibilitar el nuevo modelo de e-Administración y el correcto desarrollo de los procedimientos administrativos digitales.

En origen, el concepto de interoperabilidad se refería a la colaboración interadministrativa en materia tecnológica, por lo que, en cierta manera se encontraba vinculado básicamente al principio de cooperación tecnológica entre Administraciones públicas para conseguir conectarse o intercomunicarse. Esta noción de interoperabilidad se ceñía exclusivamente a la esfera interna de las Administraciones. Sin embargo, en el momento en el que se comenzaron a desarrollar las políticas de implantación de la Administración electrónica el propio concepto de interoperabilidad se vio modificado, debiendo adaptarse al nuevo contexto marcado por el objetivo de la prestación de servicios públicos y el desarrollo de procedimientos administrativos electrónicos para los ciudadanos y empresas. En los últimos tiempos han proliferado un buen número de definiciones de interoperabilidad. Debido a la importancia capital que el efectivo establecimiento de un marco de interoperabilidad tiene para la implantación y prestación de servicios y procedimientos de Administración electrónica, tanto la Unión Europea como algunos de sus Estados Miembros (en el plano nacional) han decidido establecer definiciones jurídicas de lo que debe entenderse por

interoperabilidad⁴. Así, la Unión Europea, en el artículo 3º apartado f) de su Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC) define la interoperabilidad como la “capacidad de los sistemas de tecnologías de la información y las comunicaciones (TIC), y de los procesos empresariales a los que apoyan, de intercambiar datos y posibilitar la puesta en común de información y conocimientos”. La citada definición comunitaria de la interoperabilidad se refiere tanto a la dimensión interna de la e-Administración como a la externa, y dado su carácter normativo, en principio, debe ser respetada por los distintos legisladores nacionales a la hora de regular sus sistemas y redes internas de Administración electrónica. Este necesario y escrupuloso respeto se infiere en la legislación española de 2015 debido a las múltiples referencias a la misma, aunque la cobertura legal de la interoperabilidad en España no sea, en mi opinión, la adecuada. No sucede lo mismo en Perú, donde la Ley de Gobierno Digital sí regula ampliamente en sus artículos 26 y siguientes la interoperabilidad, otorgándole cobertura legal suficiente y adecuada. La interoperabilidad remite a la idea de compatibilidad y de conectividad, como ya hemos apuntado, pero no se refiere únicamente a un ámbito, nivel o dimensión sino que como se ha llegado a afirmar tiene un carácter poliédrico, es decir, se materializa o se debería materializar mediante distintas dimensiones (Cerrillo i Martínez, 2010, p. 762). De hecho, así lo ha entendido el legislador peruano, que en el artículo 28 de la Ley de Gobierno Digital ha establecido cuatro niveles o capas de interoperabilidad:

- Interoperabilidad a nivel organizacional: Se ocupa del alineamiento de objetivos, procesos, responsabilidades y relaciones entre las entidades de la Administración Pública para intercambiar datos e información para el ejercicio de sus funciones en el ámbito de sus competencias.
- Interoperabilidad a nivel semántico: Se ocupa del uso de los datos y la información de una entidad garantizando que el formato y significado preciso de dichos datos e información a ser intercambiada pueda ser entendido por cualquier aplicación de otra entidad de la Administración Pública. Dichas entidades deben adoptar los estándares definidos por el ente rector para el intercambio de datos e información.
- Interoperabilidad a nivel técnico: Se ocupa de los aspectos técnicos relacionados con las interfaces, la interconexión, integración, intercambio y presentación de datos e información, así como definir los protocolos de comunicación y seguridad. Es ejecutado por personal de las Oficinas de Informática o las que hagan sus veces de las entidades de la Administración Pública, de acuerdo con los estándares definidos por el ente rector.
- Interoperabilidad a nivel legal: Se ocupa de la adecuada observancia de la legislación y lineamientos técnicos con la finalidad de facilitar el intercambio de datos e información entre las diferentes entidades de la Administración Pública, así como el cumplimiento de los temas concernientes con el tratamiento de la información que se intercambia.

Siguiendo la definición jurídica de principios elaborada por García de Enterría y

4 Asimismo, la e-Government Act de EEUU (2002) también se refiere a la interoperabilidad, debido a su capital importancia para la implantación de los servicios de e-Administración. La citada ley define la interoperabilidad como “the ability of different operating and software systems, applications, and services to communicate and exchange data in an accurate, effective, and consistent manner”; (Sección 101, Capítulo 36, parágrafo 3601). Como se observa, esta definición sobre interoperabilidad pretende garantizar la interacción, conectividad, interconexión y comunicación entre las aplicaciones, sistemas y plataformas tecnológicas utilizadas para la prestación de servicios de e-Administración.

Fernández Rodríguez (2002), quienes señalan que “los principios se identifican con aquellos elementos esenciales e indispensables para la consecución y desarrollo de una determinada actividad, y precisamente su calificación como principios hace referencia a su carácter básico como soportes primarios estructurales del sistema” (p. 83), ha afirmado que:

Si algo puede ser catalogado como soporte primario estructural del nuevo modelo de administrar y de las plataformas electrónicas del nuevo procedimiento administrativo común (...) es, desde luego, la interoperabilidad. Tanto es así, que sin interoperabilidad no hay posibilidad de comunicación electrónica entre las plataformas y aplicaciones que las Administraciones y administrados utilizan para realizar procedimientos electrónicos por lo que la regulación jurídica de la interoperabilidad y su garantía, a pesar de las dificultades interpretativas que puedan plantear estas normas y de las rigideces que se desprenden de las mismas en su diseño, es fundamental para el correcto desarrollo del modelo de gestión documental electrónico del nuevo procedimiento (especialmente en relación a la interacción e interconexión de archivos para el intercambio electrónico de datos y documentos entre Administraciones) (2017, p. 2899).

Asimismo, sobre el tema, he sostenido lo siguiente:

El carácter básico, estructural y esencial de la interoperabilidad ha quedado patente no solo en España sino fundamentalmente en la mayoría de normas y documentos institucionales comunitarios que coinciden en afirmar que para conseguir la implantación de servicios y procedimientos de e-Administración resulta imprescindible garantizar la interoperabilidad entre los diversos sistemas y plataformas tecnológicas utilizados por las Administraciones, los ciudadanos y las empresas (2017, p. 2891).

De hecho, en España el ya referido Reglamento de actuación y funcionamiento del sector público por medios electrónicos aprobado por Real Decreto 203/2021 ha venido a consagrarse normativamente el principio de interoperabilidad⁵. Según reitera el propio Decreto 203/2021, este principio debe ser “entendido como la capacidad de los sistemas de información y, por ende, de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos”, siendo precisamente ésta una cuestión clave e ineludible en la concesión de la Administración electrónica. La inclusión de este principio en la normativa, que ya había sido considerado como tal por la doctrina administrativista⁶, debe valorarse de una forma muy positiva y es evidente el esmero, cuidado y detalle que ha dedicado el nuevo Reglamento a las cuestiones de interoperabilidad dada su capital importancia. Como prueba de ello simplemente debemos citar la Disposición Final Segunda del Decreto 203/2021, en la que se realiza una intensa reforma del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (que no será analizado en este trabajo para no desvirtuar la centralidad del examen

-
- 5 Esta realidad ya fue puesta de manifiesto en Martínez Gutiérrez, R. (2009), y también en otros muchos trabajos posteriores tanto en materia de e-Administración como de Contratación Pública Electrónica. A este respecto véase: Martínez Gutiérrez, R. (2017) y Martínez Gutiérrez, R. (2019). La interoperabilidad como factor clave y estructural en la internacionalización de la contratación pública. En Contratación Administrativa Práctica, 159. Número especial La LCSP un año después.
- 6 Entre los trabajos más recientes que ahondan en esta cuestión puede verse Gracia Díaz, M. (2019).

del Reglamento de 2021, pero cuya importancia y trascendencia para el desarrollo efectivo de la e-Administración es fundamental). Por su parte, en Perú la relevancia que tanto la Ley del Gobierno Digital como el Reglamento otorgan a la interoperabilidad demuestran claramente su consideración como principio jurídico esencial del modelo de e-Administración.

2.2. Seguridad

La seguridad es otro de los principios nucleares del nuevo modelo de e-Administración, por lo que el concepto de seguridad debe adquirir la condición de principio esencial del nuevo procedimiento administrativo común que debe ser garantizado por el ordenamiento jurídico – administrativo. En España, el objetivo del legislador ya desde la Ley 11/2007 ha sido la exigencia del mismo nivel de garantías y seguridad en el procedimiento administrativo electrónico que el requerido para la utilización de medios no electrónicos en la actividad administrativa. La formulación de este principio tenía como propósito garantizar el establecimiento de dos modelos equivalentes de administrar, al exigir el mantenimiento del mismo nivel de garantías y seguridad independientemente de si el administrado tramita electrónicamente o en papel. Con la promulgación de las Leyes 39 y 40 de 2015, la seguridad adquirió una importancia capital ya que el almacenamiento de la información en los archivos y la tramitación de la actuación administrativa y de los procedimientos se producirá casi en exclusiva por cauces electrónicos. Así pues, tanto la articulación legal de la seguridad como las normas reglamentarias que desarrollan la misma deben ser consideradas como valores estructurales del nuevo modelo de administrar, estableciéndose al respecto normas que garanticen unos adecuados niveles de seguridad. Por otro lado, en Perú, basta una simple lectura de la Ley de Gobierno Digital en sus artículos 30 y siguientes y del Reglamento de 2021 para observar la importancia justificada que la normativa peruana ha otorgado a este principio estructural.

Con carácter general, la doctrina ha señalado dos ámbitos en relación a los cuales se debe promover un adecuado nivel de seguridad, señalando asimismo los instrumentos que han de utilizarse para promover el correcto cumplimiento de las garantías. De un lado, la seguridad de la actividad administrativa electrónica debe garantizar la correcta protección de los datos de carácter personal. En este ámbito, resultará trascendental el establecimiento de un adecuado nivel de seguridad en la infraestructura en red (Intranet) que interconecte las distintas Administraciones públicas, para que los intercambios de datos, documentos y certificaciones entre ellas puedan realizarse de manera segura lejos de ataques e injerencias externas (Fondevilla Antolín, 2017). De otro lado, se ha puesto el énfasis en el establecimiento de protocolos o estándares de actuación que garanticen un adecuado nivel de seguridad en materia de autenticidad, confidencialidad, integridad, disponibilidad y conservación de las actividades desarrolladas en el marco de los procedimientos administrativos y que deban ser objeto de archivo electrónico. De hecho, la normativa de Perú, y especialmente el Reglamento así procede en sus artículos 94 y siguientes, donde configura el marco de seguridad digital del Estado peruano y todas las cuestiones técnicas relacionadas con la gestión de la seguridad, de una forma amplia y precisa.

2.3. Otros principios: accesibilidad — usabilidad, neutralidad y proporcionalidad

Adicionalmente a los importantes principios de interoperabilidad y seguridad, también resultan de interés otros principios para la correcta articulación de la e-Administración. De hecho, tanto la Ley de Gobierno Digital de Perú en su artículo 5 como el Real Decreto 203/2021 en España, artículo 2, han venido a enunciar los principios básicos que

también deben tenerse en consideración, adicionalmente a los ya citados de seguridad e interoperabilidad. En concreto, y centrándonos en la regulación española, podemos destacar lo siguiente⁷:

En primer lugar, la letra a) de este artículo se refiere a *los principios de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías y sistemas de comunicaciones electrónicas*. La incorporación de este principio en el Decreto 203/2021 supone una innovación interesante ya que el principio de neutralidad tecnológica había sido eliminado casi por completo de las Leyes 39 y 40 de 2015 (sólo se encuentra una referencia en ambas Leyes en la regulación de las sedes electrónicas en el artículo 40 de la LRJSP) especialmente por su difícil consecución técnica. Ahora, el reglamento lo recupera con acierto a fin de:

Garantizar tanto la independencia en la elección de las alternativas tecnológicas necesarias para relacionarse con las Administraciones Públicas por parte de las personas interesadas y por el propio sector público, como la libertad para desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado.

La base para asegurar que este principio se cumpla es la utilización de estándares abiertos por el sector público, aunque esta regla general se encuentra matizada como así sucedía en la ya derogada LAECSP por la incorporación de la excepción del uso de "estándares que sean de uso generalizado" pero siempre (y esto sí lo determina expresamente el Reglamento a diferencia de la LAECSP), "de forma complementaria". De esta manera, el uso de estándares abiertos será imperativo, aunque de forma complementaria se habilite la utilización de otro tipo de software, de manera que se garantice que "las herramientas y dispositivos que deban utilizarse para la comunicación por medios electrónicos, así como sus características técnicas, serán no discriminatorios, estarán disponibles de forma general y serán compatibles con los productos informáticos de uso general".

En segundo lugar, las letras b) y c) del artículo 2 se refieren a *los principios de accesibilidad y de usabilidad o facilidad de uso*, que a mi juicio se insertan dentro del mismo principio general de acceso al modelo de e-Administración. De un lado, "el principio de accesibilidad, entendido como el conjunto de principios y técnicas que se deben respetar al diseñar, construir, mantener y actualizar los servicios electrónicos para garantizar la igualdad y la no discriminación en el acceso de las personas usuarias, en particular de las personas con discapacidad y de las personas mayores". Y, de otro lado, y en íntima conexión "el principio de facilidad de uso, que determina que el diseño de los servicios electrónicos esté centrado en las personas usuarias, de forma que se minimice el grado de conocimiento necesario para el uso del servicio". A mi juicio, y aunque ni las Leyes 39 y 40 de 2015 ni ahora el Decreto 203/2021 hagan mención alguna a la normativa reglamentaria que regula las cuestiones de accesibilidad y usabilidad desde 2007, el establecimiento de estos principios en el Reglamento supone que las obligaciones, derechos y garantías establecidos en el Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social deben tenerse obligatoriamente en cuenta por las Administraciones y organismos del sector público a la hora de diseñar y financiar el desarrollo de herramientas de e-Administración (Martínez Gutiérrez, 2009, pp. 65 y ss.).

Y, en tercer lugar, respecto a los principios aquí referenciados, la letra e) del artículo 2

7 En este punto, sigo lo establecido en mi trabajo Martínez Gutiérrez, R. (2021).

enuncia el principio de proporcionalidad, "en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos". Se trata de un principio de capital importancia y que debe ser considerado en todos los instrumentos del modelo de e-Administración, y especialmente en materia de registros, comunicaciones y notificaciones y con especial intensidad en materia de identificación y firma electrónicas⁸. La importancia de este principio se ha puesto de manifiesto también en la Ley 40/2015 (aunque ciertamente con menor intensidad de la que se predicaba en la Ley 11/2007) y, en esa línea, este principio se ha materializado en el artículo 4 relativo a los "principios de intervención de las Administraciones Públicas para el desarrollo de una actividad", al determinar en su apartado 1º que:

Las Administraciones Pùblicas que, en el ejercicio de sus respectivas competencias, establezcan medidas que limiten el ejercicio de derechos individuales o colectivos o exijan el cumplimiento de requisitos para el desarrollo de una actividad, deberán aplicar el principio de proporcionalidad y elegir la medida menos restrictiva, motivar su necesidad para la protección del interés público así como justificar su adecuación para lograr los fines que se persiguen, sin que en ningún caso se produzcan diferencias de trato discriminatorias. Asimismo deberán evaluar periódicamente los efectos y resultados obtenidos.

Como se puede comprobar, se trata de adecuar el nivel de exigencias en los trámites y actuaciones de las personas interesadas con las Administraciones a la naturaleza de la actuación a realizar, de manera que no se exijan requisitos desproporcionados para realizar trámites sencillos.

3. GARANTÍAS Y DERECHOS DE LAS PERSONAS. EN ESPECIAL, EL DERECHO A NO APORTAR DATOS Y DOCUMENTOS

3.1. Los derechos en el modelo de e-Administración en la legislación española

En España, la Ley 39/2015 de procedimiento administrativo común ha establecido 2 artículos en los cuales se regulan los derechos. De un lado, el artículo 13 establece los derechos genéricos que tienen todas las personas ante las Administraciones, a los que, de otro lado, se deben añadir los establecidos en el artículo 53 de la Ley que se refiere a los derechos específicos de las personas interesadas en la tramitación de los procedimientos. Para un estudio amplio de los derechos en España, me remito a mi trabajo *El régimen jurídico del nuevo procedimiento administrativo común*. En este artículo, me centraré en el derecho establecido en el artículo 53.1 letras c) y d) que analizaremos a continuación.

3.2. El derecho clave a no aportar datos y documentos por las personas interesadas. El acceso al dato mínimo necesario para la tramitación: su regulación en España.

Las letras c) y d) del artículo 53.1 de la LPAC establecen los derechos a no presentar documentos originales y a no presentar datos y documentos no exigidos por las

8 Esta circunstancia ha sido puesta de manifiesto por la doctrina, por citar un buen trabajo clásico que lo vincula a la identificación y firma electrónicas, véase: Martín Delgado, I. (2008). Identificación y autenticación de los ciudadanos. En Valero Torrijos, J., y Gamero Casado, E. (Coords.). La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Pùblicos. Thomson-Aranzadi.

normas aplicables al procedimiento de que se trate, que ya se encuentren en poder de las Administraciones Públicas o que hayan sido elaborados por éstas. El cumplimiento de estos derechos es clave para poder considerar implantada la e-Administración, es decir, podremos afirmar que ya está plenamente en funcionamiento el nuevo modelo de administrar cuando estos derechos estén garantizados.

En primer lugar, la letra c) del artículo 53 de la LPC se refiere expresamente a la primera categoría documental cuya presentación no debe exigirse a las personas interesadas, al regular el derecho “a no presentar documentos originales salvo que, de manera excepcional, la normativa reguladora aplicable establezca lo contrario”. Hemos de tener en consideración de que el legislador se refiere aquí a documentos originales, sin distinguir entre si se trata de documentos públicos no administrativos o administrativos, o privados, aunque viendo que en la letra d) habla de documentos elaborados por las Administraciones (deben entenderse ahí los documentos públicos administrativos originales), la lógica indica que esta letra c) se tenga que referir a documentos originales privados, documentos públicos no administrativos o, en último lugar, a documentos públicos administrativos cuyos originales no obren en los archivos de la Administración que los produjo y se encuentren en poder de la persona interesada. Pues bien, a pesar de que el legislador instaura el derecho a no aportar documentos originales, matiza al respecto que “en caso de que, excepcionalmente, deban presentar un documento original, tendrán derecho a obtener una copia autenticada de éste”.

En segundo lugar, la letra d) del artículo 53.1 configura el derecho “a no presentar datos y documentos no exigidos por las normas aplicables al procedimiento de que se trate, que ya se encuentren en poder de las Administraciones Públicas o que hayan sido elaborados por éstas”. Respecto a este derecho debemos realizar las siguientes matizaciones: 1. El derecho a no presentar estos datos y documentos se refiere a datos y documentos obrantes o elaborados en o por cualquier Administración pública. 2. Este derecho implica que todas las Administraciones públicas deban articular sus archivos electrónicos únicos bajo los parámetros de interoperabilidad y seguridad, custodiando en los mismos los documentos que elaboren pero también aquellos obrantes en los expedientes de los procedimientos administrativos ya tramitados. 3. Este derecho de las personas a no presentar estos datos y documentos constituye una auténtica obligación para todas las Administraciones públicas de colaborar en el intercambio de datos y documentos, así como también de interconectarse a través de redes seguras e interoperables como la Red SARA y TESTA. 4. Para un correcto ejercicio de este derecho es imprescindible el respeto a la normativa de protección de datos de carácter personal española y de la Unión Europea, y sería conveniente en consecuencia avanzar hacia sistemas de intercambio de información y datos basados en el principio de acceso al dato mínimo necesario para la tramitación de la actuación o del procedimiento concreto de que se trate, siendo estos mecanismos más garantistas con la tutela del derecho fundamental a la protección de datos de carácter personal que el acceso a los documentos completos.

Pues bien, con este marco de derechos, y en relación al intercambio y transmisión electrónica de datos entre Administraciones con utilización de las plataformas y sistemas intranet a través de la interoperabilidad, podemos identificar dos mecanismos de obtención de los datos necesarios: las comunicaciones electrónicas (que requieren un control *ex ante*) y los accesos directos automatizados, en los que caben dos posibilidades: a) el órgano que tramita el procedimiento accede al archivo electrónico de la Administración cedente, con carácter general tras autorización de la persona interesada, y obtiene el documento o documentos necesarios; y, b) El órgano que tramita el procedimiento, también con carácter general con consentimiento de la persona interesada, contrasta contra la base de datos del archivo electrónico de la Administración cedente de los datos o documentos si el interesado

cumple o no con los elementos exigidos en la solicitud y para cuya comprobación se requiere la cesión de los datos (por ejemplo, en este supuesto hablamos de que si para el otorgamiento de una ayuda o subvención es necesario comprobar si la persona interesada está por encima o por debajo de 12.000 euros de renta, la Administración solicitante no tenga porqué disponer de todo el documento de renta de esa persona, sino sólo si está por encima o por debajo de 12.000 euros; o, si fuese necesario comprobar si una persona es licenciada o no, que el órgano que tramita el procedimiento pueda realizar una comprobación automatizada directamente contra la base de datos del registro de títulos universitarios del Ministerio, funcionalidad de la Red interoperable SARA, que le indique si la persona interesada tiene o no el título de licenciado sin necesidad de obtener copia del documento del título). En estos supuestos, dado que el control de la adecuada cesión de datos se producirá a posteriori es preciso que quede constancia en los ficheros del cedente y del cesionario del acceso a los datos o documentos efectuado por el cesionario.

Evidentemente, la modalidad de acceso directo es más ágil que la de comunicación electrónica y, a su vez, si la misma se realiza mediante el sistema de acceso al dato mínimo necesario descrito en la letra b) del párrafo anterior, la transmisión electrónica de datos será mucho más garantista con la protección de datos personales de la persona interesada y con el principio de transparencia en la gestión de los procedimientos. En esta línea, debe mencionarse muy positivamente el Reglamento General de UE Protección de Datos de 2016 y la Ley Orgánica de protección de Datos y Garantía de Derechos Digitales de 2018, ya que establecen el denominado principio de minimización de datos (artículo 5.1.c del RGPD) que se desarrolla en el artículo 25 del RGPD sobre la base de la “protección de datos desde el diseño y por defecto”, cuya finalidad parece ser que en las transmisiones de datos no se obtenga más información y datos que los absolutamente necesarios para lo cual los archivos y bases de datos deberán diseñarse con ciertos parámetros técnicos que permitan dichas posibilidades técnicas, es decir, lo que aquí hemos denominado como acceso al dato mínimo necesario. Esta nueva vía, sin duda más garantista y adecuada al principio de transparencia y al derecho a la protección de datos de carácter personal, junto con la posibilidad de que las Administraciones puedan intercambiar ciertos datos en los procedimientos iniciados de oficio sin necesidad de consentimiento del interesado cuando nos encontramos ante el cumplimiento de una finalidad pública o una obligación legal vinculada al ejercicio de potestades públicas del órgano a la que parece habilitar la combinación de los artículos 5.1.b), 6.1.c) y e), 6.3, 9.2.g), 23.1.e) y h), y 89.1 del Reglamento General UE de Protección de Datos (y el artículo 28 de la LPAC en determinados supuestos como las facultades de inspección o sancionadoras), es posible que garanticemos un sistema mucho más coherente, seguro y ágil de transmisiones electrónicas de datos que facilite la simplificación administrativa, el desarrollo de procedimientos administrativos más acordes a las posibilidades tecnológicas actuales, la transparencia en la gestión y la privacidad de las personas, redundando todo ello en beneficio de las personas interesadas y de las Administraciones en el cumplimiento y ejercicio de sus funciones y/o misiones de interés público normativamente atribuidas por el ordenamiento jurídico⁹.

4. INSTRUMENTOS BÁSICOS PARA LA TRAMITACIÓN ELECTRÓNICA DE PROCEDIMIENTOS

4.1. Sede electrónica

La sede electrónica puede definirse como “el sitio o portal web de Internet, titularidad de

⁹ A mayor abundamiento véase: Martínez Gutiérrez, R. (2021b). Interoperabilidad = Transparencia + Protección De Datos. En Cátedra Pagoda – Observatorio de Transformación Digital del Sector Público.

una Administración pública, que sirve de plataforma para que los administrados puedan relacionarse con la misma recibiendo servicios públicos o estableciendo procedimientos administrativos electrónicos" (Martínez Gutiérrez, 2009, p.481). Sin duda, una de sus utilidades fundamentales será que sirva para iniciar formalmente los procedimientos a través del catálogo de procedimientos – registro electrónico (además, claro está, de otras funcionalidades como el acceso al expediente, la recepción de notificaciones, etc.). Este elemento básico del modelo de e-Administración tiene una deficiente regulación en la normativa de Perú, prácticamente nula, por lo que vamos a exponer en este apartado el régimen jurídico de España.

El artículo 38 de la LRJSP comienza con el concepto legal de sede electrónica, y determina en su apartado 2 que "el establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma". En base a este precepto, es evidente que las Administraciones públicas serán responsables ante el incumplimiento del "parámetro de calidad": veracidad, integridad y actualización, de la información y servicios de una sede electrónica, responsabilidad que se extiende también a los portales de internet (Valero Torrijos, 2008). Es decir, si ante una información o servicio electrónico prestado en sede incumpliendo el parámetro de calidad se produce un daño antijurídico a la persona interesada, la Administración será responsable de resarcir al perjudicado el daño ocasionado mediante los sistemas de resarcimiento propios de la responsabilidad patrimonial.

De otro lado, también merece la pena destacar la determinación con carácter básico del "contenido y servicios de las sedes electrónicas" que ha establecido el Real Decreto 203/2021 en España. El nuevo reglamento ha establecido con carácter básico el contenido mínimo y servicios de todas las sedes electrónicas lo que es lógico, simplifica la usabilidad y accesibilidad de las personas interesadas en el modelo de e-Administración, y entraña perfectamente con el carácter básico que se desprende del artículo 149.1.18 de la Constitución. De otra parte, el contenido mínimo de información y servicios es ajustado a las necesidades básicas de funcionamiento de una sede electrónica y está ajustado y justificado desde el punto de vista de la práctica administrativa. A este respecto, merece la pena destacar que el artículo 10 en su apartado 1 ha fijado el contenido mínimo de las sedes, y que el apartado 2º del mismo artículo ha delimitado los servicios mínimos que debe prestar toda sede electrónica.

4.2. Oficinas de asistencia en materia de registros y registros electrónicos

En materia de registros, la legislación y normativa de Perú sí se ha ocupado de los registros electrónicos para la recepción de escritos, solicitudes y documentos por medios electrónicos, de una manera razonablemente acertada. No obstante, no ha regulado por el momento y sí sería una necesidad imperiosa la articulación y cambio de paradigma de las oficinas presenciales de registro en oficinas de asistencia a las personas interesadas en el nuevo modelo de administrar. A estos efectos, resulta interesante traer a colación la regulación española de este elemento. Según el artículo 16.5 de la LPAC:

Los documentos presentados de manera presencial ante las Administraciones Públicas, deberán ser digitalizados (...) por la oficina de asistencia en materia de registros en la que hayan sido presentados para su incorporación al expediente administrativo electrónico, devolviéndose los originales al interesado, sin perjuicio de aquellos supuestos en que la norma determine la custodia por la Administración de los documentos presentados o resulte obligatoria la presentación de objetos o de documentos en un soporte específico no susceptibles de digitalización.

De esta manera, las oficinas de asistencia en materia de registro vienen a redefinir las oficinas de registro tradicionales y se dirigen específicamente a prestar servicio a las personas físicas no obligadas a relacionarse electrónicamente con las Administraciones, es decir, a los sujetos no obligados. Además, el artículo 12 de la LPAC regula la “asistencia en el uso de medios electrónicos a los interesados” para “garantizar que los interesados pueden relacionarse con la Administración a través de medios electrónicos, para lo que pondrán a su disposición los canales de acceso que sean necesarios así como los sistemas y aplicaciones que en cada caso se determinen” y también “en lo referente a la identificación y firma electrónica, presentación de solicitudes a través del registro electrónico general y obtención de copias auténticas”. Estas tareas se realizan en España por los funcionarios habilitados “para la identificación o firma” en materia de asistencia a las personas interesadas en las oficinas de registro presenciales, determinándose que “funcionarios que presten servicios en las oficinas de asistencia en materia de registros” serán todos ellos funcionarios habilitados para la identificación y firma de las personas físicas que no tengan obligación de relacionarse electrónicamente con las Administraciones públicas.

Finalmente, el régimen de la presentación a través de registros electrónicos en Perú sí resulta más detallado, y simplemente debemos señalar que en España cuando la persona interesada presenta un documento a través de la sede electrónica, bien sea para iniciar formalmente el procedimiento o por ejemplo para realizar alegaciones o aportar pruebas o informes, debe existir constancia de la efectiva presentación del documento y para ello se emplea el software de registro electrónico. Ahora bien, lo realmente importante es que con el nuevo marco legal de 2015 en España, la tramitación interna de los procedimientos desde su inicio será electrónica, independientemente que el inicio formal del procedimiento se produzca (1) *on line* o electrónicamente desde la sede electrónica – catálogo de procedimientos, cumplimentando el modelo normalizado de solicitud y registrando electrónicamente la solicitud, con el acuse de recibo automatizado correspondiente; o, (2) presencialmente, si la persona interesada es persona física y decide acudir a una oficina de asistencia en materia de registros con los documentos papel de la solicitud y la documentación que la acompaña, y que sea el o los funcionarios habilitados de la oficina los que transformen y digitalicen la documentación, generando las correspondientes copias auténticas electrónicas, iniciando el e-procedimiento.

En esta segunda modalidad de inicio presencial del e-procedimiento interno, los actos de comunicación y notificación entre la Administración y la persona interesada se realizarán en papel, pero toda la tramitación interna será electrónica. Así pues, será indiferente en cuanto a la tramitación electrónica interna del procedimiento si la persona interesada ha iniciado formalmente el mismo desde la sede electrónica (catálogo de procedimientos – registro electrónico) o desde la oficina de asistencia en materia de registro, y, en ambos casos, las anotaciones de los asientos registrales de entrada en el libro de llevanza o archivo – base de datos de registro se deberán realizar en orden secuencial de presentación independientemente del lugar electrónico o presencial de su presentación.

4.3. Expediente electrónico, gestión documental avanzada y archivo

La gestión documental electrónica es imprescindible para el funcionamiento del modelo de Administración electrónica a nivel interno. Si este elemento no se implementa adecuadamente, no es posible articular un sistema de e-Administración eficaz y eficiente. La regulación normativa a este respecto en el ordenamiento de Perú es intensa y adecuada, aunque dispersa. No se regula legalmente en la Ley de Gobierno Digital, sino que su regulación se encuentra en la Ley N° 27444 del Procedimiento Administrativo General,

con una base muy sucinta, encontrándose su desarrollo reglamentario en el reglamento de desarrollo aprobado por Decreto Supremo N° 029-2021-PCM, que paradójicamente no desarrolla la Ley de Procedimiento Administrativo General, donde se establece la base legal de este instrumento, sino que desarrolla la Ley de Gobierno Digital, donde no se ha incorporado regulación del expediente y gestión documental electrónica. Con todo, el reglamento sí contiene una intensa regulación de esta cuestión en sus artículos 35 a 45, partiendo de la definición de los elementos estructurales del documento electrónico y del expediente, la configuración de su índice, los metadatos, la obtención de copias, etc. A mi juicio, el principal problema en este punto es que muchas de las cuestiones establecidas en el reglamento, dada su importancia en la articulación del modelo de Administración electrónica deberían ser objeto de regulación en la Ley.

Precisamente ésta ha sido la realidad en España, donde los aspectos básicos de la gestión documental electrónica se regulan en diferentes momentos de la Ley de Procedimiento Administrativo Común, por ejemplo, las copias en los artículos 26 y siguientes, el expediente en el 70 o el archivo en el 17 (y también en el 46 de la Ley 40/2015). Quizá la cuestión más cuestionable de la regulación legal de España en materia de gestión documental es que la misma no se ha establecido en un solo capítulo de la Ley de Procedimiento, cuestión que sí se ha solventado en el reglamento aprobado por el Real decreto 203/2021.

4.4. Comunicaciones y notificaciones

La notificación es un requisito esencial para dotar de eficacia jurídica a las resoluciones o actuaciones de un procedimiento administrativo, de manera que es uno de los elementos esenciales del modelo de Administración electrónica. Según la Real Academia Española de la Lengua, “notificar” es “comunicar formalmente a su destinatario una resolución administrativa o judicial”. La noción de notificación administrativa no variará según se practique por medios tradicionales o electrónicos. La notificación electrónica “posee, pues, la misma esencia de la notificación convencional” (Martín Delgado, 2005, p. 183). La única variación se produce en el canal de comunicación que emplea la Administración para dar a conocer sus actos o resoluciones administrativas a los interesados. En la notificación electrónica se emplearán los medios electrónicos para proceder a la notificación administrativa del acto o resolución de que se trate, utilizándose para ello un sistema de notificaciones a depositar bien en dirección electrónica habilitada o bien en la sede electrónica de la Administración que notifique (en Perú a través de la “casilla única electrónica”). A través de la notificación administrativa se da a conocer al interesado o interesados en un procedimiento un acto o una resolución administrativa. Así, “la notificación es una conducta administrativa de información a los particulares por medio de la cual éstos pueden conocer el contenido de los actos administrativos y ajustar su conducta a lo que en ellos se establece” (Velasco Caballero, 2002, p. 37). Por todas estas razones, la notificación se considera una garantía esencial del procedimiento, y como tal, los Tribunales la han insertado dentro de la esencia del artículo 24 de la Constitución regulador del derecho a la tutela judicial efectiva (Véase las SSTC 59/1998, de 16 de marzo, FJ 3; 221/2003, de 15 de diciembre, FJ 4; y, STC 55/2003, de 24 de marzo, FJ 2¹⁰).

En relación a este instrumento, en el ordenamiento de Perú, la regulación legal básica del mismo se contiene en la Ley de Procedimiento Administrativo General, aunque también

10 A este respecto, resulta interesante el trabajo de Mayor Gómez, R. (2015). La notificación administrativa en la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas: novedades y cuestiones jurídicas controvertidas.

la Ley de Gobierno digital se refiere a ella en su artículo 22 relativo al “Domicilio Digital”, aunque configurándolo como “uno de los atributos de la identidad digital que se constituye en el domicilio habitual de un ciudadano en el entorno digital, el cual es utilizado por las entidades de la Administración Pública para efectuar comunicaciones o notificaciones”. En materia de notificaciones se produce algo similar a lo acontecido en materia de gestión documental electrónica, dado que el grueso de la regulación se encuentra en el reglamento de desarrollo aprobado por Decreto Supremo Nº 029-2021-PCM, en sus artículos 53 a 62, donde se establece una intensa regulación normativa muy similar a la establecida en España en la Ley de Procedimiento Administrativo Común. Teniendo en cuenta además la trascendencia constitucional de la notificación y su vinculación al derecho fundamental a la tutela judicial efectiva, en materia de notificaciones electrónicas resulta imperioso que el grueso de su regulación se realice mediante Ley, y no solo en la normativa de rango reglamentario, siendo esta la principal carencia que se observa en el ordenamiento de Perú.

4.5. Identificación y firma electrónica

Como ya hemos advertido, la identificación y firma electrónica es uno de los elementos fundamentales de la regulación legal en Perú, junto con la interoperabilidad y la seguridad. De hecho, su regulación en la Ley de Gobierno Digital es muy intensa, y también ha sido objeto de un intenso desarrollo reglamentario por el Decreto Supremo Nº 029-2021-PCM. La normativa legal de Perú, en sus artículos 13 y 14, parte de la distinción entre identificación y autenticación, aunque considera la autenticación como una identificación electrónica reforzada de las personas. No obstante, interesa señalar aquí que, a este respecto, Martín Delgado (2008) ha precisado la distinción entre las nociones de identificación y autenticación o firma de documentos, estableciendo los efectos prácticos que conlleva tal diferenciación. Con el primero de los términos (identificación) se hace referencia a la comprobación de la identidad del firmante, mientras que el segundo (autenticación) se relaciona con el documento firmado. De esta forma, mientras que la identificación estaría relacionada con la vertiente subjetiva de la firma, esto es, la persona del firmante, la autenticación lo estaría con la vertiente objetiva, es decir, el documento (p. 466 y ss.). En este punto, simplemente daremos cuenta de que en España, la base normativa de la identificación y firma electrónica es en realidad una norma de eficacia directa de la Unión Europea, el Reglamento UE 910/2014, del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, conocido comúnmente como Reglamento eIDAS. Una vez aprobado el Reglamento UE 910/2014, y a partir de su entrada en vigor, esta norma tenía primacía respecto a legislación española y en consecuencia deben respetarse todos sus elementos configuradores. Recientemente se ha promulgado la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (LRSEC), donde queda patente la absoluta primacía de la normativa de la UE, como así se determina en el artículo 1 de la Ley al autodefinirse como “complemento¹¹” del Reglamento 910/2014. Por lo que respecta a la regulación jurídica de la identificación y firma en el sector público, debemos estar a lo que determinan los artículos 9, 10 y 11 de la Ley 39/2015, de Procedimiento Administrativo Común, con respecto a la “identificación y firma de los interesados en el procedimiento administrativo”, y a los

11 Este artículo señala: “La presente Ley tiene por objeto regular determinados aspectos de los servicios electrónicos de confianza, como complemento del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE”.

artículos 40 a 45 de la Ley 40/2015, de Régimen Jurídico del Sector Público, que serán los aplicables para la identificación y firma de las Administraciones públicas.

Lógicamente, el régimen de estas dos normas de referencia para el ámbito público deberá interpretarse de conformidad al Reglamento 910/2014 y la Ley 6/2020, y finalmente también, con respecto al e-DNI, la DA 3^a de la LRSEC y los artículos 8 y siguientes de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (en adelante también LOPSC), así como el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica, que desarrollaba la regulación legal del DNI-e. A estas normas también se deben sumar las especificaciones en materia de e-firma contenidas en el Real Decreto 4/2010, por el que se aprueba el Esquema Nacional de Interoperabilidad y el Real Decreto 3/2010 por el que se aprueba el Esquema Nacional de Seguridad. Como se puede observar, en esta materia en España también existe una gran dispersión normativa, que debería ser objeto de revisión. En Perú, realmente, el marco legal básico de la identificación y firma electrónicas está bastante centralizado en la Ley de Gobierno Digital y su desarrollo en el Decreto Supremo N° 029-2021-PCM, ya que el marco legal de gobierno digital es en realidad una regulación legal de identificación, firma, seguridad e interoperabilidad.

5. EL MODELO DE REGULACIÓN LEGAL ADECUADO. PROPUESTAS

Después del análisis realizado del ordenamiento legal de Perú en materia de Administración electrónica, podemos realizar una doble consideración respecto a la regulación actual. De un lado, la regulación legal se encuentra dispersa en diferentes normas: Ley de Procedimiento Administrativo General, Ley de Gobierno Digital, etc. Evidentemente esta situación provoca una cierta inseguridad jurídica, además de que supone una dificultad interpretativa, dando la sensación de que el marco normativo de la Administración electrónica en Perú está construido a golpes y con ciertas tensiones en la regulación. De otro lado, la regulación a nivel legal de los elementos básicos y estructurales del modelo de e-Administración es claramente insuficiente, a excepción de las cuestiones de interoperabilidad, seguridad e identificación y firma electrónicas, ampliamente reguladas en la Ley de Gobierno Digital. Existen importantes instrumentos del modelo de Administración electrónica como la gestión documental (documento, expediente, copias, archivo, etc.), los registros o la notificación electrónica que disponen de una deficiente regulación legal. Es cierto que el Decreto Supremo N° 029-2021-PCM dispone de una regulación amplia y en mayor o menor medida adecuada, pero se trata de una norma reglamentaria y hay cuestiones básicas y estructurales que deben encontrarse normadas en una Ley.

Ante estas dos consideraciones evidentes que ya hemos ido señalando a lo largo del presente artículo, las propuestas de solución son claramente dos. En primer lugar, se debe terminar con la dispersión normativa legal en materia de Administración electrónica. Es necesario proceder a una unificación legal de todos los aspectos de la regulación del nuevo modelo de administrar, con una estructuración y contenido coherente y cohesionado interna y externamente¹², y, de ser posible, evitar lo que ha sucedido en España donde se ha producido una separación legal entre la regulación de la dimensión interna y de la externa en dos leyes que ha provocado una cierta falta de coherencia del modelo regulatorio, por no hablar de que muchos de los instrumentos se han ubicado erróneamente en la Ley que regula una dimensión en la que claramente no encaja (por

12 Quizá una buena referencia de estructuración normativa podría ser la que propuso en mi trabajo Martínez Gutiérrez, R. (2021a, 221 y ss.)

ejemplo, la sede electrónica, instrumento de la vertiente externa, se regula en la Ley 40/2015 que regula la dimensión interna y además se regula separadamente de los registros electrónicos, siendo dos instrumentos que deben interpretarse y regularse de manera uniforme). En segundo lugar, muchos de los aspectos regulados con acierto en el Decreto Supremo N° 029-2021-PCM deberían encontrarse regulados en la Ley, o bien tras una reforma integral de Ley de Gobierno Digital para incorporar todos los aspectos regulatorios de la e-Administración, o bien integrando todos los instrumentos y elementos del nuevo modelo de administrar en una reforma intensa de la Ley de Procedimiento Administrativo General que absorba también la actual regulación de la Ley de Gobierno Digital en materia de interoperabilidad, seguridad e identificación y firma electrónica.

6. ASPECTOS METODOLÓGICOS DEL PROCESO DE IMPLANTACIÓN DE LA E-ADMINISTRACIÓN. PROPUESTAS Y RETOS¹³

Todo proceso de reforma o de adaptación en la Administración implica tener que cumplir con una serie de aspectos metodológicos que permitan planificar el proceso de implantación y lograr los objetivos marcados con la reforma que se emprende. Los principios de buen gobierno y buena administración tienen muchos polos y vertientes, pero sin duda, una de ellas debe ser el análisis estratégico de los procesos de reforma administrativa y la determinación de fórmulas adecuadas para llevarlos a buen término. En el caso de la implantación del modelo de Administración pública electrónica y, en particular, para el diseño, desarrollo y puesta en funcionamiento de procedimientos administrativos electrónicos resulta muy recomendable cumplir con una serie de pautas lógicas y metodológicas que guíen hacia el buen camino el proceso de implantación. Evidentemente estas pautas son necesarias en todas las Administraciones y es conveniente no errar en los pasos si lo que se pretende es comprometer a toda la Administración en el proceso de implantación, que lógicamente sería lo deseable.

Desafortunadamente, las Administraciones públicas no han priorizado en su actuación la implantación correcta de los elementos tecnológicos, de forma que podemos afirmar que se ha producido una brecha entre la manera de actuar de los administrados en sus actuaciones privadas (con un alto componente tecnológico) y su forma de actuar ante las Administraciones (que sigue realizándose en la mayoría de los casos en papel). Las Administraciones deben, en consecuencia, realizar un importante esfuerzo en todos los sentidos para acompañar su forma de funcionamiento a los modos de relación habituales de la actual sociedad que sí se caracterizan por una clara apuesta por el uso de las TIC. No obstante, la adaptación plena de las Administraciones públicas al nuevo modelo de e-Administración es cuestión de poco tiempo, puesto que la sociedad no entenderá en breve otra forma de relación, pública o privada, que no tenga como base la tecnología, es decir, que no se produzca por cauces enteramente electrónicos. Y para ello sería fundamental contar con el apoyo de todos los componentes de la organización administrativa en la que se pretenda implantar la tecnología y la tramitación electrónica de procedimientos como forma habitual de realización de la actuación administrativa.

En este apartado, como se puede comprobar, no nos movemos en el mundo del Derecho sino más bien en la sociología del funcionamiento de las Administraciones, pero es evidente que los responsables de un proceso de implantación de la e-Administración deberían apoyarse en una serie de pautas metodológicas o estratégicas que permitan cumplir con los objetivos del proceso de reforma. Así pues, en estos procesos de implantación de

13 Este apartado viene a condensar el Capítulo VI de mi monografía *El procedimiento electrónico en las Administraciones Locales. Aspectos metodológicos y normativos del proceso de implantación*, del año 2018.

procedimientos administrativos electrónicos deben tenerse en consideración al menos los siguientes aspectos: 1. Liderazgo político e institucional. 2. Planificación de la implantación. 3. Implicación de los órganos administrativos fundamentales de la organización en el proceso en un primer momento, para posteriormente conseguir la implicación del máximo número posible de empleados de la Administración. 4. Modificación de la organización administrativa y su adaptación al modelo de gestión electrónico gracias a vencer el miedo al cambio mediante una adecuada formación. 5. Implantación de las modificaciones primero a nivel interno, dentro de la organización administrativa, y posteriormente a nivel externo, ofertando procedimientos y servicios a los ciudadanos. Y, 6. Inversión económica inicial y apuesta por la reutilización y transferencia de tecnología. Pasemos a analizar cada uno de ellos.

1. Liderazgo político e institucional. Para cumplir de manera exitosa con el objetivo de una adecuada implantación de procedimientos administrativos electrónicos en la Administración resulta imprescindible que exista un liderazgo político e institucional que consiga dar estabilidad al proceso, así como también que genere el necesario consenso para permitir el impulso continuado que requieren este tipo de reformas. La implantación de la e-Administración exige continuidad en el tiempo y un periodo de tiempo de implantación razonable, ya que no se trata solo de cambiar procedimientos en papel por procedimientos electrónicos, el proceso implica también drásticos cambios en la organización administrativa si lo que se pretende es que el proceso tenga elevados niveles de éxito.

2. Planificación de la implantación. Todo proceso de cambio requiere planificación y determinación de unas etapas razonables en las que desarrollar las reformas que se requieran. El equipo inicial que lidere el proceso en la Administración debe realizar una planificación en la que se asienten los aspectos metodológicos que analizaremos a continuación y que deben partir necesariamente de conseguir la máxima implicación de los órganos de la Administración.

3. Implicación de los órganos administrativos fundamentales de la organización en el proceso en un primer momento, para posteriormente conseguir la implicación del máximo número posible de empleados de la Administración. Para conseguir que el proyecto de implantación de la Administración electrónica sea exitoso es necesario que los órganos de máxima responsabilidad en la organización lideren también el proceso. Por esta razón, es recomendable constituir una Comisión de Administración Electrónica en la organización, que quizá pueda partir de comisiones preexistentes en las que ya se aglutinen los órganos de máxima responsabilidad en la Administración (por ejemplo, la Comisión de Valoración Documental y Expurgo, etc.) y en la que deben participar necesariamente órganos como la Secretaría General, la Intervención, la Tesorería, el departamento de Informática y/o Nuevas Tecnologías, la jefatura de Archivo, la Jefatura de Registro, el responsable o responsables de la emisión de notificaciones, la jefatura de personal, los jefes de todos los departamentos, así como también todos aquellos órganos y personas de la Administración que puedan colaborar en la buena marcha del proyecto. Una vez constituida esta Comisión, y aprobada la planificación pormenorizada del proceso, es necesario llegado un momento posterior abrir la Comisión a la participación de todos aquellos empleados públicos que quieran participar del proceso y que tengan ganas de formarse en este ámbito y mejorar el funcionamiento de la Administración para la que prestan servicio.

4. Modificación de la organización administrativa y su adaptación al modelo de gestión electrónico gracias a vencer el miedo al cambio mediante una adecuada formación. Una vez que el mayor número de empleados públicos de la Administración esté dispuesto a

participar en el proceso de reforma, es imprescindible que se realicen cursos de formación del nuevo modelo de Administración electrónica, que permitan vencer las resistencias y miedos al cambio tras la pertinente formación. Es lógico que los empleados públicos puedan tener reticencias al nuevo modelo de administrar electrónicamente si no conocen de forma precisa su régimen jurídico y sus implicaciones, y también es muy posible que con una adecuada formación a los empleados públicos el proceso de transformación sea mucho más eficaz, ya que así tendrán conocimiento para valorar, por ejemplo, qué trámites de un procedimiento que vaya a transformarse a electrónico pueden suprimirse sin una merma de garantías, o qué propuestas de migración del procedimiento son más ajustadas a las necesidades de la tramitación electrónica.

5. Implantación de las modificaciones primero a nivel interno, dentro de la organización administrativa, y posteriormente a nivel externo, ofertando procedimientos y servicios a los ciudadanos. Si algo hemos hecho mal muchas Administraciones ha sido, sin duda, “empezar la casa por el tejado” en la implantación de la e-Administración, volcándonos en tener a disposición de las personas interesadas unos servicios en línea que cuando tenían entrada en la Administración seguían tramitándose en papel. Los cambios deben realizarse en primer lugar a nivel interno, procediendo a la informatización del registro y del archivo, a la puesta en marcha de un trámite y gestor de expedientes electrónicos, etc., en definitiva, acometer la implantación de los procedimientos electrónicos primero a nivel interno, con el apoyo, la formación y la participación directa en la transformación de los empleados públicos, para en una segunda fase ofertar servicios públicos electrónicos y tramitación de procedimientos administrativos completamente electrónicos a las personas interesadas en sede electrónica.

Y, 6. Inversión económica inicial y apuesta por la reutilización y transferencia de tecnología. Los procesos de implantación de la e-Administración y de los procedimientos administrativos electrónicos han sido procesos costosos que muchas veces, por desconocimiento de los propios órganos de la Administración, no se han llevado a término adecuadamente. Para empezar, todo programa o software de tramitación electrónica que las Administraciones contraten debería ser de licencia pública. Esta cuestión no es baladí, y el incumplimiento de la misma ha provocado que muchas Administraciones hayan realizado gastos excesivamente elevados en productos informáticos propiedad de empresas que además les cobran ingentes sumas de dinero por las actualizaciones y mantenimientos. Parece que en los últimos tiempos la situación ha revertido, y que todas las Administraciones que contratan estos servicios lo hacen sobre la premisa de la propiedad de los programas, que además deben cumplir con normativas específicas de seguridad y de interoperabilidad. Gracias a este cambio, ahora es realmente posible la reutilización de tecnología segura e interoperable entre Administraciones tal, que por ejemplo en España se regula en la Ley 40/2015. No obstante, las adaptaciones de programas y plataformas tienen un coste de desarrollo informático del que es necesario que seamos conscientes, a sabiendas de que la inversión económica inicial, si se hacen bien las cosas, conseguirá un retorno económico y de buena gestión que sin duda será muy rentable para la Administración y para los ciudadanos.

REFERENCIAS BIBLIOGRÁFICAS

- Cerrillo i Martínez, A. (2010). Cooperación entre Administraciones Pùblicas para el impulso de la Administración Electrónica. En Gamero Casado, E. y Valero Torrijos, J. (Coords.). *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Pùblicos*. 3ª Ed. Aranzadi-Thomson Reuters.

- Fondevila Antolín, J. (2017). Seguridad. El Esquema Nacional de Seguridad. En Gamero Casado, E. (Dir.). *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*. Tirant Lo Blanch.
- García de Enterría, E., y Fernández Rodríguez, T. R. (2002). *Curso de Derecho Administrativo*. Tomo I. 11º Ed. Civitas.
- Gamero Casado, E. (2009). Interoperabilidad y Administración electrónica: conéctense, por favor. *Revista de Administración Pública*. 179, mayo-agosto.
- Gracia Díaz, M. (2019). *Sociedad de la información, e-Gobierno, e-Documento e interoperabilidad en el contexto de la globalización*. RUA – Repositorio Institucional de la Universidad de Alicante.
- Martín Delgado, I. (2005). Las notificaciones administrativas telemáticas. En Punzón Moraleda, J. (Coord.). *Administraciones públicas y nuevas tecnologías*. Lex Nova. Página 183.
- (2008). Identificación y autenticación de los ciudadanos. En Valero Torrijos, J., y Gamero Casado, E. (Coords.). *La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos*. Thomson-Aranzadi.
- Martínez Gutiérrez, R. (2007). Administración electrónica: origen, definición institucional y contexto actual. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 14.
- (2009). *Administración pública electrónica*. Civitas – Thomson Reuters.
- (2012). Servicio Público electrónico y responsabilidad. *Revista Española de Derecho Administrativo*. 155.
- (2016). *El Régimen Jurídico del Nuevo Procedimiento Administrativo Común*, Thomson Reuters – Aranzadi.
- (2017). Relaciones interadministrativas por medios electrónicos. Interoperabilidad. En Gamero Casado, E. (Dir.). *Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del Sector Público*. Tomo II. Tirant Lo Blanch.
- (2018). *El procedimiento electrónico en las Administraciones Locales. Aspectos metodológicos y normativos del proceso de implantación*. Ed. CEMCI.
- (2019). La interoperabilidad como factor clave y estructural en la internacionalización de la contratación pública. En *Contratación Administrativa Práctica*. Número especial *La LCSP un año después*. Enero.
- (2020). El régimen jurídico de la Administración digital: aspectos procedimentales. En Martín Delgado, I. (Dir.). *El procedimiento administrativo y el régimen jurídico de la Administración Pública desde la perspectiva de la innovación tecnológica*, Iustel – IVAP.
- (2021a). La plena eficacia de la e-administración. Comentario y notas fundamentales del Real Decreto 203/2021, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. *Revista de Derecho Digital e Innovación*, 8, enero-marzo.
- (2021b). Interoperabilidad = Transparencia + Protección De Datos. En Cátedra Pagoda

- Observatorio de Transformación Digital del Sector Público. Disponible en: <https://www.uv.es/catedra-pagoda/es/novedades-1286053802801/Novetat.html?id=1286182132547>
- Mayor Gómez, R. (2015). La notificación administrativa en la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas: novedades y cuestiones jurídicas controvertidas. *GABILEX*, 4, diciembre.
- Valero Torrijos, J. (2008). Responsabilidad de la Administración pública por información publicada en Internet (Comentario a la STSJ de canarias de 25 de enero de 2007). *Aranzadi Social*. 17.
- Velasco Caballero, F. (2002). Notificaciones administrativas: presunciones y ficciones. *Justicia Administrativa*, 16, julio.



LOS DERECHOS DIGITALES FUNDAMENTALES: ¿ES NECESARIA SU RECONFIGURACIÓN EN EL ORDENAMIENTO JURÍDICO?

FUNDAMENTAL DIGITAL RIGHTS: IS THEIR RECONFIGURATION IN THE LEGAL SYSTEM NECESSARY?

ÉDGAR GONZÁLEZ LÓPEZ¹

RESUMEN

El surgimiento de la sociedad digital ha hecho necesario preguntarse si la defensa de los derechos fundamentales en el ámbito digital resulta adecuada bajo los presupuestos clásicos y generales de la Constitución y del ordenamiento jurídico, o si, por el contrario, son requeridas nuevas estipulaciones. En la denominada sociedad de la información, en la cual las tecnologías de la información y las comunicaciones están en constante expansión y evolución, los ciudadanos han preferido ejercitar sus derechos y desarrollar sus relaciones sociales, culturales, religiosas, políticas y económicas en la sociedad digital, más que en la sociedad presencial. Esta realidad hace necesario que los Estados adopten un régimen jurídico especial que otorgue seguridad jurídica y una adecuada protección a los derechos fundamentales. Es el momento de hablar de los derechos digitales fundamentales.

PALABRAS CLAVE

Derechos humanos | Internet | Derechos digitales | Tecnologías de la información y las comunicaciones.

CONTENIDO

Introducción; **I.** Derechos humanos e Internet; **A.** Los peligros o riesgos para los derechos humanos en el Internet; **II.** Perspectivas de acción del Estado en relación con el Internet; **A)** Internet como servicio público o servicio de interés general económico; **A.1.** La calificación de internet como servicio público o servicio de interés general económico;

ABSTRACT

The emergence of the digital society has made it necessary to ask whether the defense of fundamental rights in the digital sphere is adequate under the classic and general assumptions of the Constitution and the legal system, or whether, on the contrary, new stipulations are required. In the so-called information society, in which information and communication technologies are constantly expanding and evolving, citizens have preferred to exercise their rights and develop their social, cultural, religious, political and economic relations in the digital society, rather than in the face-to-face society. This reality makes it necessary for States to adopt a special legal regime that provides legal certainty and adequate protection of fundamental rights. It is time to talk about fundamental digital rights.

KEY WORDS

Human rights | Internet | Digital rights | Information and communication technologies.

1 Magistrado de la Sala de Consulta y Servicio Civil del Consejo de Estado. Profesor de la Universidad Externado de Colombia, en las áreas de derecho administrativo, derecho informático y derecho de las telecomunicaciones. *Este artículo ha sido elaborado con la especial colaboración de los doctores Camilo A. Rodríguez Yong y Cristina Gómez Gracia.

A.2. El derecho de acceso a internet, como el derecho de acceso a la sociedad digital y a los derechos digitales. Un servicio público esencial; **III.** Los derechos en la sociedad digital o derechos digitales: los instrumentos para su protección en las fuentes del derecho; **A.** Los derechos fundamentales y su protección; **B.** Los derechos fundamentales y los derechos digitales en la sociedad virtual; **C.** Los derechos digitales y su protección; **IV.** Conclusiones.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 20 de junio de 2021 y aprobado para su publicación el 2 de septiembre de 2021.

INTRODUCCIÓN

Las nuevas tecnologías, y en particular las Tecnologías de la Información y las Comunicaciones, en adelante TIC, han traído importantes transformaciones en la sociedad y en los ciudadanos, no solo en los aspectos comerciales, sino también en el marco del nuevo ecosistema digital con la creación de nuevas relaciones sociales, políticas, culturales, económicas y personales.

Hay que reconocer que convivimos en una sociedad digital y, a partir de este supuesto, analizar y reconfigurar nuestras relaciones de todo orden y las nuevas realidades que determinan mantener y fortalecer la protección de las personas en cuanto a su dignidad humana, como fuente esencial de todo derecho fundamental. De esta premisa surge la necesidad de determinar si la defensa de estos derechos en la sociedad digital resulta satisfecha bajo los presupuestos clásicos y generales de la Constitución y del ordenamiento jurídico, o si son requeridas nuevas estipulaciones de un pacto social que sostenga y reafirme estos derechos y las consecuentes obligaciones de todos los ciudadanos que permitan garantizar su protección.

Son innegables los beneficios e importantes desarrollos que han aportado las tecnologías y las oportunidades que aún representan en sus dimensiones individual y colectiva, social e institucional. Sin embargo, las nuevas dinámicas que de allí se derivan plantean, en igual medida, un sinfín de retos y riesgos, no solo para los Estados sino también para los individuos e incluso para la humanidad misma, con problemas asociados a la protección de los derechos de las personas y dilemas éticos que ponen en el centro del debate incluso la preservación de nuestra especie.

El internet es el instrumento principal y básico de esta sociedad hiperconectada, a la par de otros desarrollos tecnológicos, tales como la inteligencia artificial, en adelante IA, y el Big Data. El Internet ha sido definido como la red de redes, que “no solo interconecta computadoras, sino que interconecta redes de computadoras entre sí, entendiendo por “redes de computadoras” a un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, líneas telefónicas, etc.) con el objeto de compartir diversos recursos. De esa forma, el Internet es el enlace entre múltiples redes más pequeñas que permite ampliar su cobertura al incorporarlas a una red global (Pedreschi Garcés et al, 2012)².

2 El internet surgió a finales de la década de los años 60, cuando el Departamento de Defensa de los Estados Unidos, con el propósito de intercambiar información militar, creó una red de computadores denominada Defence Advanced Research Projects Agency Network, mejor conocida con el nombre de ARPANET o DARPANET.

Para mediados de la década de los 80, la red ya no era exclusivamente una aplicación militar, pues a ella también podía acceder la academia, situación que dio lugar al surgimiento de la

Frente a esta nueva realidad parece necesario indagar si las estructuras jurídicas que regulan el deber ser de la sociedad y de los derechos de quienes la componen y sus instrumentos de eficacia y de eficiencia son suficientes para la protección de los derechos fundamentales o si se requiere de un nuevo entorno o de modificaciones al marco vigente para reinventarlos, adecuarlos y garantizar su ejercicio.

Parece un mundo de laboratorio que no deja de ser real a pesar de su virtualidad y que deviene del mismo proceso de cambio que, sin darnos cuenta, nos conduce a entregar nuestros derechos y nuestra información, sin límites, a los grandes "mesías", quienes detentan el poder de su creación, de su universalización y de su funcionamiento.

En este orden de ideas, el derecho surge como principal catalizador de los cambios sociales para hacer frente a esta problemática y con el fin de brindar las herramientas necesarias para enfrentar y mitigar los riesgos creados. Todo lo anterior, bajo el entendido de que las complejidades de la materia hacen imperioso que el estudio de las nuevas realidades se realice desde un enfoque multidisciplinario, de tal manera que participen diversas áreas del conocimiento en la identificación de problemas y en la creación de estrategias y soluciones.

Dentro del universo de cuestiones jurídicas que pueden derivarse de estas transformaciones, se encuentra un asunto de gran relevancia para todos los Estados constituidos bajo los principios democráticos: los derechos fundamentales. Al respecto, se puede evidenciar que la visión y concepción tradicional de aquellos derechos inherentes a los seres humanos y dirigidos a garantizar su dignidad han mutado en la sociedad digital. Aún más, se pudiera pensar en nuevos derechos de la misma naturaleza que irrumpen en este universo y que parecen ser necesarios para servir de soporte a los derechos fundamentales tradicionales, como sucede, en especial, con el derecho de acceso universal a internet, en una concepción muy cercana a las obligaciones de servicio universal reconocidas en el sector de las telecomunicaciones y de las TIC.

Para dilucidar si estos derechos fundamentales requieren de una protección distinta a la que ordinariamente se les otorga; o, en otras palabras, si se ven amenazados o desdibujados, en este nuevo mundo de la economía digital, es preciso referirse a los denominados derechos digitales o derechos en la sociedad digital, y algunas consideraciones sobre su desarrollo en derecho comparado.

Para su estudio, este documento aludirá en su primera parte a la relación entre los derechos humanos y el Internet. En un segundo acápite, se analizará el Internet en su dimensión de servicio de interés general o de servicio público, y las discusiones sobre la libertad absoluta o su regulación. En una tercera parte, se hará referencia a los derechos digitales y si realmente es necesaria su configuración en el ordenamiento constitucional o legal, por tratarse de nuevos derechos o nuevas reconfiguraciones de los existentes.

I. Derechos humanos e Internet

Varias consideraciones preliminares, generalmente conocidas, podrían hacerse como presupuesto para el objetivo de este documento:

- Diariamente, a través del Internet millones de personas intercambian información,

National Science Foundation Network (NSFNET). Posteriormente, en la década de los 90, la red extendió su alcance, permitiendo que un número creciente de personas accediera a ella hasta convertirse en lo que conocemos hoy como el internet abierto (Halpin, Hick y Hoskins, 2000, p. 6).

desarrollan su vida social, económica y política, y acceden a servicios públicos y privados. Igualmente, al tiempo que promueve la aparición de nuevos competidores y expande los mercados (McDiarmid y Shears, 2016, p. 37; Mihr, 2017, p. 7), el Internet permite escuchar aquellas voces que no pueden acceder a los medios tradicionales por razones económicas, falta de oportunidades o desinterés en las temáticas que se quieren expresar (Rowland, 2005, p. 55).

- El Internet trasciende las fronteras nacionales y reduce las barreras para el libre flujo de la información, permitiendo así la libre expresión, la participación democrática y el disfrute de otros derechos humanos (McDiarmid y Shears, 2016, p. 31), como el derecho a la educación o a la libertad de empresa, religiosa y de asociación.
- El Internet ha revivido la importancia de la libertad, en particular, la de expresión como una libertad individual. Ha revestido a las personas de un mayor poder, a través de una redistribución radical del control de la información y a una aproximación completamente nueva de la manera como la sociedad opera (Lucchi, 2014, p. 816).
- El Internet se ha convertido, por tanto, en un instrumento esencial para el fortalecimiento y la promoción de los derechos humanos (McDiarmid y Shears, 2016, p.31). Así, por ejemplo, ha contribuido a superar la censura a los activistas en China, a denunciar la represión de las comunidades indígenas en Latinoamérica y a facilitar los movimientos sociales en el mundo árabe (Cerda Silva, 2013, p. 17; Dickinson, 2013, p. 64). En algunos países, el Internet es la única fuente pluralista e independiente de información. En este sentido, constituye un instrumento clave para el movimiento de los derechos humanos (Lucchi, 2014, p. 814).
- El Consejo de Derechos Humanos de las Naciones Unidas ha indicado en múltiples oportunidades que los derechos humanos deben ser protegidos en el Internet (Naciones Unidas, 2012; Naciones Unidas, 2014; Naciones Unidas, 2016; Naciones Unidas, 2018). Por ello, exhortó a todos los Estados a "abordar las preocupaciones relativas a la seguridad en Internet de conformidad con sus obligaciones internacionales en materia de derechos humanos, para garantizar la protección de la libertad de expresión, la libertad de asociación, la privacidad y otros derechos humanos en Internet, entre otras cosas mediante instituciones nacionales democráticas y transparentes basadas en el estado de derecho, de forma tal que se asegure la libertad y la seguridad en la red para que pueda seguir siendo un motor enérgico del desarrollo económico, social y cultural" (Naciones Unidas, 2016).

Asimismo, el señalado órgano ha condenado los abusos y violaciones a los derechos humanos cometidos contra personas por ejercer sus derechos y libertades fundamentales en Internet (Naciones Unidas, 2018).

- Ahora bien, proteger los derechos humanos en el ámbito del Internet no resulta una tarea sencilla, pues pueden presentarse importantes tensiones (Mihr, 2017, p. 9). A manera de ejemplo, en el caso *Packingham v. North Carolina*, la Corte Suprema de los Estados Unidos analizó la validez de una ley que calificaba como delito el que una persona registrada como delincuente sexual (*sex offender*) accediera a una página comercial o a una red social en la web en la que el

delincuente supiera que los menores de edad podían ser miembros o mantener páginas web personales.

La Corte reconoció que, aunque era válido restringir el acceso a información en el Internet con el propósito de proteger a los menores de edad de los depredadores sexuales, el texto de la ley era demasiado amplio, al punto que no solo restringía el acceso a redes sociales, sino también a páginas tan variadas como amazon.com, washingtonpost.com o webmd.com.

Asimismo, señaló la corte que las redes sociales permiten a los usuarios acceder a información y comunicarse con otras personas sobre cualquier tema de su interés. Por lo tanto, al restringirse de manera tan amplia el acceso a la red, se restringe el acceso a recursos que permiten conocer la actualidad, consultar ofertas laborales, compartir opiniones, y explorar de cualquier otro modo el pensamiento y conocimiento humano. Para la Corte "estos sitios web pueden proporcionar quizás los mecanismos más poderosos de que dispone un ciudadano para hacer oír su voz. Permiten a una persona con conexión a Internet "convertirse en un pregonero con una voz que resuena más lejos de lo que podría hacerlo desde cualquier otra tribuna"".

En consecuencia, para la Corte Suprema de los Estados Unidos, prohibir totalmente el acceso a las redes sociales impide a la persona el ejercicio legítimo de los derechos derivados de la Primera Enmienda, lo cual, inclusive, aplica para los delincuentes condenados, quienes pueden obtener importantes beneficios, en particular, si buscan reformarse y llevar una vida lícita.

- En el contexto europeo, el Tribunal de Derechos Humanos de la Unión Europea, en el asunto Jankovskis v. Lituania. (Sentencia núm. 21575/08 del 17 de enero de 2017), estudió el caso de una persona detenida en la cárcel que alegaba la violación de su derecho a recibir información, por no permitírselle acceder a Internet. El Tribunal dio la razón al ciudadano, al considerar que:

El Tribunal es consciente de que en varios instrumentos del Consejo de Europa y otros instrumentos internacionales se ha reconocido el valor de servicio público de Internet y su importancia para el disfrute de una serie de derechos humanos. El acceso a Internet se entiende cada vez más como un derecho, y se han hecho llamamientos para desarrollar políticas efectivas para lograr el acceso universal a Internet y superar la "brecha digital" (véase Kalda, citada anteriormente, § 52). El Tribunal considera que esta evolución refleja el importante papel que desempeña Internet en la vida cotidiana de las personas, en particular porque cierta información está disponible exclusivamente en Internet. De hecho, como ya se ha comprobado en este caso, el sitio web de AIKOS ofrece una amplia información sobre las posibilidades de aprendizaje en Lituania.

(...)

El Tribunal concluye que la injerencia en el derecho de la demandante a recibir información, en las circunstancias específicas del presente caso, no puede considerarse necesaria en una sociedad democrática. (Traducción propia).

Estos ejemplos evidencian las tensiones que pueden surgir entre el acceso al Internet y el goce efectivo de los derechos humanos o fundamentales. Hasta donde surgen los límites

de uno y otro, y como se compenetran y convalidan, teniendo en cuenta que el Internet es la fuente principal de comunicación y, por ende, de la libertad de expresión.

A. Los peligros o riesgos para los derechos humanos en el Internet

De otra parte, el Internet, como cualquier desarrollo tecnológico, conlleva riesgos y peligros para la preservación de los derechos de los ciudadanos en cuanto a su dignidad humana.

A pesar de los grandes beneficios que brinda, el Internet involucra también importantes riesgos para los derechos humanos, en particular en lo que se refiere a los derechos a la libertad de expresión, intimidad y acceso a la información (Pollicino, y Susi, 2019, p. 120; Pollicino, 2019, p. 168). Así, por ejemplo, gracias al Internet se identificaron disidentes políticos en Irán, se intensificó la vigilancia del Estado en Inglaterra y se incrementaron las amenazas a la identidad cultural de las personas (Cerda Silva, 2013, p. 18).

Asimismo, el Internet puede ser utilizado para la realización de actividades ilícitas como la pornografía infantil, la trata de personas o la incitación al odio (Hussain, 2000, p. xi; Sereno, 2013, p. 95). También puede promover la censura o invadir indebidamente la intimidad de las personas, por ejemplo, a través del robo de información privada (números de identificación personal, cuentas bancarias y tarjetas de crédito, etc.) (Sinclair, 2015, p. 292).

El derecho a la intimidad o a la privacidad resulta fundamental para la expresión, crítica, opinión y decisión política, y, en términos generales, para la realización de la democracia deliberativa (Mavriki y Karyda, 2020, p. 7). Con todo, el Internet, a través de los datos personales que allí se recopilan, impacta la privacidad y el ejercicio de la vida económica y política de los ciudadanos.

Así, el Internet permite que actores públicos y privados supervisen y reúnan información sobre las comunicaciones y las actividades desplegadas por los usuarios, en claro detrimento de su privacidad (Cerda Silva, 2013, p. 18). El uso de la red genera datos que al ser debidamente analizados permiten conocer más información de la que el propio usuario se imagina o anticipa (hábitos de compra, preferencias de lectura y música, personas con quien se comunica, intereses y hobbies, etc.) (Waldo, Lin, y Millett, 2007, p. 89).

En esta dirección, los GPS proveen información casi en tiempo real de la ubicación de un vehículo, así como de su velocidad, lo que permite monitorear el comportamiento de los conductores. Por su parte, los teléfonos celulares pueden ser usados para determinar con un alto grado de precisión la localización de una persona (Waldo, Lin, y Millett, 2007, p. 89).

Un ejemplo ilustrativo es el caso de China, Estado con el cual proveedores del servicio de internet como Yahoo, MSN y Google suscribieron acuerdos a través de los cuales se comprometieron a censurar contenidos en sus sitios web y motores de búsqueda, así como a entregar los nombres de los usuarios que publicaran contenidos ofensivos. La entrega de dicha información llevó al arresto y detención de disidentes que usaban la red para informar a los ciudadanos sobre las acciones del gobierno (Dickinson, 2013, p. 90).

De esta suerte, la dinámica y estructura del Internet impacta de manera profunda en la intimidad de las personas, lo que ha llevado a algunos a considerar que lo que realmente existe en la red es una “privacidad pública” (Mihr, 2017, p. 15).

Generalmente, cuando usamos las redes sociales se considera que nuestra actividad se desarrolla de manera anónima o dentro del círculo íntimo de nuestros amigos. Lo mismo ocurre cuando depositamos datos privados (cuentas bancarias, número de identificación personal, etc.) en páginas web que requieren de una clave para su acceso. Sin embargo, al utilizar la red dejamos datos o rastros que pueden llegar a ser compartidos con el público, en caso de que estos no se protejan adecuadamente o sean vendidos o "hackeados".

De esta suerte, redes sociales como Facebook o Instagram son, por un lado, anónimas, pero por el otro, instrumentos a través de los cuales transferimos una gran cantidad de datos personales (Mihr, 2017, p. 16).

La problemática surgida a través de los datos y el mito de su gratuidad muestra la situación actual de indefensión de muchos ciudadanos sobre sus derechos fundamentales como la privacidad o su intimidad, y si, su simple manifestación con un sí o con una equis, en un formato presentado y elaborado por el dueño de la plataforma, como requisito excluyente y necesario para ejercer su derecho a la comunicación y a su libertad de expresión, resultan suficientes para determinar la validez del acuerdo frente a las diferencias abismales entre la posición del simple usuario y la posición de dominio y manipulación, en algunos casos, que detenta el operador de la plataforma y de los contenidos.

Diferenciar entre lo público y lo privado se vuelve algo complejo en la red. En el Internet vendemos nuestra privacidad a través de una nueva moneda: nuestros datos personales. El nuevo dólar son nuestros datos. Con ellos pagamos servicios que asumimos se ofrecen de manera gratuita (Google, Facebook, Alibaba, WhatsApp, etc.). La gran diferencia con la moneda que usamos en el mundo real es que en el Internet no tenemos el control del producto que pagamos con nuestro "dinero", y, por lo tanto, tampoco de nuestro "capital" en el mundo virtual. En la actualidad, el ciberespacio es una especie de mercado financiero de datos, en el cual no sabemos a dónde irá a parar nuestra información personal (Mihr, 2017, p. 17).

Dentro de este marco, la privacidad en el ciberespacio debe entenderse como la posibilidad de usar el Internet con un propósito privado, sin el miedo de que terceras personas, tales como los gobiernos o las compañías (agencias de inteligencia, Google, Microsoft, etc.) accedan, vendan o publiquen nuestros datos sin nuestro consentimiento (Mihr, 2017, p. 16).

Con el desarrollo del Internet, los datos se han convertido en un asunto de gran relevancia para el Estado y han contribuido a reconfigurar la relación entre este y los ciudadanos. Para una parte de la doctrina, "nunca ha habido un estado, reino, gobierno o corporación en la historia "que haya tenido el control de datos tan granulares, inmediatos, variados y detallados sobre los sujetos y objetos que les conciernen"" (Mavriki y Karyda, 2020, p. 4). Estas consideraciones se acercan mucho al peligro del "Gran Hermano", plasmado en la novela de 1984 de George Orwell.

Su inmenso poder en el mundo social y en los derechos políticos permite preguntarse si efectivamente el Internet y los desarrollos y plataformas soportadas en el mismo no pueden ni deben tener regulación o interferencia alguna, como se plantea por algunos, o si su extralimitación en el ejercicio y en la transparencia y certeza de la información presentada pueden ser un atentado al ejercicio de derecho fundamentales vinculados al derecho a elegir y a ser elegido.

En efecto, en el campo de la actividad política, los datos de las redes sociales son

particularmente valiosos, pues proveen información sobre la opinión de las personas en relación a la política y a las fuentes de información que utilizan. Asimismo, permiten tomar decisiones estratégicas en situaciones políticas específicas. Igualmente, a través del análisis de los datos en la red, las compañías, partidos políticos, grupos de interés y otras instituciones pueden influir en la conducta política de las personas (Mavriki y Karyda, 2020, pp. 6-12).

La manipulación de nuestras decisiones económicas, políticas o de cualquier otra naturaleza a través del Internet se realiza a través del uso de algoritmos y "bots", frente a los cuales la doctrina ha señalado:

Los bots son programas basados en algoritmos que actúan como "robots humanos" en Internet y cuyo objetivo es maniobrar, intervenir, moderar o simplemente manipular las opiniones y los "Me gusta" del público. Estos bots filtran la información y proporcionan nuestra propia "burbuja de privacidad o cámara de eco" en nuestro Facebook privado, WhatsApp, Instagram o Twitter. Nuestra cuenta privada de Internet o de correo electrónico se ha convertido, de un modo u otro, en objeto público de los bots sociales. Estos bots proporcionan datos, anuncios, propaganda, información o noticias que influyen en nuestro comportamiento de opinión, voto, consumo y compra. Son nuestros "algoritmos mentales" que orquestan nuestras mentes en lo que creemos que necesitamos o queremos, ya sea que esté o no basado en necesidades reales y en la verdad" (Mihr, 2017, p. 21).

De esta suerte, los algoritmos y bots moldean nuestras preferencias para crear o influir nuestras percepciones y decisiones. Debido a su creciente influencia, algunos han señalado que "con el tiempo, incluso el imperio de la ley podría ser sustituido por el imperio de los algoritmos" (Wischmeyer, 2019, p. 170).

Como se planteó en las consideraciones iniciales, puede ser que el derecho de acceso igualitario a Internet en el marco de lo que corresponde al acceso o servicio universal se configure como un derecho fundamental del ciudadano, como soporte o instrumento básico para el ejercicio de esos derechos en este mundo virtual.

Dentro de este marco, resulta de gran importancia asegurar dicho acceso, habida cuenta que la realización de algunos derechos puede verse afectada cuando el uso de la red se limita o restringe a un pequeño grupo o élite y, de esta manera, profundizar así la brecha digital.

La disparidad en el acceso al Internet crea un sistema paralelo: por un lado, están aquellas personas que acceden a la información a un bajo costo y a una alta velocidad. Por el otro lado, se ubican las personas que no pueden acceder al Internet con la misma facilidad que el grupo anterior debido a barreras como el costo del servicio o la falta de instrumentos para hacerlo (Paré, 2015, p. 86). Esta situación conlleva, por lo tanto, a que no gocen de las mismas oportunidades y disfruten de la misma manera los beneficios que se derivan del Internet.

Otro importante riesgo en el ecosistema del Internet es que los operadores de los servicios pueden influir en la manera como las personas accedemos, recibimos y compartimos la información en la red (Belli, 2016, p. 13).

Difícil no reconocer el poder de las plataformas tecnológicas como entidades mediadoras que crean valor y facilitan la interacción entre agentes que operan en distintos lados de un mercado digital de dos o múltiples caras (Hoelck y Ballon, 2015, p. 51, citado

por Pérez Martínez y Martín Núñez, 2017, p.1288). Estas plataformas incorporan un control de acceso a los recursos y servicios denominados “gatekeeper”, es decir, bajo condiciones impuestas y eliminando soluciones alternativas de otros agentes. Además, se apoyan en recursos tecnológicos, en una inversión no replicable, o en externalidades de red que tienen la típica naturaleza de facilidades esenciales o “essential facility”.

Esta tendencia a la concentración y a la retención de usuarios para maximizar el valor de sus servicios viene acompañada generalmente de la tendencia a integrarse verticalmente para ocupar un puesto en cada una de las cadenas de valor del ecosistema digital. Como lo señalan Pérez Martínez y Martín Núñez (2017, pp. 1287-1288), este fenómeno de plataformaización, sumado a la dinámica de “winner takes all”, muestran unos mercados de desarrollo exponencial de inmenso poder en los derechos de los ciudadanos. Se citan como ejemplos los casos de Google o Apple.

Dentro de este marco, el Parlamento Europeo ha destacado la importancia de las plataformas en el flujo e intercambio de información. Así, en la Resolución del 20 de octubre de 2020, por medio de la cual se hicieron recomendaciones a la Comisión sobre una Ley de Servicios Digitales ([2020/2019\(INL\)](#)), el Parlamento indicó:

Considerando que las plataformas de alojamiento de contenidos pueden determinar qué contenido se muestra a sus usuarios, influyendo así de forma significativa en la manera de obtener y comunicar la información, hasta el punto de que esas plataformas se han convertido de facto en espacios públicos en la esfera digital; que los espacios públicos deben gestionarse protegiendo los intereses públicos y respetando los derechos fundamentales y los derechos civiles de los usuarios, en particular el derecho a la libertad de expresión y de información.

La adopción de medidas por parte de los proveedores del servicio de internet para aumentar o disminuir el acceso a determinadas páginas web puede llevar a que la facultad del usuario de escoger qué leer, a donde ir, etc., sea una mera ilusión. A través de medidas de ese tipo, los usuarios pueden terminar accediendo a información o contenido al que de otra manera no hubieran accedido.

Estos graves riesgos no desdicen de los grandes beneficios y posibilidades que ofrece el Internet, tales como su velocidad, alcance global y relativo anonimato. Así, por ejemplo, gracias al Internet, es posible movilizar un gran número de personas o informar al mundo en tiempo real sobre violaciones a los derechos humanos, tales como masacres, desaparecimientos o arrestos masivos (Hussain, 2000, p. xi).

Situaciones como las descritas han llevado a que algunos gobiernos impongan restricciones al Internet con el propósito de bloquear contenidos o vigilar y detectar activistas o críticos del régimen. Igualmente, han consagrado como delitos la expresión de opiniones en la red, lo cual se ha acompañado de la expedición de normas especiales para sustentar dichas medidas (Naciones Unidas, 2011, p. 8). Dentro de los Estados que desarrollan técnicas de bloqueo para acceder a la información ubicada en la red se encuentran China, Turquía, Myanmar (Burma), Bielorrusia, Uzbekistán, Siria y Arabia Saudita, entre otros (Deibert y Villeneuve, 2005, pp. 111-124).

De esta suerte, el Internet no se encuentra por fuera del poder y el control del Estado. Así como existen barreras físicas que marcan los límites entre los países, los Estados buscan crear límites informacionales en el ciberespacio, a través de la creación e implementación de estrategias tecnológicas y jurídicas para controlar el flujo de información en el Internet (Deibert y Villeneuve, 2005, p. 111). Todas estas acciones impactan negativamente los

derechos humanos, especialmente los relacionados con el acceso a la información y la libertad de expresión (McDiarmid y Shears, 2016, p. 36).

De otra parte, en relación a la protección de los derechos humanos en el Internet, es importante destacar que, aunque los Estados son los llamados en primer lugar a su efectiva protección, en la actualidad se evidencia una creciente participación de los particulares en esta tarea, lo que inclusive ha llevado a algunos a afirmar que estos cumplen un papel quasi judicial (Bassini, 2019, p. 186).

La responsabilidad de las plataformas digitales, especialmente de las que permiten la búsqueda de información, ha sido reconocida por la jurisprudencia europea teniendo en cuenta su papel fundamental en la difusión global de los datos. En línea con lo anterior, dichas plataformas pueden afectar los derechos fundamentales a la privacidad y al habeas data.

Así, el Tribunal de Justicia Europeo señaló en el caso Google v. Agencia Española de Protección de Datos (AEPD) (asunto C-131/12):

80. A este respecto, debe señalarse, en primer lugar, que, como se ha afirmado en los apartados 36 a 38 de la presente sentencia, un tratamiento de datos personales como el controvertido en el litigio principal, efectuado por el gestor de un motor de búsqueda, puede afectar significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales cuando la búsqueda realizada sirviéndose de ese motor de búsqueda se lleva a cabo a partir del nombre de una persona física, toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada, que, sin dicho motor, no se habrían interconectado o sólo podrían haberlo sido muy difícilmente y que le permite de este modo establecer un perfil más o menos detallado de la persona de que se trate. Además, el efecto de la injerencia en dichos derechos del interesado se multiplica debido al importante papel que desempeñan Internet y los motores de búsqueda en la sociedad moderna, que confieren a la información contenida en tal lista de resultados carácter ubicuo (véase, en este sentido, la sentencia eDate Advertising y otros, C509/09 y C161/10, EU:C:2011:685, apartado 45).

Frente a estos peligros que bordean la red de redes para los derechos del tratamiento de datos personales y los que se derivan del mismo, se cuestiona igualmente la manera efectiva de garantizarlos y si dichas facultades pueden atribuirse a la plataforma privada o a una autoridad pública que tenga una competencia legal.

En la práctica, las plataformas privadas han asumido de facto facultades que normalmente están radicadas en cabeza de las autoridades públicas, como las cortes o las autoridades administrativas (Bassini, 2019, p. 186). Así, plataformas como Twitter o Facebook bloquean mensajes o cuentas de los usuarios cuando los mensajes transmitidos, a juicio de las mismas plataformas, atentan contra sus términos y condiciones. A manera de ejemplo, puede mencionarse lo acontecido con los expresidentes de los Estados Unidos y de Colombia, Donald Trump y Álvaro Uribe, casos ampliamente divulgados en los medios de comunicación.

Frente a la actuación de los particulares, una parte de la doctrina considera que estos no deben gozar de facultades para valorar el contenido de lo que se manifiesta en la red. Por su parte, una postura contraria, considera que ellos sí deben hacerlo (Susi, 2019, p. 199).

La postura que aboga por la no valoración del contenido por parte de las plataformas está en concordancia con lo manifestado recientemente por el Parlamento Europeo, el cual indicó:

Considerando que la defensa de la ley en el mundo digital no solo implica el respeto efectivo de los derechos fundamentales, en particular la libertad de expresión y de información, la intimidad, la protección y la seguridad, la no discriminación, el respeto de la propiedad y los derechos de propiedad intelectual, sino también el acceso a la justicia y a la tutela judicial efectiva; que delegar en empresas privadas decisiones sobre la legalidad de los contenidos o de las competencias en materia de aplicación del Derecho socava la transparencia y el respeto de las garantías procesales, lo que conduce a un enfoque fragmentado; que, por lo tanto, es necesario un procedimiento judicial acelerado con las garantías adecuadas a fin de asegurar la existencia de vías de recurso eficaces (Resolución del 20 de octubre de 2020, por medio de la cual se hicieron recomendaciones a la Comisión sobre una Ley de Servicios Digitales: adaptación de las normas de Derecho mercantil y civil a las entidades comerciales que operan en línea (2020/2019(INL)).

Con anterioridad, pero en la misma dirección, el relator especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión de las Naciones Unidas, Frank La Rue, había señalado:

Las medidas de censura nunca deben delegarse en una entidad privada, y que no debe responsabilizarse a nadie de contenidos aparecidos en Internet de los cuales no sea el autor. De hecho, los Estados no deben hacer uso de intermediarios ni ejercer presión sobre ellos para que censuren en su nombre, como ocurre en la República de Corea con la creación de la Comisión de Normas de las Comunicaciones de Corea, entidad semiestatal y cuasiprivada encargada de regular el contenido en línea.

Igualmente, el relator también indicó que los proveedores privados de los servicios de internet influyen como nunca antes en los derechos a la libertad de expresión y acceso a la información. De allí que resulte fundamental establecer medidas para evitar que el sector privado, contribuya o sea cómplice de violaciones a los derechos humanos (Naciones Unidas, 2011, p. 4).

Como corolario de estas vicisitudes se plantea nuevamente la prioridad del derecho de acceso a Internet:

Se han propuesto distintas alternativas con el propósito de contrarrestar los riesgos que los derechos humanos enfrentan. Así, algunos han señalado que el acceso al Internet debe considerarse una prioridad en las agendas nacionales e internacionales. En el caso de los países desarrollados, sus esfuerzos deben dirigirse a asegurar dicho acceso de una manera equitativa entre los distintos segmentos de la población. Por su parte, los países en desarrollo deben trabajar en iniciativas orientadas a actualizar su infraestructura en materia de TIC y aumentar sus redes (Paré, 2015, p. 87).

Asimismo, con el propósito de enfrentar la desigualdad en el acceso, algunos países han reconocido al Internet como un derecho universal o como un derecho fundamental. Estonia, Francia, Costa Rica, Finlandia, son algunos ejemplos de ello (Iftimiei, 2017, p. 48; Naciones Unidas, 2011, p. 4).

El Derecho a acceder a Internet comprende dos elementos: por una parte, el acceso, con algunas excepciones, a los contenidos ubicados en la red, y, por la otra, la disponibilidad de la infraestructura y tecnología necesaria para acceder a la red (cables, módems, ordenadores y programas informáticos, etc.) (Naciones Unidas, 2011, p. 4). Igualmente, el reconocimiento del Internet como derecho universal garantiza a las personas el acceso a servicios esenciales a través de las redes públicas. Además, permite que los ciudadanos tengan un mínimo estándar de alta calidad a un precio razonable (Lucchi, 2014, p. 846).

II. Perspectivas de acción del Estado en relación con el Internet

La existencia de los riesgos asociados al Internet, a la par de sus innegables beneficios, a que se hizo alusión en el capítulo primero, conduce a preguntarse si su desarrollo, funcionamiento y protección deben quedar sujetos a las reglas libres del mercado, como garante del equilibrio natural entre la demanda y la oferta, o si, de contera, puede ser necesaria una competencia del Estado para garantizar en mejor forma los derechos fundamentales digitales que se desarrollan en este universo.

Bajo otra óptica, si el acceso a Internet comporta un interés general y colectivo, similar al concepto clásico de servicio público o servicios de interés general económico. Así mismo, si la protección de los riesgos asociados a este servicio, simplemente enunciados en el acápite anterior, y el acceso a sus beneficios puede requerir alguna intervención del Estado o si, por el contrario, el exceso de intervención puede llevar a su control hasta extremos que obtengan la consecuencia contraria, es decir, la limitación de los derechos fundamentales de los ciudadanos.

Frente a estos interrogantes, la respuesta no es unánime. Como se verá más adelante, grandes operadores pugnan por la no regulación del Internet desde una perspectiva social que propenda por la igualdad de condiciones en el acceso, uso y apropiación de las TIC, para dar paso a la intervención solo desde el punto de vista de la libre competencia. Sin embargo, no son pocas las voces que han advertido la necesidad de intervención estatal en el Internet para reducir la brecha digital y garantizar el ejercicio de los derechos fundamentales (Herrera y González, 2021).

Esta discusión está relacionada con el principio de neutralidad de la red en Internet que pretende garantizar el libre ejercicio de la libertad de expresión y sus derechos inherentes:

Para algunos, una manera de proteger y promover el disfrute de los derechos humanos en el Internet es a través del fortalecimiento del principio de la neutralidad de la red, principio que, bajo la premisa de un trato no discriminatorio, asegura que las personas puedan escoger libremente el contenido, las aplicaciones y los servicios en el Internet (Belli y De Filippi, 2016, p. 2). El principio de neutralidad de la red evita que los proveedores de los servicios de Internet controlen el acceso y el contenido en el ámbito digital (McDiarmid y Shears, 2016, p. 31).

En esta dirección, el principio de neutralidad de la red asegura las premisas esenciales que sustentan la arquitectura del Internet, esto es, la ausencia de control por un solo jugador público o privado y el no bloqueo o degradación del tráfico de datos (Felten, 2016, p. 64).

Con todo, es importante destacar que la defensa del principio de la neutralidad no es unánime. Así, mientras una parte de la doctrina considera que este principio debe protegerse por todos los medios posibles, lo cual justifica la intervención estatal, una postura contraria opina que la neutralidad de la red debe ser el resultado del mercado.

En este sentido, a través de la competencia, la demanda de los usuarios y el mercado es posible lograr los mismos beneficios que se pretenden alcanzar con la regulación estatal (Pisanty, 2016, p. 130). A este tema nos referiremos más adelante.

Considerar que la sociedad digital debe ser ajena a cualquier intervención, o que existe una libertad absoluta del Internet, sin límites de protección del otro y sin otra regulación distinta de las normas que le sirvan para su funcionamiento, a nuestro juicio, no parece posible de sostener. El mito de la bondad natural de la red de redes, como lo afirma De la Quadra Salcedo en “Los derechos en la sociedad digital: visión subjetiva y visión institucional” (en proceso de publicación, sección 1, párr. 12,), es exactamente eso, y es evidente la necesidad de abandonarlo, pues la generalización del Internet abre nuevos riesgos frente a los ataques que se presentan a los derechos de las personas y al conjunto de las infraestructuras críticas que sostienen la sociedad³.

Otra posible alternativa es la adopción de normas especiales. Un ejemplo interesante es lo que acontece con la Unión Europea en donde actualmente se está estudiando una propuesta de reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales). Esta propuesta tiene entre sus objetivos “fomentar un comportamiento responsable y diligente por parte de los prestadores de servicios intermediarios para garantizar un entorno en línea seguro, que permita a los ciudadanos de la Unión y a otras partes ejercer libremente sus derechos fundamentales, en particular, la libertad de expresión e información”.

Con el propósito de enfrentar riesgos relacionados con la distribución de contenidos y la libertad de expresión, la propuesta consagra medidas dirigidas a crear un “marco de gobernanza moderno y con garantías de futuro, que proteja de manera efectiva los derechos y los intereses legítimos de todas las partes implicadas, y sobre todo de los ciudadanos de la Unión”. En esta dirección, se establecen salvaguardas para asegurar la libertad de expresión, la participación del usuario en el entorno en línea, la tutela judicial efectiva, el derecho a la no discriminación, la protección de los datos personales y la privacidad en línea.

A) Internet como servicio público o servicio de interés general económico

A.1. La calificación de internet como servicio público o servicio de interés general económico

En el ordenamiento jurídico colombiano, sui generis en el derecho comparado, se trató de englobar en el concepto de las TIC los servicios de telecomunicaciones en la medida en que estos emiten, transmiten y reciben información por medios electrónicos⁴. Al respecto,

-
- 3 Como lo sostiene De la Quadra en “los derechos en la sociedad digital: visión subjetiva y visión institucional” (en proceso de publicación, sección 1, párr. 13), “los ataques puntuales o sistemáticos -que pueden afectar el suministro eléctrico o de agua, al control de tráfico aéreo o ferroviario, a hospitales, semáforos, coches inteligentes, las comunicaciones electrónicas, acceso a cuentas bancarias, a interferencias en la democracia, la inteligencia artificial, el big data o el perfilado de las personas etc.- no permiten sostener ya una visión libertaria cuya única respuesta sea la de que Internet o, más ampliamente, la sociedad digital ha de ser un territorio libre de cualquier intervención.”
 - 4 Resolución 202 de marzo de 2010 del Ministerio de las Tecnologías de la Información y las Comunicaciones de Colombia, la cual mantiene su vigencia en virtud de la delegación establecida por la Ley 1341 de 2009, Ley de TIC, para que este ente rector expida el glosario de definiciones aplicables al sector, según su artículo 6º.

la Ley 1341 de 2009, en su artículo 6, define las TIC como el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento y transmisión de información como: voz, datos, texto, video e imágenes. En otras palabras, está referido al conjunto de bienes que permiten la compilación, procesamiento, almacenamiento y transmisión de información por medio electrónico.

A pesar del loable propósito del legislador para integrar en el concepto de TIC, históricamente abierto a la libertad de empresa, a las telecomunicaciones, de un pasado con fuerte regulación e intervención del Estado, lo cierto es que las telecomunicaciones mantienen un régimen jurídico distinto. Al fin y al cabo, el artículo 10 de la Ley consagra los servicios de telecomunicaciones como un servicio público, aunque bajo una contradicción evidente: señala la titularidad del Estado, pero a continuación establece su habilitación de manera general.

En síntesis, las telecomunicaciones son un servicio público en Colombia⁵ con un régimen de habilitación general⁶, para lo cual no se requiere título de concesión o de cualquier otra naturaleza para consolidarse como proveedor de redes y servicios de telecomunicaciones. En forma similar al derecho europeo, los permisos y limitaciones para la entrada al mercado se encuentran más en los recursos escasos, como es el caso del espectro radioeléctrico, el cual está sujeto al acto administrativo de permiso que pueda otorgar el Mintic, previo un proceso de selección pública.

Teniendo en cuenta que el Internet es un servicio de telecomunicaciones en el ordenamiento jurídico colombiano, la conclusión de su naturaleza resulta evidente, esto es, que se trata de un servicio público en los términos de los artículos 365 y siguientes de la Constitución, los cuales reclaman una intervención del Estado para garantizar su finalidad social. No obstante, está sometido, como regla general, a un modelo de gestión de competencia, en el cual el Estado conserva su regulación.

En el marco de la Unión Europea, como desarrollo de las obligaciones de servicio público, ya no del concepto universal y omnicomprensivo del mismo, se regulan los servicios de interés general, que corresponden a aquellas actividades sometidas o no a las reglas de competencia, pero que siempre cumplen misiones de interés general, sociales y de bienestar colectivo, coincidentes así en parte con el servicio público. En estos servicios no interesa tanto quién detenta la titularidad o quién los presta, si el sector público o privado, como si interesa en la noción clásica del servicio público, sino que su nota principal estriba en la congruencia de los servicios con las necesidades de interés general, lo cual implica que se sometan a obligaciones específicas de servicio público.

Al parecer, los servicios de interés económico general no eliminaron los servicios públicos tradicionales, más bien deben ser concebidos como una evolución de estos últimos. La no desaparición del concepto de servicio público ha llevado a entender este como una forma o especie de los servicios de interés económico general. Así lo ilustra Sánchez Morón (2013) en los siguientes términos:

De ahí que, en el marco de la Unión Europea, el proceso de liberalización de los servicios haya sido un proceso controlado y que haya abierto un debate paralelo sobre las exigencias del interés general de los ciudadanos en relación con los

-
- 5 A diferencia de las TIC que no son telecomunicaciones, las cuales no son calificadas como servicio público.
- 6 Como excepción se encuentran los servicios de radiodifusión sonora, los cuales requieren contrato de concesión, previa una licitación.

servicios liberalizados. De este debate deriva la no eliminación –ni siquiera la regresión en términos sustantivos- de la idea de servicio público, pero sí una concepción diferente del mismo y de las relaciones entre el Estado y el mercado, que ha dado lugar a un nuevo concepto, más amplio, de servicios de interés general. (...) Los servicios de interés económico general, así definidos, pueden ser de titularidad pública o privada. Muchos de ellos han sido o siguen siendo considerados de titularidad pública en diversos países, es decir, como servicios públicos en sentido estricto, según nuestra propia terminología. Sin embargo, en este sector es donde se ha producido una sensible privatización en los últimos tiempos, a veces impulsada por el Derecho derivado europeo y en otros casos por normas nacionales. En consecuencia, pueden tratarse de servicios públicos o no, aunque si lo son, difícilmente podrán configurarse como monopolios públicos, ya que están sometidos en general al régimen de la competencia” (p. 775).

Ahora bien, dentro de las características principales de los servicios de interés general, dentro de los que se cuentan los servicios públicos, la doctrina española (Sánchez Morón, p. 172 y ss.) ha identificado:

- (i) La mutabilidad, que indica que cuando las condiciones de prestación del servicio no permitan lograr la satisfacción del interés general, el Estado puede modificar las condiciones de prestación del servicio, cuando así sea necesario para lograr la satisfacción del interés general.
- (ii) La igualdad, que contribuye a reducir la desigualdad real en el acceso a los servicios públicos, en particular en tratándose de aquellos servicios que no tienen cobertura en todo el territorio ni su acceso cubre a todos los ciudadanos. Estos servicios deben proveerse de forma igualitaria y sin discriminar a los usuarios. Sin embargo, es permitido el establecimiento de condiciones particulares para permitir a determinados usuarios el acceso, medidas que de todas maneras deben ser razonables y proporcionadas.
- (iii) La calidad propende porque los operadores se preocupen por el perfeccionamiento de sus operaciones, pues ello finalmente redundará en una mayor satisfacción para el usuario. En consecuencia, la Administración goza de facultades de regulación, planificación, ejecución, evaluación y control de la actividad del prestador, con el propósito de garantizar un estándar mínimo de servicio o su mejoramiento. Dentro de los mecanismos que pueden implementarse se ubican las denominadas cartas de servicio, las evaluaciones de calidad y la imposición de requisitos y niveles mínimos servicio.
- (iv) La asequibilidad determina que los servicios de interés económico general deben ser accesibles a cualquier persona, pues a través de ellos se promueve la cohesión económica y social. En consecuencia, los servicios deben prestarse a la luz de condiciones económicas asequibles, sin que en todo caso esto signifique su gratuidad. Para lograr un servicio accesible para las personas, la Administración puede establecer un sistema de tarifas o precios máximos, que sin embargo deben tener en cuenta el coste de la prestación del servicio. Igualmente, puede imponer la provisión de prestaciones gratuitas, tales como las llamadas de emergencia.

En Colombia, como regla general, la prestación de servicios públicos no implica el principio de libertad de ingreso, pues, dado el interés de la colectividad, están sometidos

a permisos, autorizaciones o concesiones, según la naturaleza de la actividad⁷. El caso de las telecomunicaciones es diferente pues, como se ha dicho, existe una habilitación general de ley.

Independientemente del principio de libertad de entrada o de autorización previa, lo cierto es que en el desarrollo de una actividad de servicio público está inmerso el interés general, lo cual presupone, además de un régimen jurídico particular o especial, una intervención estatal⁸.

De esta dimensión social del servicio público se desprende la garantía de la universalidad del servicio público, que encuentra justificación en el hecho de que los servicios públicos incluyen prestaciones que son fundamentales para el desarrollo de la vida humana en condiciones dignas, de tal suerte que debe garantizarse su realización. Es conocido el concepto de acceso o servicio universal aplicable en la legislación colombiana para el sector de TIC: Se busca garantizar a todos los ciudadanos el acceso razonable a la prestación, sin tomar en consideración su localización geográfica y la rentabilidad para el operador.

De las consideraciones expuestas se colige que calificar una actividad como servicio público tiene sendas repercusiones en el sentido de constituir derechos en cabeza de los ciudadanos y correlativamente crear obligaciones a cargo del Estado y de los prestadores, sean públicos o privados. En este caso, el Estado conserva la facultad de regulación, vigilancia y control del servicio.

A.2. El derecho de acceso a internet, como el derecho de acceso a la sociedad digital y a los derechos digitales. Un servicio público esencial

Ante el imponente reto de promover la prestación del servicio de internet, la actividad de prestación del servicio de internet y, en particular, para garantizar su acceso, algunos países han adoptado como política su intervención en la actividad.

En el 2013, México realizó una importante reforma constitucional y, al año siguiente, emitió una legislación para el sector de las telecomunicaciones y radiodifusión que comprende la Ley Federal de Competencia Económica (LFCE) y la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR), en la que se establece que las telecomunicaciones son servicios públicos de interés general, lo cual crea obligaciones a cargo del Estado.

Dentro del conjunto de medidas adoptadas, se destaca la constitucionalización del derecho de acceso al Internet. Así, el artículo 6 de la Constitución Mexicana, referido a la libertad de expresión, impuso al Estado la obligación de garantizar el derecho de acceso a las tecnologías de la información y las comunicaciones, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet.

7 Los servicios públicos de transporte y de banca. Existen también servicios públicos domiciliarios como los servicios eléctricos, de agua y alcantarillado y de aseo, regulados en la Ley 142 de 1994, que también consagran una habilitación general para su prestación.

8 El concepto de interés general dependerá de la realidad social, política y jurídica de cada Estado. Esta concepción del servicio público está plasmada en el ordenamiento jurídico colombiano, en el artículo 430 del Código Sustantivo del Trabajo, que indica “(...) se considera como servicio público, toda actividad organizada que tienda a satisfacer necesidades de interés general en forma regular y continua, de acuerdo con un régimen jurídico especial, bien que se realice por el Estado, directa o indirectamente, o por personas privadas”.

Esta medida, junto con las relativas al fomento de la competencia, la política de inclusión digital a cargo del ejecutivo, la creación del Instituto Federal de Comunicaciones, como órgano autónomo constitucional, ha tenido efectos muy positivos, entre los que se cuentan: niveles de penetración más elevados en el servicio de banda ancha, mejoras en la calidad del servicio, en especial, en materia de velocidad de banda ancha y volúmenes de transferencia de datos, y más de 50 millones nuevas suscripciones a servicios de internet móvil, entre otras (OCDE, 2017).

Argentina, por su parte, en el año 2014 declaró de interés público el desarrollo de las Tecnologías de la Información y las Comunicaciones, estableció el servicio universal con la finalidad de posibilitar el acceso de todos los habitantes del país, sin distinción, a los servicios TIC en condiciones de calidad y a un precio justo y razonable y le otorgó al acceso a las redes de telecomunicaciones el carácter de servicio público esencial y estratégico de las TIC.

Así mismo, reconoció el derecho humano a las comunicaciones y a las telecomunicaciones, para lo cual le encargó al Estado un rol planificador que incentivara la función social de las TIC. No obstante, al año siguiente, el Decreto de Necesidad y Urgencia (DNU) n.º 267 derogó gran parte de las disposiciones referidas en materia de servicios de comunicaciones y de TIC, y abandonó la idea del acceso a estos últimos como un derecho humano para darle prioridad a una visión más económica de oferta y demanda.

Sin embargo, en el año 2020, a través del Decreto de Necesidad y Urgencia (DNU) n.º 690, se pretendió revivir algunas disposiciones y se declaró a las TIC como servicios públicos esenciales y estratégicos en competencia, con lo cual se le otorgó el carácter de esenciales a los servicios de internet, telefonía celular y TV paga. Como consecuencia de esa declaratoria, se estableció, entre otras medidas, que los precios de estos servicios serían regulados por el Ente Nacional de Comunicaciones, que debe, además, establecer la prestación básica universal obligatoria que deberá ser brindada en condiciones de igualdad. Una de los efectos de mayor impacto de esta normativa fue que el aumento de precios o modificación de los mismos por parte de los licenciatarios TIC quedó suspendido en el marco de la emergencia por la Covid-19.

Dentro de las razones que se plasmaron en la motivación de este decreto, subyace i) el reconocimiento del derecho humano de acceso al Internet y a las TIC, por ser el portal de acceso a otros derechos (educación, libre expresión, información, desarrollo económico y social, etc.), y ii) la relevancia de la fijación de reglas especiales por parte del Estado para garantizar el acceso equitativo, justo y a precios razonables. Es necesario acotar que en la actualidad esta reglamentación se encuentra suspendida como respuesta a la medida cautelar que solicitó Telecom por considerar que no están dados los presupuestos legales que permitan calificar como servicio público a una actividad privada libre que se realiza en condiciones de competencia.

En esta misma línea, Brasil, por medio del Decreto 10.282 de 2020, les otorgó a las telecomunicaciones y al Internet el carácter de servicios públicos esenciales, por cuanto su no disponibilidad pondría en peligro la supervivencia, la salud o la seguridad de la población. Esta calificación repercutió positivamente en el sector y permitió la adopción de algunas medidas como la prohibición a los gobiernos locales de imponer restricciones en la movilidad de los trabajadores.

Como consecuencia de la pandemia, en Chile se puso de relieve la brecha en materia digital: 55 comunas del país cuentan niveles de conectividad inferiores al 1% y 60.000 personas se encuentran en las zonas del silencio. Cambiar estas cifras y cerrar la

brecha digital fue una de las motivaciones principales que impulsó el proyecto de ley que confiere al Internet la calidad de servicio público de telecomunicaciones y que ya fue aprobado en primer trámite constitucional por el Senado. Dentro del catálogo de disposiciones, la norma faculta al presidente para que, dentro del trámite del proyecto de ley de Presupuestos, y a través de la presentación de la respectiva glosa presupuestaria, disponga, con cargo a los recursos del Fondo de Desarrollo de las Telecomunicaciones, un subsidio para el pago de las cuentas de servicios de internet para la población más vulnerable.

En marzo de 2021, el Congreso de Perú aprobó en primera votación el proyecto de reforma a la Constitución Política que eleva a rango constitucional el derecho de acceso a internet. El proyecto consagra este derecho en el artículo 14, referido al derecho a la educación, en los siguientes términos: "El Estado garantiza el derecho de acceso a internet. En las entidades, instituciones y espacios públicos su acceso es gratuito. Asimismo, promueve el desarrollo científico y tecnológico del país a través de la formación en las tecnologías de la información y comunicación, en especial para el sector educativo y en las zonas rurales del país".

El argumento principal de la reforma, cuya elaboración se basa en cuatro iniciativas legislativas en la materia, es que el acceso al internet es un medio idóneo o habilitador para el ejercicio de otros derechos fundamentales, tal como lo reconoció el Tribunal Constitucional Peruano, mediante sentencia con Exp. N.º 02-2001-AI/TC, en relación con el derecho a la información. También se señaló que esta medida favorecería el cumplimiento de los objetivos trazados en distintas políticas públicas como la Agenda Digital Peruana 2.0, la Estrategia Nacional de Tecnologías en Educación y el Plan Nacional de Alfabetización Digital.

A la par de los desarrollos legislativos mencionados, han existido otros importantes avances en esta materia por vía jurisprudencial.

Así, en Costa Rica, el derecho al Internet, ya sea como un servicio público esencial o como un derecho fundamental, fue objeto de pronunciamiento por parte del Tribunal Constitucional. Al respecto, la autoridad judicial señaló que este derecho conlleva: i) su protección a través del recurso de amparo, ii) la obligación del Estado de promover su democratización, procurando de esta manera disminuir la brecha digital, y iii) el deber estatal de garantizar un acceso mínimo a la red. Asimismo, en opinión del magistrado Cruz Castro, al ser el acceso al Internet un derecho fundamental, los proveedores del servicio no pueden ser los llamados a definir la periodicidad y la velocidad mínima funcional para determinar el uso justo del servicio (Sala Constitucional de la Corte Suprema de Justicia de Costa Rica, 2017).

El Tribunal Constitucional de Costa Rica tuvo en cuenta en su pronunciamiento la sentencia del Consejo Constitucional Francés de 10 de junio de 2009 (sentencia No. 2009-580 DC), en la cual se calificó el acceso a Internet como un derecho básico, con fundamento en el artículo 11 de la Declaración de los Derechos del Hombre y del Ciudadano de 1789 que tutela la libre comunicación de pensamientos y opiniones.

El reconocimiento del Internet como un derecho fundamental ha permitido a la Sala Constitucional costarricense decidir recursos de amparo a favor a personas que viven en zonas apartadas y enfrentan problemas de accesibilidad (Miranda Bonilla, 2016, p. 13).

Recientemente, fue promulgada en Colombia la Ley 2108 de 2021, por medio de la cual se modifica la Ley 1341 de 2009 y se declara el acceso a internet como uno de los servicios públicos de telecomunicaciones con carácter esencial. Así, esta norma tiene como objeto:

[E]stablecer dentro de los servicios públicos de telecomunicaciones, el acceso a Internet como uno de carácter esencial, con el fin de propender por la universalidad para garantizar y asegurar la prestación del servicio de manera eficiente, continua y permanente, permitiendo la conectividad de todos los habitantes del territorio nacional, en especial de la población que, en razón a su condición social o étnica se encuentre en situación de vulnerabilidad o en zonas rurales y apartadas (artículo 1).

En relación con los estados de excepción y las emergencias sanitarias que sean declaradas por el Ministerio de Salud y Protección Social, la ley enuncia una serie de reglas de obligatorio cumplimiento para los proveedores de redes y servicios de telecomunicaciones (PRST), en los eventos en los cuales el usuario incurre en impago del servicio. En estos casos, la norma obliga a los PRST a prestar algunos servicios de manera gratuita⁹.

En lo referido al acceso de internet gratuito, existe una estrecha relación con el ejercicio de derechos fundamentales (salud, educación), de los cuales no pueden ser privados los usuarios por razones puramente económicas. Se busca que prevalezca el carácter esencial del servicio sobre el concepto económico. Esta perspectiva social sobre la dimensión económica de la actividad da cuenta de la importancia de la intervención estatal en la materia, pues de otra forma, bajo las reglas del mercado, la gratuitad en ciertas prestaciones estaría reservada, por ejemplo, para los eventos en los cuales esta reporte beneficios para el operador por resultar atractiva para potenciales clientes.

En síntesis, el derecho de acceso a Internet debe constituirse en un derecho digital de todo ciudadano, en ocasiones calificado como servicio público esencial, dada su relevancia para garantizar los derechos fundamentales y su desarrollo en la sociedad digital. Lo anterior, porque su ejercicio y protección en el entorno digital tienen el mismo elemento común de los derechos fundamentales consagrados en las normas constitucionales: propender por la dignidad humana.

Otra de las conclusiones corresponde a entender que el Internet, como puerta de entrada a la sociedad digital y al ejercicio de los derechos adecuados a este entorno, no puede dejarse a las libres reglas de la oferta y la demanda bajo el pretexto de una libertad absoluta y sin límites de quienes detentan los poderes para su ejercicio y funcionamiento o aún para los ciudadanos que intervienen en este universo. Su extralimitación claramente conduce al recorte y desconocimiento de derechos fundamentales de los ciudadanos que no pueden ser sometidos a las reglas propias de quienes tengan mayor capacidad adquisitiva para establecer que solo ellos pueden tener acceso al internet.

Así mismo, la intervención estatal resulta necesaria para proteger derechos fundamentales cuando los ciudadanos entregan sus derechos y sus datos y, en últimas, su libertad, a quienes detentan una posición dominante en el control de las plataformas y de la información que cursa sobre las mismas. Como es conocido, esta información requerida por los ciudadanos para satisfacer sus necesidades de bienes y servicios en las plataformas

9 Para los planes de telefonía móvil (voz y datos) en la modalidad pospago cuyo valor no exceda 1,5 Unidades de Valor Tributario (UVT), se debe mantener la opción de efectuar recargas para usar el servicio en la modalidad prepago, envío de doscientos mensajes de texto gratis y la recepción de estos sin ninguna restricción, la navegación gratuita en treinta direcciones de Internet (URL), que serán definidas por el Ministerio de las Tecnologías de la Información y las Comunicaciones y la Comisión de Regulación de Comunicaciones, para acceder a servicios de salud, atención de emergencias, del gobierno y de educación. Para los servicios de telefonía móvil (voz y datos) en la modalidad prepago, se estableció la misma obligación en materia de mensajería de texto (SMS).

no tiene una respuesta adecuada por parte de los dueños de estas aplicaciones. En efecto, la primera información que se le entrega al usuario en el medio virtual no es la que mejor satisface sus necesidades, sino la que más conviene a los intereses económicos de estas grandes multinacionales. Generalmente, los proveedores de estos bienes y servicios le pagan al dueño de la plataforma para que los ubique en los primeros lugares, en detrimento de los derechos de los usuarios y normalmente sin su conocimiento.

Restaría analizar si la configuración tradicional de los derechos fundamentales en las normas de rango constitucional de nuestros países pueden ser suficientes para la garantía de los derechos de los ciudadanos en el ecosistema digital, y de este supuesto, indagar si se traducen en nuevos derechos que pueden denominarse digitales o si, siendo las mismas manifestaciones y desarrollos de los derechos tradicionales, no obstante, pueden requerir un nuevo ordenamiento que permita su mayor protección en situaciones fácticas desconocidas en una sociedad presencial.

Las consideraciones expuestas permiten afirmar que los derechos en la sociedad digital, relacionados con derechos fundamentales, aunque con distintas configuraciones, como se verá más adelante, se soportan, al parecer, sobre un derecho fundamental vinculado al concepto de servicio público que corresponde al derecho de acceso a internet. No podría ser de otra manera, pues la puerta de entrada a la sociedad digital es exactamente el acceso a internet y al ejercicio de los derechos que tienen todos los ciudadanos para preservar su dignidad humana.

Ello implica una labor del Estado para garantizar esta finalidad social y de los particulares que intervienen en el ecosistema digital para preservar estos derechos en sus dos vertientes, esto es, en su visión personal e individualizada y en su visión institucional. Al fin y al cabo, corresponden y dan sustento al concepto de democracia y al Estado Social de Derecho en el mundo digital.

III. Los derechos en la sociedad digital o derechos digitales: los instrumentos para su protección en las fuentes del derecho

A. Los derechos fundamentales y su protección

En el marco de los derechos constitucionales se consagran los derechos fundamentales. Este concepto generalmente se reserva a aquellos derechos inherentes a toda persona en razón a su dignidad humana y, por ello, gozan de las máximas garantías normativas, institucionales y jurisdiccionales, como son los derechos a la vida, la libertad e igualdad ante ley, la libertad de conciencia, de cultos, de expresión e información, la honra, el derecho de circulación y residencia, el derecho al trabajo (arts. 11 a 25 C.P), entre otros. Son derechos de carácter universal y están reconocidos en tratados, convenios e instrumentos internacionales (como la declaración de los derechos del hombre y del ciudadano) y que vinculan a los Estados.

Las normas constitucionales y supraconstitucionales son el marco necesario y adecuado para determinar cuáles derechos pueden tener este rango de fundamentales, aunque puedan existir diferencias doctrinales propias del iusnaturalismo, que parecen predicar su origen en concepciones religiosas, humanísticas o idealistas y que, por ello, no requerirían de su consagración escrita para reclamar su existencia. Parece más ajustado señalar que serán derechos fundamentales aquellos que se establezcan en la norma suprema o las normas que tengan este rango.

Por tanto, un derecho fundamental es un derecho subjetivo esencial de las personas

que se consagra en la Constitución Política colombiana, así como los procesos para su protección, entre ellos, el reconocido recurso de amparo de tutela. La acción de tutela es la garantía que establece en Colombia la Constitución de 1991 para todas las personas con el fin de lograr la protección judicial inmediata de sus derechos fundamentales¹⁰.

Estos derechos son de aplicación directa, puesto que no están supeditados a un desarrollo legal para su vigencia y amparo a todas las personas. En todo caso, aunque en el estado constitucional la Ley no es la norma primaria del Derecho, pues en este lo es la Constitución, de todas maneras, continúa siendo por razones de legitimidad democrática, la norma que dentro del ordenamiento jurídico desarrolla en forma expansiva los derechos fundamentales y su ejercicio.

Precisamente, en Colombia las leyes estatutarias (art. 152 C.P.) regulan los elementos estructurales esenciales de los derechos fundamentales y de los mecanismos para su protección y pleno ejercicio. Es decir, el Constituyente de 1991 consideró que la ley puede ser el vehículo para garantizar el disfrute general de los derechos constitucionales, en condiciones de igualdad para todos, el instrumento para regular las facultades de exigirlos y obtenerlos jurídicamente y la norma que establezca obligaciones públicas que promuevan su cumplimiento real y efectivo.

Ahora bien, la importancia de que se reconozca un derecho como de carácter fundamental y se eleve a rango constitucional radica en que se le otorga la máxima protección jurídica en el Estado Democrático de Derecho, pues se le dota de la fuerza normativa propia de la Constitución y su supremacía, de manera que, por una parte, se impone a todos los poderes públicos, quienes quedan vinculados a su respeto y protección (límite al ejercicio del poder público) y, por otra, se convierte en un conjunto de valores o fines de las relaciones de los ciudadanos con el Estado, sino también frente a los otros miembros de la comunidad.

Así, cuando el Estado y la comunidad deciden elevar al rango de derechos fundamentales determinadas facultades, libertades, prerrogativas o prestaciones, su eficacia se torna en un compromiso ineludible de respeto y garantía por todos; y, en ese proceso, frente a cada faceta de un derecho se debe, entonces, determinar cuáles garantías son más efectivas para su plena realización, en el marco de las competencias de los distintos órganos del Estado y ramas del poder público (Corte Constitucional, Sentencia T-428 de 8 de junio de 2012).

Por supuesto, consagrando derechos en la Constitución Política obedece a un consenso social sobre la necesidad de establecer esa garantía básica que han de tener los ciudadanos en un momento y contexto histórico y social determinado. Depende de factores políticos, culturales y jurídicos que se presenten en la sociedad en una época específica y que animan a los poderes públicos y los asociados a activar un proceso que conduzca a modificar el pacto social y a establecer en la parte dogmática de la Constitución nuevos derechos.

La experiencia internacional de establecer un nuevo régimen de protección, garantía y respeto de los derechos fundamentales, como consecuencia de los nuevos entornos tecnológicos y digitales de la actualidad, evidencia la creciente problemática que genera

10 El artículo 86 de la Constitución colombiana indica que: Toda persona tendrá acción de tutela para reclamar ante los jueces, en todo momento y lugar, mediante un procedimiento preferente y sumario, por sí misma o por quien actúe a su nombre, la protección inmediata de sus derechos constitucionales fundamentales, cuando quiera que estos resulten vulnerados o amenazados por la acción o la omisión de cualquier autoridad pública.

su utilización en el marco de la sociedad de la información y las tecnologías.

B. Los derechos fundamentales y los derechos digitales en la sociedad virtual

La transición digital en un mundo global ha demandado esfuerzos para que en esta era se salvaguarden los derechos fundamentales y las garantías conquistadas en su protección. Por ejemplo, en el Plan de Acción de la Unión Europea sobre Derechos Humanos y Democracia para 2020-2024, se ha planteado la necesidad de abordar el impacto de la tecnología en los derechos humanos y de la propia definición del uso de estas tecnologías como derechos de las personas o comunidades, bajo la denominación de derechos digitales, los que comúnmente la doctrina ha llamado derechos de cuarta generación o cuarta ola de derechos humanos (López Zamora, 2020, p. 199).

La irrupción vertiginosa de la realidad de la sociedad virtual y el ejercicio de los derechos y cumplimiento de los deberes por parte de quienes intervienen en sus relaciones sociales, culturales, políticas, religiosas y económicas, parecen, como es obvio, no estar acompañadas del necesario estudio y posterior regulación que permitan su preservación. Esta premisa resulta aplicable, no solo para quienes prestan los servicios de internet, los operadores de las plataformas y aplicaciones, sino también para los gobiernos y para los usuarios que interactúan en este universo de redes sociales.

Los desarrollos tecnológicos, por su misma naturaleza y sus avances vertiginosos, irrumpen en la sociedad como una situación de hecho frente a los naturales beneficios que otorgan a la sociedad en general y a los ciudadanos para su comunicación.

Es el diario vivir que la mayoría de las personas apunten sus miradas y gran parte de su tiempo al ordenador o al teléfono móvil, de tal manera que sus relaciones se desarrollan, en su mayoría, de forma virtual, y sin mayor tiempo y precisión para determinar cómo puede ser y debe ser la protección de los derechos fundamentales. Aún más, si ellos pueden ser conculcados con el simple quehacer diario y con la explotación económica de quienes intervienen en el ecosistema digital.

Hacemos referencia a quienes detentan derechos sobre los contenidos, a los servicios online, a las tecnologías habilitadoras, a los operadores de telecomunicaciones que suministran la conectividad y a los que suministran los dispositivos físicos que permiten el interfaz del usuario y aplicaciones, como lo enseña la cadena de valor planteada por A.T. Kearny (2010).

En este escenario, su análisis y la eventual regulación solo surge después, cuando se puede comprender el alcance y los efectos jurídicos que tienen estas nuevas interacciones de la sociedad virtual. Así ha sido y seguirá siendo, como lo enseña la historia de la regulación en el sector de telecomunicaciones y de las tecnologías de la información y las comunicaciones.

A esto apuntan estas consideraciones que muestran, a nuestro juicio, la necesidad de preservar los derechos digitales, independiente de su discusión de si se trata de nuevos derechos o si son simplemente los derechos tradicionales desarrollados bajo una nueva configuración acorde a este universo virtual.

Para ello, puede ser necesario precisar de qué estamos hablando y cuál ha sido el panorama en derecho comparado de algunos países que han iniciado su estudio y determinado la necesidad de preservarlos, especialmente cuando pueden desconocer los derechos fundamentales inherentes a la dignidad humana.

La dimensión en la nueva configuración de los derechos fundamentales en la sociedad digital todavía resulta impredecible en su alcance y puede llegar a extremos de deshumanizar la sociedad y marcar una defensa de una ideología tecnológica que propugne por una nanotecnología pura y amoral y por un desarrollo de una sociedad conformada por una raza superior sin mayores rasgos de enfermedades genéticas a la cual solo tendrían acceso unos privilegiados, esto es, la pequeña población que cuente con una inmensa capacidad económica y dispositiva¹¹.

Como se observa, no resulta fácil precisar todas las problemáticas surgidas de la nueva sociedad digital y de los riesgos de considerar que la técnica- más allá de los beneficios que tiene para el desarrollo de la sociedad- pueda ser pregonada como una nueva ideología, con los peligros que conlleva para la mayoría de la población, imposibilitada de acceder a estos nuevos desarrollos¹².

Ello no quiere decir que debe proclamarse la inacción. Por el contrario, el desarrollo actual de la sociedad digital muestra la necesidad de contar con instrumentos jurídicos efectivos que permitan la defensa de los derechos de los ciudadanos, en especial, de los derechos que le son inherentes a su dignidad humana.

C. Los derechos digitales y su protección

En cuanto si estos derechos digitales son derechos nuevos o corresponden a los tradicionales con nuevos contornos, parte de la doctrina (López Zamora, 2020, p.199), señala que carecen de la cualidad de "novedosos", y, por ende, no habría posibilidad de plantear la existencia de una nueva generación.

En general, los derechos digitales defienden los mismos intereses, libertades y fundamentos de las tres generaciones de derechos que presenta la evolución política y el tránsito constitucional de los modelos de Estado: los derechos y libertades individuales, los derechos económicos, sociales y culturales y los derechos de la solidaridad o colectivos a la paz, medio ambiente, no discriminación de minorías, pese a que se ejerzen en un entorno distinto para evitar los atropellos jurídicos propiciados en el Internet y las redes en los que se generan riesgos de vulneración de esos derechos ya consagrados y preexistentes.

Discursos de odio en las redes sociales y en Internet por comunidades digitales, violaciones al derecho a la privacidad; vulneraciones a la honra, imagen y reputación de las personas; desinformación con intereses oscuros y manipulaciones de las masas; el uso de sistemas de reconocimiento de la identificación no autorizada de las personas (facial o dactilar) y las potenciales vulneraciones del derecho de asociación o la libertad de expresión, entre muchos otros, revelan que las tecnologías, las redes sociales y el Internet se prestan para vulneraciones de los derechos humanos ya reconocidos universalmente.

Estas evidentes transgresiones a los derechos mínimos de las personas, no limitados a la

11 En efecto, los grandes avances en la investigación humana y en la salud que permitan mejorar los genes desde antes del nacimiento para detectar enfermedades y eliminarlas a futuro solo estarían al alcance de unos pocos que cuenten con la inmensa capacidad económica de asegurar una especie de raza superior y selectiva. Esta teoría que pregonó por aceptar todo lo que genere la tecnología conlleva un cuestionamiento ético respecto de los derechos de la mayoría de la población, en especial, de quienes no cuentan con mayores recursos o se encuentran en situación de vulnerabilidad.

12 Sobre el particular, puede consultarse: Habermas, Jürgen (1968) y De la Quadra Salcedo (2018).

intimidad o a los datos personales y conculcados por los actores que intervienen en las redes sociales, por los mismos operadores de los servicios y aplicaciones de la sociedad de la información y por los mismos gobiernos, muestran la preocupación y la necesidad de que el instrumento normativo o las fuentes del derecho enfrenten esta problemática.

Ello se ha traducido en lo que se denomina una “constitución digital” o una “declaración de derechos digitales” que parecen mostrar la necesidad de nuevas declaraciones de derechos, frente a una posible insuficiencia de los tradicionales y en el texto de su consagración constitucional.

Son muchas las iniciativas surgidas de la sociedad civil y de la declaración de derechos en Internet en algunos países¹³. Haremos referencia a algunos sistemas y metodologías utilizadas que permiten inferir como son los propios usuarios de la sociedad digital los que reclaman regulaciones que les den protección y seguridad a sus derechos, con la claridad de que esa normativa debe estar limitada a la finalidad buscada, pues su desborde puede llevar exactamente al fin contrario: un abuso de poder de los gobiernos para restringir los derechos y garantías políticas.

Dentro de este marco, resulta necesario analizar lo que se viene calificando como derechos digitales y cuál es su contenido y novedad en relación con los derechos fundamentales reconocidos en nuestras cartas políticas. El mismo derecho de acceso a Internet puede dar lugar a cuestionamientos en su clasificación respecto a si es un derecho humano fundamental con autonomía o una proyección de los existentes, en este marco de la regulación de los derechos digitales¹⁴.

A partir de este supuesto, es menester determinar si se justifica una nueva regulación que los preserve, o si el desarrollo de las fuentes del derecho, en especial de la jurisprudencia de nuestras cortes, puede resultar suficiente para su protección.

Finalmente, deberá establecerse si su alcance en su concepción personalista y subjetiva en la sociedad digital y su preservación colman las aspiraciones y finalidades de estos derechos, y más allá de los fundamentos de la democracia y del Estado Social de Derecho. Hacemos alusión a que muchas de las transgresiones que se presentan en este mundo virtual afectan gravemente los derechos en una visión institucional como es el caso de las garantías políticas, los famosos “fake news”. En otras palabras, como lo sostiene De la Quadra en “los derechos en la sociedad digital: visión subjetiva y visión institucional” (en proceso de publicación, sección 5) si debe mirarse esta protección de los derechos en la visión personalista y también en la visión colectiva, social e institucional.

13 Así se puede ver: la Declaración de Derechos en Internet de la Cámara de Diputados Italiana del 26 de junio de 2015; la Ley brasileña 12.965 de 23 de abril de 2014, sobre el establecimiento de principios, garantías, derechos y deberes para el uso de internet; la Ley Orgánica española 3/2018 Protección de Datos Personales y garantía de los derechos digitales; la Ley francesa número 2016-1321 del 7 de octubre de 2016 para la República digital, o la Constitución Mexicana en sus reformas de los años 2013 y 2016.

14 La doctrina también se ha propuesto el reto de identificar si los derechos “digitales” son nuevos derechos con carácter particular y propio. Así, por ejemplo, Pollicino (2020) se preguntó si el acceso a internet es un derecho humano o fundamental que goza de autonomía semántica, conceptual y constitucional o si se trata solamente de una condición para el disfrute de otros derechos, es decir, una proyección de estos, en clave de la experiencia italiana. Al respecto, concluyó que, en el derecho internacional, Internet parece ser considerado un medio más a través del cual se ejerce y protege la libertad de expresión o la participación democrática en la sociedad de la información.

Sobre el primer tema, algunos autores, como López Zamora (2020, p. 203), describen varios de los derechos digitales que deben ser considerados¹⁵, y que, en general, tienen coincidencia con los desarrollos doctrinales y legislativos en algunos países.

Además, resulta conveniente referirse a la Ley Orgánica española 3 de 2018, la cual incorpora un título denominado “Garantía de los Derechos Digitales”, en el que se establece un reglamento de protección de datos. No puede desconocerse que gran parte del desarrollo de los derechos digitales deviene de la reciente preocupación por la protección de los datos y que son un problema central en el mundo digital. Sin embargo, pueden existir derechos propios no enraizados solo en los datos.

También debe hacerse referencia a la Declaración italiana de derechos en Internet, de carácter no vinculante, que resulta en gran parte coincidente con los derechos en la era digital a que se refiere la Ley española.

Una simple enunciación de la mayoría de estos derechos evidencia, por una parte, un reconocimiento de derechos nuevos propios de la sociedad digital, como el derecho a la neutralidad del Internet, el derecho de acceso universal a Internet, y, de otra parte, un desarrollo de los derechos tradicionales enmarcados en este servicio. Entre ellos, los derechos a la educación digital, a la seguridad digital, a la desconexión digital y al olvido, este último aplicable, no solo en la búsqueda de Internet, sino también en las redes sociales y servicios equivalentes¹⁶.

Si se observa su contenido, se encuentran coincidencias con la preservación de los derechos tradicionales adecuados a un entorno digital: los derechos a la libertad, el honor, la intimidad, la opinión, la información veraz y el debido proceso. Algunos derechos surgen como inherentes a la concepción de la persona y a su dignidad humana

15 Bajo esta filosofía, y aun cuando sistematizar los derechos que afectan al individuo inmerso en la realidad digital no es una tarea fácil, existen varios derechos digitales a considerar:

- Derecho de libertad: derechos y libertades en el entorno digital, a la protección de datos, a la identidad en el entorno digital, al pseudonimato, a no ser localizado y perfilado, a la seguridad digital, a la herencia digital.
- Derechos al honor, intimidad e imagen en la red: derechos de rectificación, actualización de la información y derecho al olvido en redes sociales y buscadores.
- Derechos de igualdad: Derecho a la no discriminación e igualdad, a la protección de los menores y mayores, así como de las personas con discapacidad.
- Derechos de acceso universal, neutral y seguro a Internet y derecho a la educación digital.
- Derechos de participación: Derecho a la neutralidad en internet, a la libertad de expresión e información, a la participación ciudadana y educación digital, así como los derechos digitales en las relaciones con las administraciones públicas.
- Derechos en el entorno laboral y empresarial. Derechos de los trabajadores y límites en los controles basados en las tecnologías de la información.
- Derechos a la portabilidad en redes sociales y servicios similares.
- Derechos en diversas áreas: Derecho de acceso a los datos para la investigación científica, al desarrollo tecnológico y sostenible, a la protección de la salud, a la libertad de creación y acceso a la cultura, respecto disposiciones por causa de muerte como el derecho al testamento digital, frente a la inteligencia artificial y la neurotecnología.

16 Los derechos incorporados en la Ley Orgánica 3 de 2018 de España, que resultan muy similares a la declaración italiana son: derecho a la neutralidad de la red, derecho de acceso universal a internet, derecho a la seguridad digital, derecho a la educación digital, derecho al olvido en búsquedas de internet, derecho al olvido en servicios de redes sociales y servicios equivalentes, derecho de portabilidad en servicios de redes sociales y servicios equivalentes.

y otros parecen consagrarse como los efectos que sobre cada persona y sus derechos tienen los programas, mecanismos, dispositivos y sistemas de la sociedad digital, tal como lo sostiene De la Quadra en "los derechos en la sociedad digital: visión subjetiva y visión institucional" (en proceso de publicación, sección 2.1.2, párr. 3-11).

Otras metodologías no enlistan los derechos, sino establecen reglas dirigidas a garantizar en estos ámbitos virtuales los derechos vigentes, pero con una nueva denominación o ampliación en su regulación. Es el caso de Francia (Ley n.º 2016-1321 del 7 de octubre de 2016) y de Brasil (Ley 12.965 de 23 de abril de 2014).

Es novedoso y ciertamente indicativo que en el ordenamiento jurídico francés se intitule la norma bajo la denominación de "República digital", aunque su desarrollo alude a la efectividad de los derechos de los ciudadanos y usuarios respecto de las nuevas tecnologías en los diferentes ámbitos del derecho. Desde ese punto de vista, se introducen modificaciones a las normas de códigos tan variados como las relaciones entre el público y la Administración, el medio ambiente, la contratación pública, la justicia administrativa, la energía y los derechos de los ciudadanos en su relación con la Administración, entre otros.

También se destaca un tema no suficientemente desarrollado y donde se percata que esta protección de los derechos digitales no puede limitarse a la regulación de Internet, sino en general a los medios tecnológicos para que estas reglas puedan ser aplicables en cualquier ámbito de la sociedad digital. Un ejemplo de ello, puede observarse a propósito de los desarrollos de la IA y del Big Data, donde también resulta importante preservar los derechos digitales.

Seguramente un análisis detallado de los derechos enlistados en estas legislaciones de derecho comparado o de las mismas reglas que aseguran los derechos de los ciudadanos en la sociedad digital, pueda permitir arribar a la conclusión de que se trata de los mismos derechos tradicionales, o, por lo menos, que tienen una relación directa o indirecta con los mismos.

Consideramos que esa no es la premisa que merece destacarse, esto es, si se trata realmente de nuevos derechos o si son los mismos tradicionales bajo una nueva reconfiguración.

De las enumeraciones de derechos y posiciones y facultades de los usuarios sobre sus derechos en la sociedad digital se encuentran coincidencias con derechos tradicionales, tales como, el derecho al trabajo y el derecho a la desconexión digital en el trabajo; el derecho a la desconexión digital y a la seguridad digital vinculadas con los derechos a la intimidad y a la información. Varios encuentran su sustento en la libertad de expresión, la intimidad, la protección de datos, el secreto de las comunicaciones y el derecho de igualdad.

Aún más, el derecho de acceso a Internet, como la puerta para acceder a la sociedad digital, que pareciera ser un nuevo derecho, encuentra también relación con el derecho a la igualdad para el ejercicio de derechos como el de información y educación.

Como último aspecto que contribuye a responder la pregunta que nos planteamos, al referirnos a los derechos digitales, es importante hacer alusión al carácter novedoso de alguno de ellos, con el fin de mostrar que, si bien están sustentados en derechos tradicionales fundamentales, muestran un amplio desarrollo que podría justificar una regulación que permita la eficacia de su protección y la seguridad jurídica de quienes pueden esgrimir su derecho a la defensa ante su conculcación.

Ya mencionamos el derecho de acceso a Internet derivado si se quiere del principio de igualdad y del servicio universal, pero que, sin ninguna duda, comporta una novedad que podría requerir un reforzamiento normativo para garantizarlo a todos los ciudadanos, en la medida en que, como se ha señalado, es la puerta de entrada al ejercicio de los derechos digitales fundamentales en este nuevo universo.

El derecho al olvido, en las búsquedas de Internet y en redes sociales y servicios equivalentes, es un buen ejemplo de lo afirmado. Los datos no pueden congelarse y mantenerse sin límites en el tiempo en detrimento de los derechos de los ciudadanos en cuanto a su honor e intimidad. Este aspecto es especialmente diciente en una sociedad digital donde los datos pueden mantenerse en el tiempo durante muchos años y claramente afectan al ciudadano, a diferencia de los medios impresos que fácilmente caen en el olvido.

El Tribunal de Justicia Europeo tuvo oportunidad de referirse al tema en el caso Google v. Agencia Española de Protección de Datos (AEPD) (asunto C-131/12), como se plantea en la siguiente síntesis:

La actividad de los motores de búsqueda como Google constituye un tratamiento de datos de carácter personal, del que es responsable el propio motor, dado que éste determina los fines y los medios de esta actividad.

Ese tratamiento está sometido a las normas de protección de datos de la Unión Europea, dado que Google ha creado en un Estado miembro un establecimiento para la promoción y venta de espacios publicitarios y cuya actividad se dirige a los habitantes de ese Estado.

Las personas tienen derecho a solicitar del motor de búsqueda, con las condiciones establecidas en la Directiva de protección de datos, la eliminación de referencias que les afectan, aunque esta información no haya sido eliminada por el editor ni dicho editor haya solicitado su desindexación. En caso de no atenderse su solicitud, las personas tienen derecho a recabar la tutela de la AEPD y de los Tribunales.

El derecho a la protección de datos de las personas prevalece, con carácter general, sobre el "mero interés económico del gestor del motor de búsqueda" salvo que el interesado tenga relevancia pública y el acceso a la información esté justificado por el interés público.

Se trata de saber si una noticia cierta y publicada en el pasado debe mantenerse por la eternidad en la medida en que se incorpora en las plataformas y buscadores y, como lo señala la sentencia, persigue de por vida a la persona afectada. Además, incorporar una noticia en los buscadores permite replicarla en forma exponencial a todos los que tienen acceso a plataformas como Google y, obviamente, a mantener un "inri" que perdurará aún después de su fallecimiento.

En conclusión, en esta sentencia se reconoce el derecho al olvido para no hacer desproporcionada e irracional una carga para un ciudadano.

Como lo señala el profesor De la Quadra en "los derechos en la sociedad digital: visión subjetiva y visión institucional" (sección 4.1, párr. 10) el Tribunal no se ha transformado en legislador, sino que, con fundamento en principios y valores presentes en la norma, ha dado una respuesta diferente en la articulación de derechos contrapuestos, sobre la base de que los presupuestos de hecho y los datos en el mundo digital y presencial son diferentes. No hay trato desigual al dar soluciones diferentes respecto de la presencialidad y del mundo digital.

En el listado de estos derechos aparece el testamento digital vinculado a los derechos de propiedad, herencia e imagen de una persona fallecida. Se trata de un pronunciamiento judicial del Tribunal Federal alemán (Bundesgerichtshof) de 12 de julio de 2018 (asunto III ZR 183/17), en el cual se otorga el derecho a lo padres que pretenden recuperar y disponer de los datos y comunicaciones recogidas en una red social de su hija fallecida, a lo que se negaba la red social.

Como se afirmó, la disyuntiva de regularlos o no, no atiende tanto a que se trate de nuevos derechos sino a discernir cual puede ser el mejor instrumento para su protección. De lo que se trata realmente, es de preguntarse si es necesario incorporar una nueva regulación para la protección de estos derechos digitales, vista la gravedad que tiene su desprotección en estas redes sociales y en las plataformas, y, además, el desconocimiento de derechos que en su visión institucional pueden afectar y afectan efectivamente los bastiones de la democracia.

Como argumento contrario, podría afirmarse que, si se trata de los mismos derechos tradicionales, en varias ocasiones y propio de la adecuación de las normas al entorno histórico en que se aplican, la jurisprudencia de nuestras altas cortes se ha preocupado por su garantía y protección y que, por ende, no serían requeridas mayores elucubraciones sobre estos temas.

Una posición en este sentido no sería compatible con la importancia del tema y con su desarrollo, a veces impensable, así estén soportados en los derechos tradicionales.

En efecto, no existe duda de la seguridad jurídica de consagrarse una regulación expresa en beneficio de la preservación de estos derechos digitales fundamentales, que daría mayor eficacia y tranquilidad a quien pretenda ejercer su derecho de defensa ante los gobiernos y ante los propietarios de los buscadores y plataformas. Sigue siendo la pelea y confrontación entre el David y el Goliat, donde un simple usuario se enfrenta al poder de las plataformas que en muchos casos ni siquiera los gobiernos han podido limitar, dada su posición dominante en el mercado y su predominio en las comunicaciones sociales. De la misma manera, sucede respecto del ciudadano que se enfrenta al gobierno de turno en la búsqueda de preservar su derecho a la dignidad.

Otro argumento corresponde a los perfiles insospechados de estos derechos en la sociedad digital y que pueden transcurrir varios años para que los tribunales emprendan su estudio, con la incertidumbre de que puedan aprehender su contenido y dictaminen su debida protección.

Todas estas consideraciones parecen mostrar la necesidad de su inclusión en el ordenamiento jurídico, a través de su enlistamiento o de la enunciación y consagración de sus garantías y reglas para que los ciudadanos estén facultados para solicitar su protección, independiente de si se trata de derechos nuevos o desarrollo de los tradicionales o si, en algún momento histórico, pueda la jurisprudencia abordar su estudio. Gran parte de los pronunciamientos de la Corte Constitucional sobre este punto han sido reseñados por Lugo Silva (en proceso de publicación).

Pero, además, es necesaria su preservación con la asignación legal de competencias, en forma preferible a agencias independientes, que aseguren su protección y la atención oportuna frente a reclamaciones por el desconocimiento de los derechos digitales.

El nivel de jerarquía de la norma dependerá de la configuración sistemática del ordenamiento jurídico de cada país, pero resulta patente la importancia de que su regulación se ubique en el entorno más alto posible. A fin de cuentas, nos estamos

refiriendo a derechos fundamentales consagrados en nuestras constituciones y a sus desarrollos en el mundo digital.

Finalmente, es menester que su regulación no esté referida exclusivamente a Internet sino en general a la sociedad digital y al desarrollo de las tecnologías. Aunque es claro que el Internet es el espacio donde más pueden presentarse las controversias sobre los derechos digitales, no puede olvidarse el desarrollo, con sus riesgos y beneficios, de la IA y del Big Data. Son conocidos los riesgos para la democracia, especialmente, con situaciones relacionadas en el ejercicio de los derechos electorales y la difusión de "fake news" a través de redes¹⁷. Así mismo, por el efecto en la aplicación de los algoritmos que permiten definir los perfiles de los ciudadanos y afectar sus derechos políticos, de imagen, de acceso al trabajo y, en general, atentar contra el pluralismo informativo. Vista la realidad podría afirmarse que tienen un fuerte grado de responsabilidad en la polarización de las sociedades sobre temas de actualidad que claramente afectan una democracia¹⁸.

Desde otra faceta, tampoco se propone por una regulación rígida e inflexible que desborde los objetivos señalados y desincentive los avances tecnológicos. Se trata de encontrar el correcto balance para permitir el desarrollo de estas nuevas tecnologías y de los legítimos negocios que encierran para quienes resultan propietarios de los buscadores y plataformas, sin demeritar los derechos de los usuarios, sus derechos fundamentales y algunos otros como el de competencia, que, no perteneciendo a esta categoría, no dejan de ser esenciales como instrumento para el ejercicio de los derechos de los ciudadanos.

IV. Conclusiones

De lo expuesto puede concluirse la importancia para que los Estados adopten un régimen jurídico que respalde el nuevo campo de acción de los derechos fundamentales tradicionales en la era digital, les otorgue seguridad jurídica y su mejor protección. La jerarquía de norma, de ley en sus diferentes clasificaciones o de rango constitucional, que posiblemente se muestre en el desarrollo de estos derechos digitales, será necesaria, dada su importancia y el innegable desarrollo de la sociedad digital.

Ello implicará, no solo el reconocimiento de estos derechos y de las garantías para su ejercicio, sino la necesidad de dotar de competencia legal a instituciones o agencias preferiblemente independientes o autónomas que permitan hacerlos efectivos.

17 Puede recordarse el caso de Cambridge Analytica y las elecciones presidenciales de Estados Unidos del 2016.

18 Es diciente la situación presentada en Colombia desde septiembre de 2020 a junio de 2021, a propósito de las protestas populares que iniciaron por un proyecto de reforma tributaria y que se fueron expandiendo a otras peticiones causadas por los graves desequilibrios económicos en el país y agravadas por la pandemia. La polarización causada por las noticias divulgadas en las redes sociales, en los chats colectivos y en los medios de comunicación, mostraban dos realidades distintas, según el interés del emisor. Por un lado, los excesos de la fuerza pública, y de otro, los excesos y vandalismos de algunos de los que participaban en las manifestaciones, con injustificados bloqueos en las vías y accesos a las ciudades, con pretensiones variadas y algunas simplemente económicas.

Resulta muy difícil, si no imposible, para el ciudadano común que quiera conocer la veracidad de los hechos, tener una fuente real y fidedigna. Es un buen ejemplo del poder de comunicación en la sociedad digital y de cómo se incrementa la polarización de la sociedad y la violencia frente a noticias que dan cuenta de graves violaciones a los derechos humanos que evidentemente se presentaron, aunque no siempre las informadas con videos correspondían a la realidad.

Existen ya desarrollos interesantes, no siempre uniformes pero esclarecedores de su contenido, que muestran la concepción y la importancia de los derechos digitales, en su mayoría vinculados a derechos fundamentales tradicionales, que claman por una protección expresa y clara por parte de los gobiernos y en defensa de los ciudadanos respecto de todos los actores del ecosistema digital, en especial, respecto de los dueños de las plataformas y buscadores, de los demás usuarios que extralimitan su derechos y de los gobiernos de turno, que pueden intentar coartar derechos inherentes a la democracia y el Estado Social de Derecho.

En síntesis, se trata de mantener la dimensión humanista de los derechos fundamentales y preservarlas de sus posibles violaciones en los instrumentos, dispositivos, elementos, aplicaciones y sistemas de la sociedad digital. Aunque los derechos fundamentales siguen siendo los mismos de la sociedad tradicional, es claro que tienen una nueva configuración en la sociedad digital.

La defensa de los derechos de los ciudadanos en la sociedad digital simplemente corresponde al mismo sustento constitucional del respeto de la dignidad de la persona humana y de sus derechos inviolables. Pero además de esta visión personalista y subjetiva, es claro que también es pertinente la visión social e institucional de los mismos, como sucede con el derecho de participación política, el poder judicial, los partidos políticos, la sociedad civil y las reglas del mercado y la competencia. Así mismo, respecto de otros derechos sociales, de los cuales no se puede prescindir a la hora de regular los derechos digitales.

La gran conclusión es entonces que, en la denominada sociedad de la información, en la cual las tecnologías de la información y las comunicaciones están en constante expansión y desarrollo, cobran una especial importancia por su transformación los derechos digitales de los ciudadanos en sus relaciones sociales, culturales, religiosas, políticas y económicas. Gran parte de ellos, han preferido el ejercicio de sus derechos y el desarrollo de sus relaciones en la sociedad digital más que en la sociedad presencial. Por ello, son necesarios instrumentos normativos de la mayor jerarquía posible que aseguren su protección en su visión personal e institucional.

BIBLIOGRAFÍA

- ATKearny (2010). Internet value chain economics.
- Bassini, M. (2019). Fundamental rights and private enforcement in the digital age. *European Law Journal*, 25, 182-197.
- Belli, L. (2016). End-to-End, Net Neutrality and Human Rights. En L. Belli y P. De Filippi, (Ed), *Net Neutrality Compendium. Human Rights, Free Competition and the Future of the Internet* (1a. ed., pp. 13-29). Springer.
- Belli, L. y De Filippi, P. (2016). General Introduction: Towards a Multistakeholder Approach to Network Neutrality. En L. Belli y P. De Filippi, (Ed), *Net Neutrality Compendium. Human Rights, Free Competition and the Future of the Internet* (1a. ed., pp. 1-7). Springer.
- Cerda Silva, A. (2013). Internet freedom is not enough: towards an Internet based on human rights. *Sur. International Journal of Human Rights*, 18(10), 17-31.
- De la Quadra-Salcedo, T. (en proceso de publicación). Los derechos en la sociedad digital: visión subjetiva y visión institucional. En E. González López (Dir.), *Hacia*

la construcción del derecho de tic. balance de la ley 1341 de 2009 y los desafíos de la nueva ley de modernización para el sector tic. Universidad Externado de Colombia.

- De la Quadra-Salcedo, T. (2018). Retos, riegos y oportunidades de la sociedad digital. En T. de la Quadra-Salcedo y J. Piñar Mañas (Dirs.), *Sociedad digital y derecho* (1a ed., pp. 21-86). Ministerio de Industria, Comercio y Turismo, Red.es y Boletín Oficial del Estado.
- Deibert, R. J. y Villeneuve, N. (2005). Firewalls and Power: An Overview of Global State Censorship of the Internet. En M. Klang y A. Murray (Ed.), *Human Rights in the Digital Age* (1a ed., pp. 111-124). GlassHouse Press.
- Dickinson, R. (2013). Transformation of the modern state: State sovereignty and human rights in the internet age. *Connecticut Journal of International Law*, 29(1), 51-70.
- Felten, B. (2016). There's No Economic Imperative to Reconsider on Open Internet. En L. Belli y P. De Filippi, (Ed.), *Net Neutrality Compendium. Human Rights, Free Competition and the Future of the Internet* (1a. ed., pp. 63-72). Springer.
- Habermas, J. (1986). Ciencia y técnica como ideología. Tecnos.
- Halpin, E. F., Hick, S y Hoskins, E. (2000). Introduction. En E. F. Halpin, S. Hick, y E. Hoskins. (Ed.), *Human Rights and the Internet* (1a. ed., pp. 3-15). Macmillan Press Ltd.
- Herrera Zapata, L. y González Rozo, L. (2021). La Inclusión Digital como Herramienta para Lograr la Inclusión Social y los Objetivos de Desarrollo Sostenible en J. Henao Pérez. y S. Téllez Cañas (Eds.). *Disrupción tecnológica, transformación digital y sociedad. Tomo II. Política Públicas y regulación en las tecnologías disruptivas* (1a ed., pp. 127-169). Universidad Externado de Colombia.
- Hussain, A. (2000). Preface. En E. F. Halpin, S. Hick, y E. Hoskins. (Ed.), *Human Rights and the Internet* (1a. ed., pp. 10-12). Macmillan Press Ltd.
- Italia. Declaración de derechos en Internet. (26 de junio de 2015).
- Iftimiei, A. (2017). Evolution of the fundamental human rights and freedoms catalog: Access to the internet. *Revista de Drept Constitutional*, 2017(2), 48-56.
- López Zamora, P. (2020). Contextualización y desarrollo de los ¿nuevos? Derechos digitales, incorporados en el título X de la LOPDGDD, dentro del panorama de los derechos fundamentales. *Revista aforismos* (2), 197-217.
- Lucchi, N. (2014). Internet content governance and human rights. *Vanderbilt Journal of Entertainment and Technology Law*, 16(4), 809-856.
- Lugo Silva, C. (en proceso de publicación). Debates contemporáneos en torno a la protección de los Derechos de los usuarios digitales. En E. González López (Dir.), *Hacia la construcción del derecho de tic. balance de la ley 1341 de 2009 y los desafíos de la nueva ley de modernización para el sector tic.* Universidad Externado de Colombia.
- Matías Camargo, S (2013). La Teoría del Servicio Público y las Telecomunicaciones. *Diálogos de Saberes* (38).

- Mavriki, P. y Karyda, M. (2020). Big Data Analytics: From Threatening Privacy to Challenging Democracy. En *E-Democracy – Safeguarding Democracy and Human Rights in the Digital Age* (1a. ed., pp. 3-17). Springer.
- McDiarmid, A. y Shears, M., (2016). The Importance of Internet Neutrality to Protecting Human Rights Online. En L. Belli y P. De Filippi, (Ed), *Net Neutrality Compendium. Human Rights, Free Competition and the Future of the Internet* (1a. ed., pp. 31-41). Springer.
- Mihr, A. (2017). Cyber Justice. *Human Rights and Good Governance for the Internet*. Springer.
- Miranda Bonilla, H. (2016). El acceso a internet como derecho fundamental. Revista jurídica IUS Doctrina (15), 1-23.
- Naciones Unidas, Asamblea General, Consejo de Derechos Humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. UN Doc. A/HRC/17/27 (16 de mayo de 2011).
- Naciones Unidas, Asamblea General, Consejo de Derechos Humanos. Resolución sobre la promoción, protección y disfrute de los derechos humanos en Internet. UN Doc. A/HRC/RES/20/8 (16 de julio de 2012).
- Naciones Unidas, Asamblea General, Consejo de Derechos Humanos. Resolución sobre la promoción, protección y disfrute de los derechos humanos en Internet. UN Doc. A/HRC/RES/26/13 (14 de julio de 2014).
- Naciones Unidas, Asamblea General, Consejo de Derechos Humanos. Resolución sobre la promoción, protección y disfrute de los derechos humanos en Internet. UN Doc. A/HRC/32/L.20 (27 de junio de 2016).
- Naciones Unidas, Asamblea General, Consejo de Derechos Humanos. Resolución sobre la promoción, protección y disfrute de los derechos humanos en Internet. UN Doc. A/HRC/RES/38/7 (17 de julio de 2018).
- OCDE (2017). Estudio de la OCDE sobre telecomunicaciones y radiodifusión en México 2017. <http://dx.doi.org/10.1787/9789264280656-es>
- Paré, D. (2005). The Digital Divide: Why the 'The' is Misleading en M. Klang y A. Murray (Ed.), *Human Rights in the Digital Age* (1a ed., pp. 85-97). GlassHouse Press.
- Pedreschi Garcés, W; León Pachecho, J y Baldeón Miranda, C (2016). ¿Es internet un servicio público? Breves reflexiones a partir de marco normativo vigente. Revista de Derecho Administrativo (12), 85-92.
- Pérez Martínez, J y Martín Núñez, J (2018). Regulación del ecosistema digital. En E. González López (Dir.), *El ecosistema digital y las autoridades de regulación de los sectores audiovisual y TIC* (1ª ed, pp. 1277-1306). Universidad Externado de Colombia.
- Pisanty, A. (2016). Network Neutrality Debates in Telecommunications Reform: Actors, Incentives, Risks en L. Belli y P. De Filippi, (Ed), *Net Neutrality Compendium. Human Rights, Free Competition and the Future of the Internet* (1a. ed., pp. 127-139). Springer.

- Pollicino, O. (2019). Judicial protection of fundamental rights in the transition from the world of atoms to the word of bits: The case of freedom of speech. European Law Journal, 25, 155-168.
- Pollicino, O. y Susi, M. (2019). Internet and human rights law: Introduction. European Law Journal, 25, 120–121.
- Pollicino, O. (2020) The Right to Internet Access: Quid Iuris? En Von Arnauld A. et al (ed.) *The Cambridge Handbook New Human Rights*. (1º ed. p. 265-275) Cambridge University Prees.
- Sánchez Morón, M. (2013) Derecho Administrativo. Parte General (9). Editorial Tecnos.
- Rowland, D. (2005). Free Expression and Defamation en M. Klang y A. Murray (Ed.), *Human Rights in the Digital Age* (1a ed., pp. 55-70). GlassHouse Press.
- Sereno, M. P. (2013). Internet and Human Rights: Issues and Challenges. Asian Journal of Legal Studies, 2013, 93-101.
- Sinclair, N. (2015). Identity theft en *Privacy Rights in the Digital Age* (1a. ed., pp. 290-294). Grey House Publishing, Inc.
- Susi, M. (2019). The internet balancing formula. European Law Journal, 25, 198–212.
- Unión Europea. Parlamento Europeo. Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre una Ley de Servicios Digitales: adaptación de las normas de Derecho mercantil y civil a las entidades comerciales que operan en línea (2020/2019(INL)).
- Waldo, J., Lin, H. S., y Millett, L. I. (2007). *Engaging privacy and information technology in a digital age*. National Academies Press.
- Wischmeyer, T. (2019). Making social media an instrument of democracy. European Law Journal, 25, 169–181.

Jurisprudencia

- Consejo Constitucional de Francia. (10 de junio de 2009). Sentencia No. 2009-580 DC.
- Corte Constitucional de Colombia. (8 de junio de 2012). Sentencia T-428.
- Corte Suprema de Estados Unidos. (2017). *Packingham v. North Carolina*. 137 S. Ct. 1730.
- Sala Constitucional de la Corte Suprema de Justicia de Costa Rica. (14 de julio de 2017). Resolución No. 11212-2017.
- Tribunal Constitucional del Perú. (4 de abril de 2001). Expediente N.º 02-2001-AI/TC.
- Tribunal Federal de Alemania. (2 de julio de 2018). Asunto III ZR 183/17.
- Unión Europea. Tribunal de Justicia Europeo. (13 de mayo de 2014). *Google v. Agencia Española de Protección de Datos (AEPD)*. Asunto C-131/12.
- Unión Europea. Tribunal Europeo de Derechos Humanos. (17 de enero de 2017). *Jankovskis v. Lituania*. Sentencia núm. 21575/08.

Legislación

Código Sustantivo del Trabajo (1951) (Colombia).

Congreso de la República de Colombia. (11 de julio de 1994). Ley por la cual se establece el régimen de los servicios públicos domiciliarios y se dictan otras disposiciones. [Ley 142 de 1994]. Diario Oficial.

Congreso de la República de Colombia. (30 de julio de 2009). Ley por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC –, se crea la Agenda Nacional de Espectro y se dictan otras disposiciones. [Ley 1341 de 2009]. Diario Oficial.

Congreso de la República de Colombia. (29 de julio de 2021). Ley de Internet como servicio público esencial y universal. [Ley 2108 de 2021]. Diario Oficial.

Congreso de los Estados Unidos Mexicanos. (23 de mayo de 2014). Ley Federal de Competencia Económica. Diario Oficial de la Federación.

Congreso de los Estados Unidos Mexicanos. (14 de julio de 2014). Ley Federal de Telecomunicaciones y Radiodifusión. Diario Oficial de la Federación.

Congreso Nacional de Brasil. (23 de abril de 2014) Ley N° 12.965, de 23 de abril de 2014. Diario Oficial.

Constitución Política de la República de Colombia (Colombia) (1991).

Constitución Política de los Estados Unidos Mexicanos (1917) (México).

El Senado y la Cámara de Diputados de la Nación Argentina. (18 de diciembre de 2014). Ley Argentina Digital. [Ley 27.078]. Boletín Oficial.

Gobierno Nacional de Argentina. (29 de diciembre de 2015). Decreto de Necesidad y Urgencia 267/2015). Boletín Oficial.

Gobierno Nacional de Argentina. (21 de agosto de 2020). Decreto de Necesidad y Urgencia 690/2020. Boletín Oficial.

La Asamblea Nacional de Francia y el Senado. (7 de octubre de 2016). LOI no 2016-1321 du 7 octobre 2016 pour une République numérique [Ley 2016-1321, de 7 de octubre de 2016 para una República Digital].

Las Cortes Generales de España. (5 de diciembre de 2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. BOE.

Presidencia de la República de Brasil. (20 de marzo de 2020). Decreto 10.282, de 20 de marzo de 2020. Diario Oficial.



EL ENFOQUE EUROPEO DE INTELIGENCIA ARTIFICIAL

THE EUROPEAN ARTIFICIAL INTELLIGENCE APPROACH

EDUARDO GAMERO CASADO¹

RESUMEN

El desarrollo de sistemas de inteligencia artificial (IA) plantea enormes expectativas de desarrollo económico y social, permitiendo sensibles mejoras de prestaciones y servicios tanto en el sector público como en el privado. En paralelo, su empleo suscita grandes dilemas éticos y jurídicos. La Unión Europea ha consolidado un enfoque propio en la cuestión, promoviendo un marco regulatorio armonizado en todos los Estados miembros, que promueva la seguridad jurídica y se cimente en los valores europeos, cuidando la preservación de los derechos fundamentales. Esto puede suponer una desventaja competitiva para los desarrollos europeos de IA frente a los de otros lugares del mundo en los que no existan estas limitaciones y cargas regulatorias. Siendo conscientes de ello, las instituciones europeas lo consideran irrenunciable, y aspiran a que logre un efecto emulador en países y empresas terceros. En este trabajo se exponen los rasgos generales de ese enfoque, y se analiza la ambiciosa propuesta regulatoria que se encuentra en proceso de aprobación.

PALABRAS CLAVE

Inteligencia artificial | IA | Regulación | Unión Europea

ABSTRACT

The development of artificial intelligence (AI) systems raises enormous expectations for economic and social development, enabling significant improvements in benefits and services in both the public and private sectors. At the same time, their use raises major ethical and legal dilemmas. The European Union has consolidated its own approach to the issue, promoting a harmonized regulatory framework in all Member States that promotes legal certainty and is based on European values, while taking care to preserve fundamental rights. This may put European AI developments at a competitive disadvantage compared to those in other parts of the world where such regulatory constraints and burdens do not exist. Aware of this, the European institutions consider it essential, and hope that it will have an emulative effect in third countries and enterprises. This paper presents the general features of this approach and analyzes the ambitious regulatory proposal currently in the process of approval.

KEY WORDS

Artificial intelligence | AI | Regulation | European Union

¹ Catedrático de Derecho Administrativo. Universidad Pablo de Olavide, de Sevilla. ORCID 0000-0002-6734-8672. Doctor en Derecho por la Universidad de Sevilla (1994); Licenciado en Derecho (especialidad en Derecho Público) por la misma Universidad (1990). Consejero la firma Montero - Aramburu Abogados desde 2013. Académico correspondiente de la Real Academia de Legislación y Jurisprudencia de España. Premio Blas Infante de investigación en Administración Pública. Premio de investigación de la Real Academia Sevillana de Legislación y Jurisprudencia. Director de varios Proyectos de investigación de Excelencia del Plan Nacional de I+D+i del Gobierno de España. Autor de nueve monografías y director o coordinador de otras doce, publicadas en reputadas editoriales jurídicas. Coautor del "Manual básico de Derecho administrativo", (editorial Tecnos, más de 1.000 págs.) con 18 ediciones. Una de sus principales líneas de investigación es la administración electrónica y la inteligencia artificial aplicadas al sector público.

CONTENIDO

1. Introducción; **2.** Las bases del enfoque europeo de IA: El libro blanco; **2.1.** El “ecosistema de excelencia”; **2.2.** El “ecosistema de confianza”; **3.** La propuesta de reglamento estableciendo normas armonizadas sobre IA: La ley europea de inteligencia artificial; **3.1.** Ámbito de aplicación: la definición de IA. El sistema de semáforo; **3.2.** Sistemas prohibidos; **3.3.** Sistemas de alto riesgo; **3.4.** Resto de sistemas; **3.5.** Otras determinaciones relevantes; **4.** Complementariedad entre el enfoque europeo sobre IA y otros ámbitos: La estrategia europea de datos y blockchain; **5.** Valoración general; **6.** Referencias bibliográficas.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 8 de junio de 2021 y aprobado para su publicación el 23 de agosto de 2021.

1. Introducción

La inteligencia artificial (en lo sucesivo, IA), es una tecnología emergente que goza de una implantación cada vez mayor, especialmente en las economías más avanzadas, destacando China y Norteamérica. Las expectativas de desarrollo humano y crecimiento económico asociadas a la IA son extraordinarias: según la UNESCO, se espera que genere 4 billones de dólares de valor añadido para 2022², y existen ya innumerables casos de uso que avalan su utilidad en los más variados campos, tanto en el sector público como en el privado.

Ahora bien, el uso de esta tecnología también suscita muchos dilemas e interrogantes: desde la posibilidad de erigirse en un nuevo factor de desigualdad entre países (por aquéllos que carezcan de medios para implantarla), hasta los importantes reparos éticos y legales que derivan de su aplicación (discriminación, protección de datos, vías de control de decisiones sustentadas en algoritmos e IA), pasando por el hecho de que algunos de los procesos asociados a la IA y a los algoritmos determinan una evolución autónoma que impiden saber posteriormente (mediante un discurso intelectual humano) por qué estos sistemas adoptaron la decisión, esto es, con qué concretos criterios o fundamentos llegaron estos sistemas basados en IA y algoritmos a los resultados que alcanzaron.

Todo esto ha preocupado e interesado a la Academia, suscitando ya un importante acervo de aportaciones, a pesar de que el pensamiento jurídico sobre esta cuestión sea tan incipiente como la propia tecnología a analizar³. Un comentario generalizado en

2 Véase la información facilitada por el organismo en relación con la elaboración de una Recomendación sobre la ética de la IA, accesible en <https://es.unesco.org/artificial-intelligence/ethics> (última visita: 31/05/2021).

3 Por ofrecer tan solo algunas aportaciones recientes, de nuestro entorno inmediato y especialmente centradas en el sector público, podemos mencionar los trabajos incluidos en el n.º 50 (2019) de la Revista General de Derecho Administrativo, con una sección monográfica coordinada por Andrés BOIX PALOP y Lorenzo COTINO HUESO, que incluye importantes aportaciones del propio Prof. Cotino y de Agustí CERRILLO MARTÍNEZ, Juli PONCE SOLE, Antonio MERCHÁN MURILLO, Dolors CANALS AMETLLER, Marina SANCHO LÓPEZ, Clara VELASCO RICO, Wilma ARELLANO TOLEDO, Adrián PALMA ORTIGOSA y Ana ABA-CATOIRA, entre otros. También es relevante el n.º 58 de la Revista Catalana de Dret Públic, con aportaciones de Agustí CERRILLO MARTÍNEZ, Lorenzo COTINO HUESO, Ramón GALINDO CALDÉS, Ricard MARTÍNEZ MARTÍNEZ Y Julián VALERO TORRIJOS. Asimismo, los trabajos incluidos en el n.º 1 (2020) de la European Review of Digital Administration & Law (ERDAL), que incluye una sección monográfica sobre IA con valiosos trabajos de Derecho español y comparado por cuenta

estas aportaciones es la inexistencia de un marco jurídico adecuado para regular la IA.

Comparto ese reproche, si bien he procurado insistir en otros trabajos⁴ en la idea de que la omisión (hasta la fecha) de un régimen específico de la IA no supone que ser trate de una actividad sin ley (como dirían en el lejano oeste): existen principios y reglas generales del Derecho que resultan aplicables a cualquier actividad, y por consiguiente, también a la IA: igualdad y no discriminación, protección de datos, necesidad de motivación de decisiones basadas en algoritmos e IA, etc., son reglas y principios proclamados con carácter general en el escenario jurídico y que en algunos casos adquieren incluso relieve constitucional. No es necesario que se diga expresamente que la IA queda sujeta a esos límites y requisitos legales, como tampoco es necesario que se indique así expresamente en cualquier otra actividad, pues va de suyo que, debido al carácter transversal de estas normas, son aplicables a cualesquier actividades.

En cualquier caso, sí resulta conveniente regular expresa y específicamente la IA, para atender las singularidades de esta tecnología y establecerle unos límites o requisitos específicos, en casos de uso que se presentan particularmente delicados por su impacto en otros bienes y derechos de la ciudadanía.

En ese contexto se encuadran las iniciativas que viene impulsando la Unión Europea (en adelante, UE) para dotar la IA de un marco normativo específico y armonizado en toda la Unión. Salvo en ámbitos puntuales –como en la industria de fabricación–, Europa manifiesta cierto retraso en el desarrollo de soluciones de IA respecto a China y Norteamérica, tanto en el sector público como en el privado. Pero ha dado buena cuenta de su preocupación por abordar el fenómeno, tanto para potenciar el uso de la IA, como para establecer un marco normativo que lo regule de conformidad con los valores y principios europeos.

Entre los principales hitos que podemos señalar para atestiguarlo se encuentran, en

de Jean-Bernard AUBY, Agustí CERRILLO MARTÍNEZ, Daniele MARONGIU, Julián VALERO TORRIJOS, Antonio BARONE, María Cristina CAVALLARO, Andrés BOIX PALOP, Lucie CLUZEL-MÉTAYER, Cristina FRAENKEL-HAEBERLE, Elena BUOSO, Angelo Giuseppe OROFINO, Fulvio CONSTANTINO, Fabio BRAVO, Elise DEGRAVE y Giovani GALLONE. Tampoco pueden dejar de citarse los 24 números que se han publicado de la revista Inteligencia Artificial, publicada por la Iberoamerican Society of Artificial Intelligence; y los recientes trabajos de Andrés BOIX PALOP: “Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la toma de decisiones”, Revista de Derecho Público: Teoría y Método, vol.1, 2020 Alejandro HUERGO LORA (Dir.): La regulación de los algoritmos, Aranzadi-Thomson-Reuters, Cizur Menor, 2020; Julio TEJEDOR BIELSA: “Transformación digital, blockchain e inteligencia artificial en la Administración pública”, Revista Española de Derecho Administrativo, n.º209, 2020; Alba SORIANO ARNANZ: “Decisiones automatizadas y discriminación: aproximación y propuestas generales”, Revista General de Derecho Administrativo, n.º 56, 2021; y Juan Carlos HERNANDEZ PEÑA: “Decisiones algorítmicas de perfilado: régimen y garantías jurídicas”, Revista Española de Derecho Administrativo, n.º203, 2020, así como, del mismo autor, “Gobernanza de la inteligencia artificial en la Unión europea. La construcción de un marco ético-jurídico aún inacabado”, Revista General de Derecho Administrativo, n.º 56, 2021.

4 Véase Eduardo GAMERO CASADO: “Compliance (o cumplimiento normativo) de desarrollos de inteligencia artificial para la toma de decisiones administrativas”, Diario La Ley, n.º50, Sección Ciberderecho, de 19/04/2021; accesible en <https://diariolaleylaleynext.es>; así como mi trabajo “Necesidad de motivación e invalidez de los actos administrativos sustentados en inteligencia artificial o en algoritmos”, Almacén de Derecho, 04/02/2021, accesible en <https://almacendedederecho.org>

primer lugar, dos relevantes documentos de la Comisión Europea: la Comunicación de la Comisión Europea Inteligencia artificial para Europa COM (2018) 237, de 27 de abril; y el Plan coordinado sobre la inteligencia artificial, Comunicación de la Comisión Europea COM (2018) 795, de 7 de diciembre, donde la cuestión se aborda con profundidad y se sientan las bases para los pasos sucesivos. Poco más tarde se aprobó la Comunicación COM (2019)168, de 8 de abril, Generar confianza en la inteligencia artificial centrada en el ser humano. Seguidamente debemos destacar el Libro blanco de la UE sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y a la confianza⁵: un documento clave en la cuestión, en el que se establecen las líneas maestras de una futura regulación en la materia y al que dedicaremos el siguiente apartado del trabajo; de este documento también cabe destacar su íntima conexión con la Estrategia europea de datos, Comunicación de la Comisión COM (2020) 66 final, aprobada el mismo día y sobre la que volveremos más tarde.

En paralelo a la Comisión, también el Parlamento Europeo ha impulsado varias iniciativas, entre las que cabe destacar el Marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas⁶; y más recientemente, su Resolución sobre Inteligencia artificial: cuestiones de interpretación y de aplicación del Derecho internacional⁷.

Pero, sin lugar a dudas, el documento más relevante hasta la fecha es la Propuesta de Reglamento del Parlamento Europeo y el Consejo estableciendo reglas armonizadas sobre inteligencia artificial (Ley de inteligencia artificial) [sic] y modificando determinados actos legislativos de la Unión⁸. Se trata de la primera versión de una ambiciosa propuesta normativa a la que dedicaremos atención pormenorizada en el apartado 3 de este trabajo.

Para concluir este recorrido, debemos hacer mención al Reglamento (UE) 2021/694, del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240. Esta disposición, cuyo rango normativo equivale al de una ley europea, y que por tanto resulta de especial interés dado su carácter vinculante, regula en su art.5 los objetivos específicos de la Unión en materia de IA. Aludiremos a su contenido en los lugares oportunos.

La aproximación al tema en todos estos precedentes se inspira en unas premisas básicas que sintetizamos así:

- Se requiere un enfoque europeo común en torno a la IA. La eventual existencia de modelos y estrategias nacionales diferentes pondría en peligro la seguridad jurídica, reduciría la confianza de los ciudadanos y dificultaría el surgimiento de una industria europea dinámica, al ser diferente el marco legal en cada uno de los países miembros. Debe evitarse la fragmentación del mercado único.
- Es preciso que la IA europea se asiente en los valores y derechos fundamentales

5 Comunicación de la Comisión Europea COM(2020) 65 final, de 19 de febrero.

6 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)].

7 Resolución del Parlamento Europeo, de 20 de enero de 2021, sobre inteligencia artificial: cuestiones de interpretación y de aplicación del Derecho internacional en la medida en que la UE se ve afectada en los ámbitos de los usos civil y militar, así como de la autoridad del Estado fuera del ámbito de la justicia penal [2020/2013(INI)].

8 Accesible en <https://digital-strategy.ec.europa.eu> (Última visita: 31/05/2021).

de la Unión, como la dignidad humana, la protección de la privacidad o la sostenibilidad ambiental. Resulta especialmente sensible en este punto el enfoque antropocéntrico y la reivindicación de supervisión y control humano de los sistemas de IA.

Con estas premisas de partida procedamos a profundizar en la cuestión.

2. Las bases del enfoque europeo de IA: El libro blanco

La estrategia europea en materia de IA lanzada en 2018 se ha perfilado en el Libro blanco de 2020. A partir de sus postulados se desplegarán las diferentes líneas de actuación de la UE en la materia. Por ello resulta especialmente necesario detenerse en algunos de sus contenidos, pues nos suministran las claves con las que interpretar otros pasos que se están dando (como la propuesta de Reglamento) y que se darán en el futuro.

2.1. El “ecosistema de excelencia”

Con esta expresión, la Comisión Europea alude a la necesidad de crear un entorno de impulso a la IA en el conjunto de la economía y del sector público de la UE. Se trata, esencialmente, de un marco político. En colaboración con los sectores público y privado, los objetivos del marco son movilizar recursos para obtener un ecosistema de excelencia en los desarrollos de IA a lo largo de toda la cadena de valor, partiendo de la investigación y la innovación, así como crear los incentivos adecuados para acelerar la adopción de soluciones basadas en IA.

Sus principales líneas de acción son las siguientes:

- a) Colaboración con los Estados miembros. A tal efecto ya se aprobó un Plan coordinado en 2018 (citado), vigente hasta 2027, en el que se proponen casi 70 acciones conjuntas en áreas como la investigación, la inversión, la penetración en el mercado, el impulso de capacidades y talento, los datos, etc. Se pretende movilizar 20.000 millones de euros anuales en IA a todo lo largo de la presente década, para superar así el desfase existente respecto de otros bloques económicos mundiales.
- b) Potenciación de los centros de investigación en IA, a fin de que colaboren entre sí y alcancen envergadura suficiente para competir con los organismos que se encuentran a la vanguardia mundial. Como líneas prioritarias de investigación de aplicaciones de IA se señalan los sectores de la industria, la sanidad, el transporte, las finanzas, las cadenas de valor agroalimentarias, la energía y el medio ambiente, la silvicultura, la observación terrestre y el espacio.
- c) Desarrollo de habilidades. Es preciso fomentar programas educativos en IA que amplíen sensiblemente el universo de personas familiarizados con el manejo de esta tecnología. De esta manera se pretende formar a trabajadores y mejorar la cualificación profesional en materia de IA.
- d) Orientación a las pequeñas y medianas empresas (pymes). Este tipo de empresas suponen un importante pilar de la economía y del empleo en Europa, y se pretende evitar que, por las dificultades inherentes a su tamaño, queden al margen de los desarrollos de IA, perdiendo liderazgo y competitividad. Se promueve la cooperación entre pymes y la dotación de líneas de financiación específica para sus proyectos.

- e) Promoción de la asociación público-privada en materia de IA, en el marco del programa Horizonte Europa.
- f) Promover la implantación de la IA en el sector público, priorizando la atención sanitaria, las administraciones rurales y los operadores de servicios públicos.

Algunas de estas líneas de acción han pasado de ser soft law a convertirse en mandatos normativos, mediante el Reglamento (UE) 2021/694 (citado), por el que se establece el Programa Europa Digital: su rango normativo equivale al de una ley europea, y por tanto resulta de especial interés dado su carácter vinculante. En su art.5.1 regula los objetivos específicos de la contribución financiera de la Unión en materia de IA:

- Desarrollar y reforzar las capacidades y los conocimientos básicos de IA en la Unión, incluidos la creación y el fortalecimiento de los recursos de datos de calidad y sus correspondientes mecanismos de intercambio y las bibliotecas de algoritmos, garantizando al mismo tiempo un enfoque integrador y centrado en las personas, en consonancia con los valores de la Unión;
- Hacer accesibles las capacidades a las que se refiere la letra a) a todas las empresas, en especial a las pymes y las empresas emergentes, así como a la sociedad civil, las organizaciones sin ánimo de lucro, los centros de investigación, las universidades y las administraciones públicas, con objeto de maximizar sus beneficios para la sociedad y la economía europeas;
- Reforzar y poner en red instalaciones de ensayo y experimentación de IA en los Estados miembros;
- Desarrollar y reforzar los sistemas de producción y aplicación comerciales para facilitar la integración de tecnologías en las cadenas de valor y el desarrollo de modelos empresariales innovadores, para reducir el tiempo necesario para pasar de la innovación a la explotación comercial y fomentar la adopción de soluciones basadas en la IA en ámbitos de interés público y en la sociedad.

Siendo relevante todo ello, mayor interés se presenta para este trabajo la vertiente o dimensión jurídica de la IA, que pasamos a analizar seguidamente.

2.2. El “ecosistema de confianza”

Ya en la Introducción del Libro blanco se promueve un marco normativo para la IA que genere un ecosistema de confianza: “Generar un ecosistema de confianza constituye un objetivo político en sí mismo, y debe ofrecer seguridad a los ciudadanos para que adopten las aplicaciones de la inteligencia artificial y seguridad jurídica a las empresas y organismos públicos para que innoven usando esta última”. En el mismo lugar se sientan las directrices de ese ecosistema: “este marco debe velar por el cumplimiento de las normas de la UE, especialmente las normas de protección de los derechos fundamentales y los derechos de los consumidores, y en concreto con relación a los sistemas de inteligencia artificial que operan en la UE y presentan un riesgo elevado. La Comisión respalda firmemente un enfoque antropocéntrico”.

Además de esta necesidad intrínseca u ontológica –íntimamente conectada con los valores europeos–, la aprobación de un marco normativo europeo persigue un efecto pragmático: evitar la fragmentación del mercado único, de manera que las exigencias impuestas a los desarrollos de IA sean las mismas en toda la UE, permitiendo así la libre

circulación de la tecnología.

Y por añadidura, se proclama como objetivo confeso de esta regulación el de influir en esta materia allende las fronteras europeas. De un lado, sobre las grandes corporaciones tecnológicas mundiales, por una cuestión reputacional (supondría un valor añadido a la marca el alinearse con los requerimientos europeos y afirmar ante sus clientes y usuarios que respetan tales reglas y principios no solo en Europa, sino en todo el planeta), así como por pura economía de escala (si han de desarrollar productos adaptados a los estándares europeos, su rentabilización tiende a la implantación en otros mercados). Pero también, procurando influir en el ordenamiento de otros países, llegando el Libro blanco a insinuar que no se favorecerán los acuerdos comerciales de la UE con los países que no comparten los valores europeos en esta materia.

El Libro blanco identifica perfectamente (pág.14) los principales problemas que hacen necesaria una regulación de la IA: "Aunque la IA puede ofrecer muchas ventajas, por ejemplo, mejorando la seguridad de los productos y los procedimientos, también puede resultar nociva. Los daños pueden ser tanto materiales (para la seguridad y la salud de las personas, con consecuencias como la muerte, y menoscabos al patrimonio) como inmateriales (pérdida de privacidad, limitaciones del derecho de libertad de expresión, dignidad humana, discriminación en el acceso al empleo, etc.) y pueden estar vinculados a una gran variedad de riesgos. El marco regulador debe centrarse en cómo minimizar los distintos riesgos de sufrir daños, especialmente los más significativos". De modo que se identifican dos tipos esenciales de riesgos: sobre los derechos y sobre la seguridad; en el Libro blanco se detalla el alcance de estos riesgos, y se determina que el marco normativo debe orientarse esencialmente a su evitación o minimización.

En cuanto a los derechos, los que se encuentran expuestos a mayores riesgos son: la dignidad humana; la ausencia de discriminación por razón de sexo, raza u origen étnico, religión o credo, discapacidad, edad u orientación sexual; la protección de los datos personales y de la vida privada; el derecho a una tutela judicial efectiva y a un juicio justo; la libertad de expresión; la libertad de reunión; y la protección de los consumidores. En la mayoría de situaciones, la afección a estos derechos debida de defectos en el diseño de las soluciones de IA, por diferentes causas:

1. Infracción de la normativa de protección de datos personales al recopilar los bancos de datos mediante los que se entrena y programan los algoritmos.
2. Deficiencias en los bancos de datos que se utilizan para programar los algoritmos, dando lugar a sesgos de alcance discriminatorio: por ejemplo, que los inmigrantes incumplen las condiciones de otorgamiento de subvenciones (caso real que ha supuesto recientemente la caída del gobierno holandés), o desviaciones de raza o de género según las imágenes mediante las que entrena los sistemas de IA.
3. Deficiencias en el diseño de los sistemas, que obedecen a unas reglas lógicas distintas de las humanas y resultan en cierto sentido impredecibles, dando lugar a fallos de funcionamiento.
4. Imposibilidad de conocer esa lógica en ciertos casos, como los sistemas de IA basados en deep learning, redes neuronales y los llamados algoritmos de caja negra. En estos casos se pone en entredicho el derecho a conocer las razones por las que se adopta una decisión, siendo difícil (si no imposible) entenderla o rebatirla, y vulnerándose correlativamente la tutela judicial efectiva de las

personas afectadas por ella.

Por lo que se refiere a la seguridad, nos adentramos en un escenario de potenciales riesgos físicos derivados de los sistemas de IA. Resultan particularmente obvios en casos como la conducción autónoma, ya sea de tráfico rodado o aéreo; pero no cabe descartar este riesgo en toda suerte de productos manufacturados que pueden ocasionar daños a consumidores y usuarios. En este trabajo, centrado en los desarrollos de IA para el sector público, esta dimensión tiene menor interés relativo, aunque no puede descartarse por completo, en la medida que la prestación de ciertos servicios públicos, como la sanidad y el transporte, apliquen soluciones de IA.

En los dos planos, el Libro blanco recuerda que "Los desarrolladores e implementadores de la inteligencia artificial ya están sujetos a la legislación europea en materia de derechos fundamentales (la protección de datos, la privacidad o la no discriminación, entre otros), protección de los consumidores y normas sobre la seguridad de los productos y responsabilidad civil". Así pues, no se trata de regular ex novo, sino de colmar los vacíos que se aprecien, así como de aclarar las especificidades que resulten convenientes en atención a las particularidades que entraña la IA.

Los siete principios básicos que la Comisión Europea considera necesario establecer y regular para una IA fiable son⁹:

- acción y supervisión humanas;
- solidez técnica y seguridad;
- gestión de la privacidad y de los datos;
- transparencia;
- diversidad, no discriminación y equidad;
- bienestar social y medioambiental;
- rendición de cuentas.

Sentadas estas bases, en lugar de seguir el hilo conductor del Libro blanco (que nos ha sido útil para identificar las inquietudes y líneas maestras de actuación), a continuación resulta más provechoso adentrarse en la propuesta regulatoria que ya ha elaborado la comisión Europea para determinar cómo se articulan tales principios básicos.

No obstante, conviene cerrar este apartado con una nueva mención al Reglamento (UE) 2021/694 (citado), por el que se establece el Programa Europa Digital, en la medida que contiene una previsión ya vigente y que resulta oportuno destacar. En su art.5, dedicado a la IA, esta disposición establece la siguiente regla (apartado 1, in fine): "Las soluciones basadas en la IA y los datos que se faciliten deberán respetar el principio de privacidad y seguridad desde el diseño y deberán respetar plenamente la normativa sobre protección de datos". Se materializan, por tanto, en el Derecho positivo, algunas de las prescripciones previamente anunciadas por los documentos de la Comisión Europea.

⁹ Relacionados en el Libro blanco, pág.11; así como en la Comunicación de la Comisión COM(2019) 168, pág.4; ambos citados.

3. La propuesta de reglamento estableciendo normas armonizadas sobre IA: La ley europea de inteligencia artificial

El carácter estratégico y prioritario que entraña la IA para la UE ha quedado de manifiesto en la celeridad con la que se ha presentado por la Comisión Europea un proyecto normativo en la materia¹⁰: la “Propuesta de Reglamento del Parlamento Europeo y el Consejo estableciendo reglas armonizadas sobre inteligencia artificial (Ley de inteligencia artificial) [sic] y modificando determinados actos legislativos de la Unión” (en lo sucesivo, RIA).

Lo primero que hemos de decir es que la regulación europea adquiere la forma de Reglamento, no de Directiva¹¹: es decir, equivale a una ley europea, y de ahí esta mención específica - y también poco frecuente -, en el propio título de la disposición. Con la opción por esta forma normativa se logran dos objetivos principales¹²: el texto tiene efecto directo, es decir, eficacia vinculante, tanto para los Estados miembros como para la ciudadanía, desde su entrada en vigor, sin necesidad de acto alguno de trasposición al Derecho interno, lo que agiliza la aplicación efectiva de sus postulados sin necesidad de aguardar los plazos de trasposición; y logra un mayor grado de uniformidad en el régimen sustantivo y en su aplicación práctica, lo que constituye una de las razones que alimentan la promulgación de una norma europea sobre IA, a fin de potenciar la seguridad jurídica de ciudadanos y empresas.

En la memoria de acompañamiento de la propuesta se le predicen los siguientes objetivos específicos: 1) Garantizar que los sistemas de IA introducidos en el mercado de la Unión y utilizados sean seguros y respeten la legislación vigente sobre derechos fundamentales y los valores de la Unión; 2) Garantizar la seguridad jurídica para facilitar la inversión y la innovación en IA; 3) Mejorar la gobernanza y la aplicación efectiva de la legislación existente sobre derechos fundamentales y requisitos de seguridad aplicables a los sistemas de IA; y 4) Facilitar el desarrollo de un mercado único de IA legal, seguro y fiable de aplicaciones y evitar la fragmentación del mercado. Más sintéticamente, podemos decir que se pretende evitar la fragmentación del mercado interior en cuanto a los requisitos esenciales de los sistemas de IA en diferentes países, así como potenciar la seguridad jurídica acerca de la interpretación uniforme de tales requisitos.

Para lograr tales objetivos, la propuesta declara sustentarse en un enfoque regulador horizontal equilibrado y proporcionado, circunscrito a los requisitos mínimos necesarios

10 Accesible en <https://digital-strategy.ec.europa.eu> (última visita: 31/05/2021). Las citas literales que se hacen en este trabajo de este texto son traducciones propias, dado que la única versión oficial del documento es en inglés.

11 La base jurídica de la disposición es el artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), que prevé la adopción de medidas para garantizar el establecimiento y el funcionamiento del mercado interior.

12 Esta opción también se ha seguido en otras materias que presentan conexión o proximidad, como el Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/ CE (Reglamento eIDAS); o 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 (Reglamento general de protección de datos). El resultado ha sido que los Estados miembros apenas han dictado normas de Derecho interno en desarrollo de los reglamentos europeos, que se convierten en la disposición directamente invocada y esencialmente aplicable por todos los operadores jurídicos de la Unión.

para abordar los riesgos y problemas vinculados a la IA, sin limitar ni obstaculizar indebidamente el desarrollo tecnológico ni aumentar de forma desproporcionada el coste de la comercialización de las soluciones de IA. Este enfoque "de mínimos" no se traduce en una menor densidad normativa, toda vez que el texto articulado más sus anexos sobrepasan las 120 páginas; el principio de intervención mínima se refiere más bien a la intensidad de la regulación y la intervención, que procura mantener un delicado equilibrio entre las limitaciones que se imponen a la tecnología para alcanzar los fines propuestos por la normativa, y el libre mercado, en cuya capacidad de autocontrol descansa particularmente esta norma, como hemos de ver más adelante.

3.1. Ámbito de aplicación: la definición de IA. El sistema de semáforo

Importa destacar que el art.2 de la propuesta declara la aplicación del RIA a los proveedores que comercialicen o pongan en servicio sistemas de IA en la Unión, independientemente de que dichos proveedores estén establecidos en la Unión o en un tercer país; así como a los usuarios de los sistemas de IA ubicados en la Unión; y a los proveedores y usuarios de sistemas de IA que estén ubicados en un tercer país, cuando el resultado producido por el sistema se utilice en la Unión. Con estas cautelas se evitan fugas de aplicación derivadas de la deslocalización de proveedores y usuarios.

Una importante premisa para abordar esta regulación es definir qué se entiende por IA. La determinación de una descripción precisa de esta tecnología es crucial para lograr seguridad jurídica en su aplicación, delimitando su ámbito de aplicación de manera suficientemente precisa, pero al mismo tiempo, con la flexibilidad que requiere la eventual evolución de la tecnología.

La definición se encuentra en el art.3.1 RIA: "sistema de inteligencia artificial (sistema de IA): software desarrollado con una o varias de las técnicas y enfoques enumerados en el anexo I y que puede, para un conjunto determinado de objetivos definidos por el ser humano, generar resultados como contenidos, predicciones, recomendaciones o decisiones que influyen en los entornos con los que interactúan". Conforme al Anexo I, tales técnicas y enfoques son los siguientes:

- a) Enfoques de aprendizaje automático, incluyendo el aprendizaje supervisado, no supervisado y de refuerzo, utilizando una amplia variedad de métodos incluyendo el aprendizaje profundo;
- b) Enfoques basados en la lógica y el conocimiento, incluyendo la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, el razonamiento (simbólico) y los sistemas expertos;
- c) Enfoques estadísticos, estimación bayesiana, métodos de búsqueda y optimización.

El art.4 RIA faculta a la Comisión para adoptar actos delegados mediante los que modifique y actualice el Anexo I conforme a la evolución del mercado y de la tecnología. A decir de la Comisión -en la memoria de acompañamiento a la propuesta-, la definición de sistema de IA pretende ser lo más neutra posible desde el punto de vista tecnológico y a prueba de futuro, teniendo en cuenta la rápida evolución tecnológica y del mercado.

En cuanto a la estructura medular de la regulación, el reglamento sigue un enfoque basado en el riesgo, diferenciando en su Título II (clave de bóveda de toda la norma)

entre los usos de la IA que crean un riesgo inaceptable, un riesgo alto y un riesgo bajo o mínimo, en lo que coloquialmente se conoce como sistema de semáforo. De este modo se gradúa proporcionalmente la intensidad de las limitaciones y requisitos impuestos a los sistemas de IA, en función del riesgo que cada sistema comporte para los bienes jurídicos tutelados por la regulación.

3.2. Sistemas prohibidos

El primer grupo viene representado por los sistemas prohibidos, esto es, prácticas de IA que quedan vedadas en la UE. Se establecen en el art.5.1 y son las siguientes:

- a) La comercialización, puesta en servicio o uso de un sistema de IA que despliegue técnicas subliminales más allá de la conciencia de una persona con el fin de distorsionar materialmente su comportamiento de manera que cause o pueda causar a esa persona o a otra un daño físico o psicológico;
- b) La comercialización, puesta en servicio o uso de un sistema de IA que explote cualquiera de las vulnerabilidades de un grupo específico de personas debido a su edad, discapacidad física o mental, con el fin de distorsionar materialmente el comportamiento de una persona perteneciente a ese grupo de manera que cause o pueda causar a esa persona o a otra un daño físico o psicológico;
- c) La puesta en el mercado, la puesta en servicio o la utilización de sistemas de IA por parte de las autoridades públicas o en su nombre para la evaluación o clasificación de la fiabilidad de las personas físicas durante un determinado período de tiempo, basándose en su comportamiento social o en sus características personales o de personalidad conocidas o previstas, y cuya puntuación social conduzca a una de las siguientes situaciones o a ambas:
 - (i) El trato perjudicial o desfavorable de determinadas personas físicas o de grupos enteros de ellas en contextos sociales que no guardan relación con los contextos en los que se generaron o recopilaron originalmente los datos;
 - (ii) El trato perjudicial o desfavorable a determinadas personas físicas o a grupos enteros de ellas, injustificado o desproporcionado con respecto a su comportamiento social o a su gravedad;
- d) La utilización de sistemas de identificación biométrica a distancia "en tiempo real" en espacios de acceso público con fines policiales, a menos y en la medida en que dicha utilización sea estrictamente necesaria para uno de los siguientes objetivos¹³:
 - (i) La búsqueda selectiva de posibles víctimas específicas de delitos, incluidos los niños desaparecidos;
 - (ii) La prevención de una amenaza específica, sustancial e inminente para la vida o la seguridad física de las personas físicas o de un ataque terrorista;
 - (iii) La detección, localización, identificación o enjuiciamiento de un autor o sospechoso de una infracción penal contemplada en el apartado 2 del artículo 2 de la Decisión marco 2002/584/JAI del Consejo y sancionada en el Estado miembro en cuestión con una pena o una medida de seguridad privativa de

13 Los apartados 2 a 4 del art.5 añaden criterios y requisitos de aplicación de este supuesto.

libertad por un período máximo de al menos tres años, según determine la legislación de dicho Estado miembro.

Debe repararse en que esta lista, en realidad, es corta. Y en particular, que no rechaza la implantación de sistemas de IA cuyos resultados resultan todavía incomprensibles para la mente humana, como el deep learning, las redes neuronales o los algoritmos de caja negra. Tales sistemas podrán utilizarse, sometiéndose, en su caso, a las reglas que analizamos a continuación.

3.3. Sistemas de alto riesgo

Regulados en el Título III y en los Anexos II y III, constituyen el eje central de toda la regulación. Estos sistemas no están prohibidos, pero se sujetan a una serie de restricciones y a mecanismos de control ex ante y ex post mediante los que garantizar la aplicación efectiva del Reglamento. Se trata de una luz naranja en el semáforo, puesto que estos sistemas se pueden implantar siempre que se reúnan los requisitos que el propio Reglamento establece.

La delimitación de los sistemas de alto riesgo se articula mediante dos fórmulas acumuladas:

- 1) El art.6.1 RIA, que se encuentra esencialmente preocupado por la seguridad de los consumidores y usuarios, y califica como de alto riesgo los sistemas de IA que constituyan componentes de seguridad de un producto, o que sean en sí mismos productos, incluidos en la legislación europea de armonización expresamente reseñada en el Anexo II, siempre que el producto o componente deba someterse en dicha legislación a una evaluación de conformidad por parte de un tercero (acreditación y certificación de productos y componentes) antes de su comercialización o puesta en servicio. La lista del Anexo II incluye máquinas, juguetes, productos sanitarios, vehículos a motor, aeronaves, embarcaciones, ascensores, equipos radioeléctricos, equipos de presión, aparatos de gas, equipos marinos, componentes ferroviarios, etc.
- 2) El art.6.2 RIA, mediante el que, por remisión al Anexo III (que la Comisión Europea está facultada a modificar y actualizar, de acuerdo con criterios predeterminados por la norma¹⁴) se relacionan nominativamente sistemas de IA cuyos riesgos ya se han materializado a día de hoy o existe un elevado consenso en la probabilidad de que se materialicen en un futuro próximo. Esta lista es heterogénea y presta cobertura a bienes jurídicos muy diversos. A pesar de su amplitud, conviene conocerla por ser sintomática tanto de las inquietudes que inspiran la normativa, como el alcance que tendrá su aplicación. De tal manera que, en el Anexo III se consideran de alto riesgo los sistemas de IA que se implementen en cualquiera de las siguientes áreas:
 1. Identificación biométrica remota “en tiempo real” e identificación de las personas físicas;
 2. Gestión y funcionamiento de las infraestructuras críticas: tráfico rodado y suministro de agua, gas, calefacción y electricidad.
 3. Educación y formación profesional: a) Los sistemas de IA destinados a ser utilizados para determinar el acceso o asignar a las personas físicas a las

14 Se establecen en el art.7.2 RIA, estableciendo orientaciones para la evaluación de los riesgos.

instituciones educativas y de formación profesional; b) Los sistemas de IA destinados a ser utilizados con el fin de evaluar a los estudiantes en las instituciones educativas y de formación profesional y para evaluar a los participantes en las pruebas comúnmente requeridas para la admisión en las instituciones educativas.

4. Empleo, gestión de los trabajadores y acceso al autoempleo: a) Los sistemas de IA destinados a ser utilizados para la contratación o selección de personas físicas, especialmente para anunciar las vacantes, cribar o filtrar las solicitudes, evaluar a los candidatos en el curso de las entrevistas o pruebas; b) Al destinado a ser utilizado para tomar decisiones sobre la promoción y la terminación de las relaciones contractuales relacionadas con el trabajo, para la asignación de tareas y para el seguimiento y la evaluación del rendimiento y el comportamiento de las personas en dichas relaciones.
5. Acceso y disfrute de los servicios privados esenciales y de los servicios y prestaciones públicas: a) Los sistemas de IA destinados a ser utilizados por las autoridades públicas o en nombre de ellas para evaluar el derecho de las personas físicas a las prestaciones y servicios de asistencia pública, así como para conceder, reducir, revocar o reclamar dichas prestaciones y servicios; b) Los sistemas de IA destinados a ser utilizados para evaluar la solvencia de las personas físicas o establecer su puntuación de crédito, con la excepción de los sistemas de IA puestos en servicio por proveedores a pequeña escala para su propio uso; c) Los sistemas de IA destinados a ser utilizados para despachar, o para establecer la prioridad en el despacho de los servicios de primera respuesta de emergencia, incluidos los bomberos y la ayuda médica.
6. Criminalidad: Los sistemas de IA destinados a ser utilizados por las autoridades policiales para a) Realizar evaluaciones individuales del riesgo de las personas físicas con el fin de evaluar el riesgo de una persona física de delinuir o reincidir o el riesgo para las posibles víctimas de delitos; b) Utilizarse por las autoridades policiales como polígrafos y herramientas similares o para detectar el estado emocional de una persona física; c) Detectar falsificaciones profundas; d) Evaluar la fiabilidad de las pruebas en el curso de la investigación o el enjuiciamiento de delitos; e) Predecir la ocurrencia o reincidencia de una infracción penal real o potencial basada en la elaboración de perfiles de personas físicas, o la evaluación de rasgos y características de la personalidad o del comportamiento delictivo anterior de personas físicas o grupos; f) Elaborar perfiles de personas físicas en el curso de la detección, investigación o enjuiciamiento de delitos; g) Analizar la delincuencia en relación con las personas físicas, permitiendo a las autoridades policiales buscar grandes conjuntos de datos complejos, relacionados o no, disponibles en diferentes fuentes de datos o en diferentes formatos de datos, con el fin de identificar patrones desconocidos o descubrir relaciones ocultas en los datos.
7. Gestión de la migración, el asilo y el control de fronteras: Los sistemas de IA destinados a ser utilizados por las autoridades públicas a) Como polígrafos y herramientas similares o para detectar el estado emocional de una persona física; b) Para evaluar un riesgo, incluido un riesgo para la seguridad, un riesgo de inmigración irregular o un riesgo para la salud, planteado por una persona física que pretende entrar o ha entrado en el territorio de un Estado miembro; c) Para la verificación de la autenticidad de los documentos de

viale y de la documentación justificativa de las personas físicas y detectar los documentos no auténticos mediante la comprobación de sus características de seguridad; d) Para el examen de las solicitudes de asilo, visado y permisos de residencia y las reclamaciones asociadas con respecto a la elegibilidad de las personas físicas que solicitan un estatus.

8. Administración de justicia y procesos democráticos: Sistemas de IA destinados a ayudar a una autoridad judicial a investigar e interpretar los hechos y la ley y a aplicar la ley a un conjunto concreto de hechos.

Una vez delimitados los sistemas de alto riesgo, el Capítulo II del Título III regula los requisitos que deben reunir estos sistemas para poder implantarse. Toda la construcción se articula mediante un sistema de gestión de riesgos que toma ciertas características del régimen implantado por el RGPD, pero también aporta notas provenientes de otros ámbitos, así como muchas de estas determinaciones forman parte ya de las prácticas implantada por algunos operadores del ramo.

De tal manera que se debe realizar, por una parte, una evaluación de los riesgos derivados del sistema de IA; pero, además, se ha de implementar un sistema de gestión de riesgos para afrontar cualquier episodio que se presente. Con ser prolífica la regulación, el principal problema que plantea es sin embargo su indeterminación: se articula mediante conceptos jurídicos indeterminados, que no disponen aún de pautas claras de interpretación en el marco de esta concreta actividad (sistemas de IA), lo que produce una inevitable sensación de incertidumbre, por no decir de ansiedad; algo semejante a lo que sucedió cuando se aprobó el RGPD y se construyeron sus determinaciones bajo el principio de responsabilidad proactiva. Tal y como sucedió con esta disposición, será la práctica acumulada con el curso de los años, bajo las directrices que vayan emitiendo los supervisores, lo que permitirá aquilatar adecuadamente todo este régimen y definir más certeramente sus determinaciones¹⁵.

Para avalar el satisfactorio cumplimiento de estas exigencias se establecen una serie de obligaciones. Así, antes de la comercialización o puesta en servicio de un sistema de IA de alto riesgo se elaborará la documentación técnica de soporte, -art.11 RIA- de manera que demuestre que el sistema cumple los requisitos establecidos en el Reglamento, y proporcione a las autoridades nacionales competentes y a los organismos notificados toda la información necesaria para evaluar la conformidad del sistema de IA con dichos requisitos. Para orientar a los operadores, se incluye en el Reglamento un Anexo IV que pormenoriza la documentación técnica de que debe disponerse como soporte al sistema de IA para acreditar el cumplimiento normativo.

Además, los sistemas de IA de alto riesgo se diseñarán y desarrollarán con capacidades que permitan el registro automático de eventos ("logs") durante su

15 A modo de ejemplo, el art.9.4 RIA regula de este modo la manera de identificar las medidas de gestión de riesgos más adecuadas: "A la hora de identificar las medidas de gestión de riesgos más adecuadas, se garantizará lo siguiente: a) La eliminación o reducción de los riesgos en la medida de lo posible mediante un diseño y desarrollo adecuados; b) en su caso, la aplicación de medidas adecuadas de mitigación y control en relación con los riesgos que no puedan eliminarse; c) el suministro de información adecuada con arreglo al artículo 13, en particular en lo que respecta a los riesgos mencionados en la letra b) del apartado 2 de este artículo, y, en su caso, la formación de los usuarios. A la hora de eliminar o reducir los riesgos relacionados con el uso del sistema de IA de alto riesgo, se tendrán debidamente en cuenta los conocimientos técnicos, la experiencia, la educación y la formación que cabe esperar del usuario, así como el entorno en el que se pretende utilizar el sistema".

funcionamiento -art.12 RIA-.

Como es sabido, la calidad de los datos utilizados para la programación es uno de los grandes desafíos de los sistemas de IA. La inadecuación de los bancos de datos puede resultar en sesgos o producir disfunciones del sistema. El art.10 RIA establece garantías y requisitos específicos en relación con esta cuestión. No lejos de ella se sitúan los principios y obligaciones en materia de precisión, solidez y ciberseguridad de los sistemas de IA, regulados en el art.15 RIA.

De otro lado, una de las exigencias más reiteradas por la doctrina jurídica en relación con los sistemas de IA es la necesidad de garantizar su transparencia, de manera que los sujetos afectados por la toma de decisiones basadas en ellos puedan conocer el proceso lógico que ha conducido a adoptar la decisión y verificar así su adecuación a Derecho. La cuestión se regula en el art.13 RIA, a mi modo de ver deficientemente, pues exige que los sistemas se diseñen y desarrollen de forma que se garantice que su funcionamiento es lo suficientemente transparente como para que los usuarios puedan interpretar los resultados del sistema y utilizarlos adecuadamente, pero no se impone la necesidad de difundir el proceso lógico mediante el que se llega a tales resultados. Hay en ese precepto otros deberes de transparencia relativos a la información de que deben disponer los sistemas de IA.

Una previsión de enorme importancia es la que establece el art.14 RIA, en relación con el enfoque antropocéntrico de los sistemas de IA, estableciendo el deber de que se diseñen y desarrollen de tal manera que puedan ser supervisados eficazmente por personas físicas durante el período en que el sistema de IA esté en uso -por tanto, desde su diseño hasta su abandono, pasando por todo su ciclo de vida-, incluso con herramientas adecuadas de interfaz hombre-máquina. El precepto desglosa una serie de medidas, que son relevantes, pero a mi juicio, insuficientes. Considero que uno de los aspectos esenciales de la supervisión humana es la verificación del marco jurídico vinculante para el sistema de IA, y en especial, el respeto de los derechos fundamentales que puedan resultar comprometidos como consecuencia de su funcionamiento. La supervisión humana es esencial para lograrlo. Para que se ajuste a esta finalidad, debe llevarse a cabo por especialistas: no vale cualquier supervisión humana. En este sentido, considero que la supervisión debería confiarse expresamente a equipos multidisciplinares, en el que tengan cabida tanto técnicos como juristas.

El aspecto más problemático -y menos inteligible- del Reglamento son los diferentes mecanismos o procedimientos por los que evaluar y acreditar el cumplimiento de todos estos requisitos. Se articula un sistema de componente intensamente privado, en el que es el propio sujeto obligado, así como un tercero independiente (organismos notificados), quienes soportan el peso del proceso, según los casos.

El capítulo III del Título III establece un conjunto de obligaciones horizontales para los proveedores de sistemas de IA de alto riesgo. También se imponen obligaciones a los usuarios y a otros participantes de la cadena de valor de la IA, como por ejemplo, importadores, distribuidores o representantes autorizados. No solo se impone el deber de elaborar toda la documentación técnica de soporte del sistema para acreditar el cumplimiento de los requisitos, sino que también se articula un mecanismo de evaluación de conformidad del sistema; cuando se haya demostrado que el sistema cumple los requisitos establecidos en el Capítulo II, los proveedores elaborarán una declaración UE de conformidad y colocarán en el producto el marcado CE de conformidad.

En este aspecto, cada Estado miembro designará una autoridad responsable de establecer

y aplicar los procedimientos necesarios para la evaluación, designación y notificación de los organismos de evaluación de la conformidad, así como de su seguimiento, pudiendo designar a tal efecto un organismo nacional de acreditación, pero no siendo ello estrictamente necesario. De este modo se habilitará a quienes cumplan tales requisitos como organismos notificados, quienes llevarán a cabo la evaluación de conformidad los sistemas de IA para verificar el cumplimiento de sus requisitos.

Las soluciones técnicas precisas para lograr el cumplimiento de los requisitos pueden ser proporcionadas por normas o por otras especificaciones técnicas cuando tales normas eventualmente existan -de momento no nos constan-; o bien, desarrollarse de acuerdo con los conocimientos generales de ingeniería o científicos, a discreción del proveedor del sistema de IA. Esta flexibilidad permite a los proveedores de sistemas de IA elegir la manera de satisfacer sus necesidades, teniendo en cuenta el estado de la técnica y los avances tecnológicos y científicos en este campo; pero al mismo tiempo genera altas dosis de incertidumbre, puesto que, al no tratarse de un sistema de normalización y certificación industrial, pueden existir modelos o criterios divergentes de validación del cumplimiento normativo. Existe, por otra parte, un claro riesgo de disparidad de criterios entre los diferentes supervisores nacionales, que pueden establecer protocolos distintos de verificación y cumplimiento en cada Estado miembro, arruinando la pretendida uniformidad regulatoria que el Reglamento aspira a lograr. Sería necesario articular un mecanismo efectivo de unificación de estos criterios y protocolos a nivel europeo.

La escala normativa en los procesos de evaluación de conformidad está compuesta por los siguientes estratos -arts.40 ss. RIA-:

- 1) Cuando existan normas armonizadas a nivel europeo (como las reglamentaciones de seguridad de los productos), la conformidad con ellas presume el cumplimiento de los requisitos del Capítulo II en la medida que dichas normas cubran esos requisitos.
- 2) Cuando no existan normas armonizadas o la Comisión considere que son insuficientes, o que es necesario abordar problemas específicos de seguridad o de derechos fundamentales, la Comisión podrá adoptar, mediante actos de ejecución, especificaciones comunes; los sistemas de IA de alto riesgo que sean conformes con las especificaciones comunes se presumirán conformes con los requisitos del Capítulo 2.
- 3) En los casos más sensibles del Anexo III (sistemas de alto riesgo), la verificación de conformidad se realizará mediante un control externo, realizado por un organismo notificado, y cuyo alcance se encuentra pormenorizado en el Anexo VII. Este control se acreditará mediante un certificado de conformidad.
- 4) En el resto de los casos -salvo alguna excepción puntual-, se seguirá un procedimiento de evaluación de conformidad basado en un control puramente interno (autocontrol), de acuerdo con lo especificado en el Anexo VI.

Para sintetizar el alcance de todo esto, la memoria de acompañamiento de la propuesta de RIA afirma que "una evaluación exhaustiva de la conformidad ex-ante mediante controles internos, combinada con una fuerte aplicación ex-post, podría ser una solución eficaz y razonable para esos sistemas, dada la fase inicial de la intervención reguladora y el hecho de que el sector de la IA es muy innovador y los conocimientos técnicos para la auditoría sólo se están acumulando ahora. Una evaluación a través de controles internos para los sistemas de IA "autéonomos" de alto riesgo requeriría un cumplimiento total, efectivo y debidamente documentado ex ante de todos los requisitos de la normativa

y el cumplimiento de sólidos sistemas de gestión de la calidad y el riesgo, así como un seguimiento posterior a la comercialización. Una vez que el proveedor haya realizado la evaluación de conformidad pertinente, deberá registrar esos sistemas autónomos de IA de alto riesgo en una base de datos de la UE que será gestionada por la Comisión para aumentar la transparencia y la supervisión pública y reforzar la supervisión a posteriori por parte de las autoridades competentes. En cambio, por razones de coherencia con la legislación vigente sobre la seguridad de los productos, las evaluaciones de conformidad de los sistemas de IA que sean componentes de seguridad de los productos seguirán un sistema con procedimientos de evaluación de la conformidad de terceros ya establecidos en la legislación sectorial pertinente sobre la seguridad de los productos”.

Naturalmente, todo esto no saldrá gratis. La memoria de acompañamiento incluye un cálculo de costes en los sistemas de alto riesgo, del siguiente tenor: “El cumplimiento de estos requisitos supondría unos costes de entre 6.000 y 7.000 euros para el suministro de un sistema medio de IA de alto riesgo, alcanzando aproximadamente un total de 170.000 euros para 2025. Para los usuarios de IA, también existiría un coste anual por el tiempo dedicado a garantizar la supervisión humana cuando ésta sea apropiada, dependiendo del caso de uso. Se ha calculado que estos costes ascienden aproximadamente a entre 5.000 y 8.000 euros al año. Los costes de verificación podrían ascender a otros 3.000 a 7.500 euros para proveedores de IA de alto riesgo”. Es obvio que la carga derivada de esta regulación determinará una desventaja competitiva para los desarrollos europeos de sistemas de IA.

3.4. Resto de sistemas

Para el resto de sistemas de IA, que aparentemente no serían problemáticos, la solución prevista por el Reglamento es la autorregulación, esto es, la aprobación de códigos de conducta propios e internos por parte de los operadores de sistemas de IA, que pueden asumir voluntariamente el cumplimiento de requisitos y exigencias establecidas en el Reglamento para los sistemas de alto riesgo, o bien idear otras garantías de su propia cosecha. También pueden incluir compromisos voluntarios relacionados, por ejemplo, con la sostenibilidad medioambiental, la accesibilidad para las personas con discapacidad, la participación de las partes interesadas en el diseño y el desarrollo de los sistemas de IA y la diversidad de los equipos de desarrollo.

En este sentido, el Título IX del Reglamento regula la creación de códigos de conducta, lo que pretende mover a los proveedores de sistemas de IA que no sean de alto riesgo a que apliquen voluntariamente los requisitos obligatorios para los sistemas de alto riesgo, creando y aplicando por sí mismos dichos códigos.

3.5. Otras determinaciones relevantes

Mencionaremos, para finalizar, algunas otras cuestiones relevantes establecidas por el Reglamento, para lo que seguimos sustancialmente la síntesis contenida en su memoria de acompañamiento.

El Título VI establece los sistemas de gobernanza a nivel de la Unión y nacional. A nivel de la Unión, la propuesta establece una Junta Europea de Inteligencia Artificial, compuesta por representantes de los Estados miembros y de la Comisión. Con esta Junta se pretende facilitar una aplicación fluida, eficaz y armonizada del Reglamento.

A nivel nacional, los Estados miembros deberán designar una o varias autoridades nacionales competentes y, entre ellas, la autoridad nacional de control, con el fin de supervisar la aplicación y ejecución del Reglamento. El Supervisor Europeo de Protección

de Datos actuará como autoridad competente para la supervisión de las instituciones, agencias y organismos de la Unión cuando entren en el ámbito de aplicación de este reglamento.

El título VIII establece las obligaciones de control e información para los proveedores de sistemas de IA en lo que respecta a la vigilancia y la información posterior a la comercialización y a la investigación de los incidentes relacionados con la IA y su mal funcionamiento. Las autoridades de vigilancia del mercado también controlarían el mercado e investigarían el cumplimiento de las obligaciones y requisitos para todos los sistemas de IA de alto riesgo ya comercializados. Este control a posteriori debe garantizar que una vez que la IA sistema ha sido puesto en el mercado, las autoridades públicas tienen los poderes y recursos necesarios para intervenir en caso de que los sistemas de IA generen riesgos inesperados que justifiquen una acción rápida. También supervisarán el cumplimiento por parte de los operadores de las obligaciones que les impone el Reglamento. Los Estados miembros podrán designar (y aprovechar la experiencia de) las autoridades sectoriales existentes, a las que se les confiarían también las competencias para supervisar y hacer cumplir las disposiciones del Reglamento. Las autoridades de supervisión y ejecución también tienen la facultad de solicitar y acceder a cualquier documentación mantenida a raíz del Reglamento y, cuando sea necesario, solicitar a las autoridades de vigilancia del mercado que organicen pruebas del sistema de IA de alto riesgo a través de medios técnicos.

En el mismo Título VIII se impone además a los proveedores de IA la obligación de informar a las autoridades nacionales competentes sobre los incidentes graves o el mal funcionamiento que constituyan una infracción de las obligaciones en materia de derechos fundamentales tan pronto como tengan conocimiento de ellos, así como sobre cualquier retirada de los sistemas de IA del mercado. A raíz de estas notificaciones, las autoridades nacionales competentes investigarán los incidentes o el mal funcionamiento, recogerán toda la información necesaria y la transmitirán a la Comisión, quien complementará esta información sobre los incidentes con un análisis exhaustivo del mercado global de IA.

En orden a facilitar la labor de control de la Comisión y de las autoridades nacionales, el Título VII regula la creación de una base de datos a escala de la UE para los sistemas de IA autónomos de alto riesgo con implicaciones principalmente en los derechos fundamentales. La base de datos, de acceso público, será gestionada por la Comisión. Los proveedores de sistemas de IA estarán obligados a registrarlos antes de comercializarlos o ponerlos en servicio de otra manera. También permitirá verificar si un sistema de IA de alto riesgo cumple los requisitos establecidos en el Reglamento y ejercer mayor supervisión sobre aquellos sistemas de IA que supongan un alto riesgo para los derechos fundamentales.

El Título X hace hincapié en la obligación de todas las partes de respetar la confidencialidad de la información y los datos y establece normas para el intercambio de la información obtenida durante la aplicación del Reglamento, previsión que pretende proteger los secretos industriales.

El mismo Título también incluye medidas para garantizar la aplicación efectiva del reglamento mediante sanciones eficaces, proporcionadas y disuasorias en caso de infracción de las disposiciones. Su cuantía puede llegar a ser muy elevada: hasta 30 millones de euros o el 6% del volumen anual total de negocio, por ejemplo, cuando se implanten sistemas de IA prohibidos.

El Título XI faculta a la Comisión para adoptar, en su caso, actos de ejecución que

garanticen la aplicación uniforme del reglamento o actos delegados que actualicen o complementen las listas de los anexos I a VII. Es una competencia muy relevante, cuya pervivencia en el texto definitivo del Reglamento es dudosa, a la vista de los antecedentes.

Para concluir, el Título XII contiene la obligación de la Comisión de evaluar periódicamente la necesidad de actualizar el anexo III y de elaborar informes periódicos sobre la evaluación y revisión del reglamento.

4. Complementariedad entre el enfoque europeo sobre IA y otros ámbitos: La estrategia europea de datos y blockchain

Para completar la panorámica del enfoque europeo sobre IA, no puede desconocerse su íntima conexión con estas dos líneas de acción de la Unión Europea.

Por lo que se refiere a la estrategia europea de datos, el fomento de la innovación impulsada por la IA está estrechamente vinculado con la propuesta de Reglamento sobre la gobernanza europea de datos (Ley de Gobernanza de Datos)¹⁶, la Directiva de Datos Abiertos¹⁷ y otras iniciativas en el marco de la estrategia de la UE para los datos¹⁸. Mediante la progresiva implementación de estas previsiones se establecerán mecanismos y servicios de confianza para la reutilización, el intercambio y la puesta en común de datos que son esenciales para el desarrollo de modelos de IA impulsados por datos de alta calidad.

Y en cuanto a blockchain, es significativo que la Comisión Europea y el Banco Europeo de Inversiones hayan emitido muy recientemente un informe sobre "Inteligencia artificial, blockchain y el futuro de Europa: cómo las tecnologías disruptivas crean oportunidades para una economía verde y digital"¹⁹, en el que se promueve la inversión en estas tecnologías disruptivas como palanca para el desarrollo.

5. Valoración General

La primera conclusión que debemos formular es que no cabe dudar del carácter estratégico y prioritario que la UE concede al desarrollo de la IA, y de su preocupación por establecer un marco normativo en la materia que concuerde con los valores fundamentales y fundamentales de la Unión.

En relación con sus aplicaciones a la IA, el enfoque europeo supone indudablemente un hándicap al desarrollo de soluciones y un coste de mercado añadido. Imponer limitaciones reduce las utilidades desarrolladas, y exigir requisitos determina costes de cumplimiento. Los sistemas de IA asiáticos y norteamericanos, al no encontrarse limitados por estas circunstancias, pueden implementar sistemas de IA que aprendan más rápidamente y a menor coste, lo cual representa una ventaja competitiva.

Pero es una carga que Europa ha estado siempre dispuesta a pagar, no solo en materia de IA, sino en otros muchos ámbitos. Representa una línea de pensamiento profundamente

16 Comunicación de la Comisión Europea COM (2020)767, de 25 de noviembre.

17 Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio, relativa a los datos abiertos y la reutilización de la información del sector público.

18 Comunicación de la Comisión COM (2020)66, de 19 de febrero. No por casualidad, esta comunicación se aprobó el mismo día que el Libro blanco sobre inteligencia artificial.

19 En su versión original, "Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy", European Commission and European Investment Bank, Luxemburgo, junio de 2021.

imbricada en los valores europeos y que entraña indudablemente con el humanismo cristiano, que sitúa al individuo en el centro de la escena y valora su dignidad como valor supremo del Ordenamiento jurídico: de hecho, todo el sistema constitucional en los países europeos está centrado en el respeto y protección de los derechos fundamentales de la persona frente a cualesquiera injerencias o potenciales lesiones.

Análogamente a lo que sucede, por ejemplo, con el medio ambiente o los derechos laborales. De igual forma que Europa no se plantea modificar sus políticas en estos ramos, sino antes al contrario, profundizar en ellas, a pesar de que ello represente una desventaja competitiva para las industrias europeas respecto a las del resto del mundo y haya conducido a la deslocalización de muchas fábricas.

Se debe afirmar, también, que la propuesta de Reglamento europeo de IA constituye una iniciativa valiosísima. A pesar de su extensión y de la complejidad técnica de su contenido, y a pesar también de la diversidad de intereses y sensibilidades que confluyen en esta normativa, las instituciones europeas han sido capaces de elaborar una propuesta muy madura en un tiempo sencillamente récord. Se dispone así de un significativo punto de partida, del que la regulación final no se encontrará muy alejada, lo que permite a los operadores ir ajustando su actividad a los postulados de la propuesta, evitando incurrir en gastos inútiles por promover desarrollos de sistemas de IA que finalmente resulten incompatibles con el marco regulatorio.

Con ser prolífa la regulación, el principal problema que plantea es sin embargo su indeterminación: se articula mediante conceptos jurídicos indeterminados, que no disponen aún de pautas claras de interpretación en el marco de esta concreta actividad (sistemas de IA), lo que produce una inevitable sensación de incertezza, por no decir de ansiedad; algo semejante a lo que sucedió cuando se aprobó el RGPD y se construyeron sus determinaciones bajo el principio de responsabilidad proactiva. Tal y como sucedió con esta disposición, será la práctica acumulada con el curso de los años, bajo las directrices que vayan emitiendo los supervisores, lo que permitirá aquilatar adecuadamente todo este régimen y definir más certeramente sus determinaciones.

Ahora resta una intensa etapa de análisis de las propuestas y comentarios recibidos durante la fase de consulta pública, así como un proceso de negociación a varias bandas: de la Comisión con otras instancias europeas copartícipes del procedimiento normativo, como el Consejo y el Parlamento Europeo; pero también, con los Estados miembros, que pueden manifestar sensibilidades diferentes, en especial respecto de los temas relativos a la seguridad ciudadana. El plazo habitual de tramitación en la UE de una iniciativa normativa de esta envergadura y naturaleza es de tres años, pero en este caso no sería raro que dicho plazo se acorte: no solo por el carácter estratégico que tiene de suyo la aprobación de la norma, sino además porque se espera que muchos de los recursos movilizados mediante los Fondos Next Generation UE (unos 700.000 millones de euros) se destinen al desarrollo digital, y en ese escenario es crucial disponer cuanto antes del marco regulatorio de la IA para que las inversiones que se realicen sean sostenibles en el tiempo.

Para concluir, el RIA establece el plazo de un año de *vacatio legis* para su entrada en vigor. Se diría que todo este horizonte resulta entonces muy lejano. Nada menos cierto: la mera difusión de la propuesta de RIA ya ha supuesto movimientos en el sector, orientados a procurar el cumplimiento de las exigencias del reglamento, en la medida de lo posible, en los desarrollos de sistemas de IA que emprendan a partir de ahora.

6. Referencias bibliográficas

- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (s/f). Elaboración de una Recomendación sobre la Ética de la Inteligencia Artificial. <https://es.unesco.org/artificial-intelligence/ethics>
- Gamero, E. (2021). Compliance (o cumplimiento normativo) de desarrollos de inteligencia artificial para la toma de decisiones administrativas. Diario La Ley, Nº 50, Sección Ciberderecho. <https://diariolaleylaleynext.es>
- Gamero, E. (2021). Necesidad de motivación e invalidez de los actos administrativos sustentados en inteligencia artificial o en algoritmos. Almacén de Derecho. <https://almacendedederecho.org>
- Comisión Europea (2020). Libro Blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_es.pdf
- Comisión Europea. (2020). Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la Gobernanza Europea de Datos (Ley de Gobernanza de Datos).
- Comisión Europea y el Banco Europeo de Inversiones. (2021). Artificial intelligence, blockchain and the future of Europe: How disruptive technologies create opportunities for a green and digital economy. https://www.eib.org/attachments/thematic/artificial_intelligence_blockchain_and_the_future_of_europe_report_en.pdf
- Diario Oficial de la Unión Europea. (2019). DIRECTIVA (UE) 2019/1024 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 20 de junio de 2019 relativa a los datos abiertos y la reutilización de la información del sector público (versión refundida).
- Comisión Europea. (2021). Propuesta de Reglamento por el que se establecen normas armonizadas de inteligencia artificial (Ley de Inteligencia Artificial) y que modifica determinados actos legislativos de la Unión Europea. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF



LA ARTICULACIÓN JURÍDICA DEL ENTORNO DIGITAL: INSUFICIENCIAS Y SOLUCIONES EN LA DELIMITACIÓN DE LOS SECTORES DE REFERENCIA ANTE EL DESAFÍO DE LOS SERVICIOS OVER THE TOP (OTT)

THE LEGAL ARTICULATION OF THE DIGITAL ENVIRONMENT: INSUFFICIENCIES AND SOLUTIONS IN THE DELIMITATION OF THE REFERENCE SECTORS TO THE CHALLENGE OF OVER THE TOP (OTT) SERVICES

JOSÉ VIDA FERNÁNDEZ¹

RESUMEN

La tradicional delimitación del entorno digital en sectores de referencia como son las telecomunicaciones (comunicaciones electrónicas), el audiovisual y los servicios de la sociedad de la información (servicios TIC) se ha visto afectada por la aparición de innumerables servicios prestados a través de Internet que ofrecen funcionalidades propias de estos servicios pero que no encajan en su definición, por lo que escapan de la aplicación de su régimen jurídico. Estos servicios over the top (OTT) están alterando el equilibrio de los distintos sectores, al competir con los demás operadores sin someterse a su mismo régimen jurídico, evadiendo obligaciones necesarias para alcanzar objetivos de interés general. Frente a este desafío, la Unión Europea ha optado por ampliar el ámbito de aplicación para incluirlos en el régimen jurídico correspondiente, pero sometiéndolos a unas obligaciones específicas y distintas de las propias de los operadores tradicionales para facilitar su desarrollo a la vez que se garantizan objetivos de interés público.

ABSTRACT

The traditional delimitation of the digital environment in reference sectors such as telecommunications (electronic communications), audiovisual and information society services (ICT services) has been affected by the appearance of innumerable services provided through the Internet that offer features typical of these services but that do not fit into their definition, so they escape the application of their legal regime. These over the top (OTT) services are altering the balance of the different sectors, by competing with other operators without submitting to the same legal regime, avoiding obligations necessary to achieve objectives of general interest. Faced with this challenge, the European Union has chosen to expand the scope of application to include them in the corresponding legal regime, but subjecting them to specific and different obligations from those of traditional operators to facilitate their development while pursuing objectives of public interest.

1 Profesor Titular de Derecho Administrativo de la Universidad Carlos III de Madrid, Subdirector del Máster en Derecho de las Telecomunicaciones, Protección de Datos, Audiovisual y Sociedad de la Información y miembro del Instituto Pascual Madoz de Territorio, Urbanismo y Medio Ambiente. Licenciado en Derecho con premio extraordinario por la Universidad de Granada y Doctor Europeo por la Universidad de Bolonia (Italia). Ha realizado numerosas estancias de investigación en centros de reconocido prestigio como la Scuola di Specializzazione in Studi sull'Amministrazione Pubblica, SPISA (Bolonia); Institute of Advanced Studies (Indiana University); o Boalt Hall (Berkeley Law, UCLA). Contacto: jose.vida@uc3m.es

El presente trabajo se ha realizado como parte del proyecto de investigación "El impacto de la inteligencia artificial en los servicios públicos: Un análisis jurídico de su alcance y consecuencias en la asistencia sanitaria" (PGC2018-098243-B-I00) que se desarrolla bajo la dirección del profesor José Vida Fernández dentro de la convocatoria 2018 de «Proyectos de I+D de Generación de Conocimiento» del Programa Estatal de Generación de Conocimiento y Fortalecimiento Científico y Tecnológico del Sistema de I+D+i del Ministerio de Ciencia e Innovación.

PALABRA CLAVE

Regulación | Sector digital | Servicios de telecomunicaciones | Servicios audiovisuales | Servicios de sociedad de la información | Servicios OTT.

KEYWORDS

Regulation | Digital sector | Telecommunications services | Audiovisual services | Information society services | OTT services.

CONTENIDO

1. Introducción: la articulación jurídica de los sectores que constituyen el entorno digital; **2.** La tradicional delimitación de los sectores que integran el entorno digital y caracterización de su respectivo régimen jurídico; **2.1.** La delimitación originaria del sector de las telecomunicaciones: El régimen jurídico de los servicios de comunicaciones electrónicas; **2.2.** La delimitación originaria del sector audiovisual: El régimen jurídico de los servicios de comunicación audiovisual; **2.3.** La delimitación originaria de los servicios de sociedad de la información: El régimen jurídico de los servicios de la sociedad de la información; **3.** Las insuficiencias en la delimitación de los sectores del entorno digital ante el empuje de los servicios digitales Over the Top (OTTs); **3.1.** El surgimiento de los servicios Over the Top (OTT) y su incidencia en la tradicional articulación jurídica de los sectores económicos; **3.2.** La respuesta jurisprudencial ante las insuficiencias en la delimitación de los sectores económicos; **4.** La nueva delimitación de los sectores del entorno digital: la ampliación de las definiciones y la adaptación de los regímenes jurídicos sectoriales; **4.1.** La nueva definición de los servicios de comunicación electrónica y la adaptación de su régimen jurídico; **4.2.** La nueva definición de los servicios de comunicación audiovisual y la adaptación de su régimen jurídico; **4.3.** La nueva definición de los servicios de intermediación y de las plataformas digitales y su nuevo de su régimen jurídico; **5.** Conclusión; **6.** Bibliografía. **7.** Anexo de normativa y jurisprudencia.

SOBRE EL ARTÍCULO

El presente artículo fue recibido por la Comisión de Publicaciones el 27 de septiembre de 2021 y aprobado para su publicación el 13 de octubre de 2021.

1. INTRODUCCIÓN: LA ARTICULACIÓN JURÍDICA DE LOS SECTORES QUE CONSTITUYEN EL ENTORNO DIGITAL

El proceso de transformación tecnológica alcanza a todas las dimensiones de nuestra realidad, la cual es ya, eminentemente, digital. La mayoría de nuestras actividades, ya sean profesionales o personales, se desarrollan en entornos digitales que se nos manifiestan de una manera continua y homogénea. Así, alguien puede asistir a una reunión online, preparar, enviar un informe y descansar consultando sus redes sociales mientras disfruta de su serie favorita. Todo ello lo hace de manera natural a través de distintas redes, dispositivos, servicios y aplicaciones dentro de una misma realidad digital.

Sin embargo, este entorno digital dista mucho de ser continuo y homogéneo ya que se compone de distintos elementos que lo hacen posible. Encontramos, entonces, redes y servicios que permiten la comunicación electrónica (ya sea fija o móvil), con el consiguiente envío y recepción de datos a través de distintos dispositivos e interfaces (computadora, tablet, smartphone, smartTV, vehículos, alarmas, etc.) que se conectan para prestar un creciente y variado repertorio de servicios independientes (envío de un mensaje de correo electrónico, videollamadas, compras en plataformas, contenidos audiovisuales, información en cloud o un vehículo autónomo).

Desde un punto de vista económico-empresarial, el sector digital se encuentra articulado en

distintos subsectores entre los que se pueden distinguir los servicios de telecomunicaciones (o de comunicaciones electrónicas) que prestan conectividad, los servicios digitales (servicios de la sociedad de la información o servicios TICs), que ofrecen funcionalidades a partir de esa conexión a distancia, y los servicios audiovisuales (o de comunicación audiovisual) que facilitan contenidos. Los usuarios pueden apreciar esta fragmentación a partir de las distintas facturas que tienen que abonar para poder disfrutar de ese entorno digital, ya que tendrá un contrato con un operador de telecomunicaciones, otros contratos con distintas plataformas de televisión online o de video bajo demanda y, por último, otros contratos con su plataforma de comercio electrónico, su proveedor de servicios cloud, etc., aunque cada vez se ofrecen más servicios empaquetados.

Esta estructura coincide con la articulación jurídica a la que se somete este entorno digital que, en ningún país, se regula de forma homogénea bajo una única norma sino a través de distintos subsistemas conformados por normas específicas que ordenan cada sector conforme a un fundamento y a una lógica propia. De este modo, nada o poco tiene que ver el régimen jurídico de las telecomunicaciones con el de los servicios audiovisuales o de los servicios de la sociedad de la información, ya que presentan niveles de intervención de muy diversa intensidad, por lo que no resulta indiferente ser clasificado como operadores de uno u otro sector.

La definición de estos servicios y el consiguiente sometimiento a uno u otro régimen jurídico han evolucionado en las últimas décadas como consecuencia de la convergencia de las telecomunicaciones, el audiovisual y las tecnologías de la información que, sin embargo, no han sido regulados en la configuración de un marco jurídico único. Por el contrario, la tradicional delimitación de estos sectores se ha visto afectada por el empuje de nuevos servicios prestados por Internet que ofrecen funcionalidades propias de estos servicios pero que no encajan en su definición, por lo que quedan al margen de su régimen jurídico.

Estos servicios *over the top* (OTT) que operan por encima de la normativa de los distintos sectores están alterando su equilibrio al competir con los demás operadores sin someterse a su mismo régimen jurídico, comprometiendo asimismo la eficacia de esta normativa y los objetivos de interés público general que con ella se persiguen. La creciente relevancia de estos servicios OTT genera unas importantes dificultades en la articulación jurídica de estos sectores que conforman el entorno digital en tanto desbordan los regímenes jurídicos de referencia, por lo que se plantea si someterlos a la misma regulación que a los operadores tradicionales de dichos sectores o mantenerlos al margen para que conserven su impulso creativo e innovador.

Se trata de un problema que carece de una solución definitiva, pero resulta imprescindible actuar poniendo en marcha soluciones como la adoptada en la Unión Europea, que ha optado por ampliar el ámbito de aplicación del régimen jurídico de los distintos sectores, incluyéndolos así en un mismo régimen jurídico, pero sometiéndolos a unas obligaciones específicas y distintas de las propias de los operadores tradicionales para facilitar su desarrollo a la vez que se garantizan los objetivos de interés público general.

2. LA TRADICIONAL DELIMITACIÓN DE LOS SECTORES QUE INTEGRAN EL ENTORNO DIGITAL Y CARACTERIZACIÓN DE SU RESPECTIVO RÉGIMEN JURÍDICO

2.1. La delimitación originaria del sector de las telecomunicaciones: El régimen jurídico de los servicios de comunicaciones electrónicas

Desde el inicio del proceso de liberalización de las telecomunicaciones a finales de

la década de los años ochenta del siglo pasado, se planteó en el ámbito europeo el problema de la delimitación de este sector como consecuencia de las innovaciones tecnológicas que, precisamente justificaban la apertura de los monopolios naciones y la consecución de un mercado común de telecomunicaciones. En este sentido, en el Libro Verde de la Liberalización de las Telecomunicaciones de 1987, la Comisión apuntaba de forma tan precoz como acertada a un problema que iría en aumento en las décadas siguientes, como era la delimitación de las telecomunicaciones y su distinción de otros sectores conexos que, hasta ese momento, habían estado perfectamente delimitados (Comisión Europea, 1987, p. 9).

La propia Comisión volvió a ocuparse sobre la cuestión diez años después en el Libro Verde sobre la Convergencia de 1997², en el que señaló lo imprescindible de contar con un marco reglamentario adecuado a este nuevo fenómeno que venía a transformar los servicios tradicionales ofrecidos por las telecomunicaciones y los medios de comunicación, en cuanto a su gama y diversidad. En este documento se analizaban los retos de la convergencia a nivel tecnológico, en tanto la digitalización estaba permitiendo que los servicios de comunicaciones (con independencia de que utilizasen imágenes, sonidos, datos o voz) se pudiesen ofrecer a través de distintas redes, por lo que ya no era posible seguir identificando ciertas redes con servicios concretos. De hecho, la Comisión hacía referencia específicamente al problema de las definiciones legales y la incertidumbre con respecto al régimen jurídico aplicable a una determinada actividad, para lo que propuso adaptar las definiciones existentes de manera que se tuvieran en cuenta los avances y tendencias tecnológicas.

Este planteamiento es el que justifica que, con ocasión de la revisión del marco jurídico del sector a través de un conjunto de Directivas denominado Paquete Telecom de 2002 se desplazase el término “telecomunicaciones” por el de “comunicaciones electrónicas”³. En todo caso, debe tenerse en cuenta que no son conceptos sustitutivos, sino que las telecomunicaciones abarcan un ámbito más amplio en el que se encajan las comunicaciones electrónicas que constituyen su elemento esencial⁴, por lo que el término telecomunicaciones sigue empleándose tanto a nivel europeo como interno de

2 Libro Verde sobre la convergencia de los sectores de telecomunicaciones, medios de comunicación y tecnologías de la información y sobre sus consecuencias para la reglamentación - En la perspectiva de la sociedad de la información [COM (97) 623 final, de 3 de diciembre de 1997].

3 Se justifica este cambio en los considerandos 6 y 7 de la Directiva 2002/77/CE de la Comisión, de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas, precisamente por la evolución tecnológica registrada en el sector de las telecomunicaciones y como consecuencia del fenómeno de la convergencia de los sectores de las telecomunicaciones, los medios de comunicación y las tecnologías de la información. El Paquete Telecom estaba encabezado por la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, denominada “Directiva marco”, a la que acompañaban las llamadas “Directivas específicas” (Directiva 2002/20/CE de autorización, Directiva 2002/19/CE de acceso, Directiva 2002/22/CE de servicio universal y Directiva 97/66/CE de los datos personales e intimidad en las telecomunicaciones).

4 En efecto, las telecomunicaciones incluyen otras cuestiones que van más allá de la simple transmisión de señales, como las relacionadas con el despliegue de las redes, su seguridad o la interoperabilidad de los terminales que se rigen en normas específicas como la Directiva 2014/53/UE (Directiva RED) de armonización de equipos radioeléctricos terminales; el Reglamento (UE) 2015/2120 de neutralidad de la red; o la Directiva 2014/61/UE (BBcost) de despliegue de las redes de comunicaciones electrónicas de alta velocidad en infraestructuras susceptibles de alojarlas.

los Estados miembros, como es el caso de España donde la norma de referencia en el sector es la Ley General de Telecomunicaciones⁵.

Bajo la denominación de comunicaciones electrónicas se agrupan todas las redes y los servicios necesarios para la comunicación a distancia, independientemente de la red utilizada (cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos -los que incluía redes fijas como el cable o inalámbricas como el satélite-) y del tipo de servicio (desde la telefonía vocal a la transmisión de señales de radio y televisión), que quedaban sometidos a un marco regulador común. Ahora bien, se debe aclarar que la "regulación convergente" que se prodiga bajo las comunicaciones electrónica no pretendía unificar el régimen de los sectores implicados (telecomunicaciones, audiovisual, servicios de la sociedad de la información), sino que la convergencia se limita a los "medios de transmisión" que soportan la actividad en estos sectores. Es decir, que todo lo relativo a las redes y servicios para la transmisión de señales estuviese bajo el mismo régimen jurídico aplicable a las comunicaciones electrónicas contenido en el Paquete Telecom, independientemente del tipo de contenidos transmitidos, ya fuesen servicios audiovisuales o de la sociedad de la información.

De este modo, las comunicaciones electrónicas quedaron delimitadas en función de los elementos que las integran, a saber, las redes, los servicios y los recursos asociados, tal y como fueron definidos en la Directiva Marco⁶. Lo más relevante aquí es la definición de los servicios de comunicaciones electrónicas que son aquellos consistentes en el transporte de señales a través de redes de comunicaciones electrónicas. De esa manera, se trata de incluir todos los servicios de transmisión independientemente de sus características (ya sean servicios mayoristas como la interconexión fija y móvil, el alquiler circuitos o la transmisión datos, o servicios finales para los usuarios como la telefonía fija y móvil, la banda ancha fija y móvil, etc.) unificándose así bajo una misma normativa todos los servicios de telecomunicaciones que, durante el proceso de liberalización habían

- 5 En el caso de España, se ha mantenido este planteamiento en las sucesivas Leyes Generales de Telecomunicaciones de los años 1998, 2003 y 2014 y se mantiene en el anteproyecto que actualmente se encuentra en tramitación. El hecho de que en España se legisle sobre las telecomunicaciones y no sobre las comunicaciones electrónicas tiene que ver con el reparto de competencias a nivel territorial, ya que el artículo 149.1.21º CE atribuye al Estado competencia exclusiva sobre las telecomunicaciones, por lo que el legislador estatal ha optado por dictar un único cuerpo normativo (la LGTel) que incorpora, además del régimen de las redes y servicios de comunicaciones electrónicas (con aspectos como la condición de operador, los derechos y obligaciones de operadores y usuarios, o el servicio universal), otros aspectos como es el régimen de la instalación de equipos y sistemas, la interceptación legal de las telecomunicaciones, la conservación de datos, o la evaluación de conformidad de equipos radioeléctricos, transponiéndose así en un mismo texto legal una normativa europea dispersa.
- 6 Las redes de comunicaciones electrónicas se definían de forma omnicomprensiva incluyendo todos los sistemas de transmisión (red de par cobre, fibra óptica, cable coaxial, las redes telefonía móvil, etc.), independientemente de la tecnología empleada (sean cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos) y de la utilización que se les dé (tendido eléctrico, redes para la radio, televisión y cable) y de la información que transporten (art. 2 a) Directiva Marco y Anexo LGTel Def. 3). Los servicios de comunicaciones electrónicas se definían como aquellos prestados, por lo general a cambio de una remuneración que consisten, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas (art. 2 a) Directiva Marco y Anexo LGTel Def. 35). Por último, los recursos asociados son definidos como las infraestructuras físicas, los sistemas, dispositivos, los servicios asociados u otros recursos o elementos asociados con una red de comunicaciones electrónicas o con un servicio de comunicaciones electrónicas que permitan o apoyen el suministro de servicios a través de dicha red o servicio o tengan potencial para ello (art. 2 e) de la Directiva Marco y del Anexo LGTel Def. 39).

estado sometidos a regímenes dispares, incluidos los servicios de transmisión en las redes utilizadas para la radiodifusión.

Como se ha adelantado, la convergencia afecta solo a la transmisión y no a los servicios que la utilizan, ya sean para ofrecer contenidos (servicios audiovisuales) o funcionalidades (servicios de sociedad de la información), por lo que quedan excluidos del régimen de las comunicaciones electrónicas los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos, en tanto se entiende que se trata de servicios de comunicación audiovisual. Asimismo, quedan excluidos los servicios de la sociedad de la información que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas.

La separación entre la regulación de la transmisión (comunicaciones electrónicas) y la regulación de los contenidos y servicios transmitidos (audiovisual y servicios de la sociedad de la información) derivó en la construcción de regímenes jurídicos estancos, basados en unas definiciones que se han mantenido inalteradas durante casi dos décadas hasta las nuevas definiciones que, en el caso de los servicios de comunicaciones electrónicas, ha introducido el Código Europeo de las Comunicaciones Electrónicas aprobado por la Directiva (UE) 2018/1972⁷.

A partir de estas definiciones, se establece un régimen jurídico completo y detallado para las comunicaciones electrónicas que, en España, se contiene por ahora en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones⁸. Esta se caracteriza por la intensidad de la intervención pública desplegada en tanto se califican como servicios de interés general que se presta en régimen de libre competencia. Por lo tanto, aunque estemos ante un sector plenamente liberalizado, al tratarse de unos servicios en red tendentes al monopolio natural y que no responden a criterios de equidad, quedan sometidos a un importante bloque de medidas para garantizar el funcionamiento competitivo del mercado y la consecución de los objetivos de servicio público, convirtiéndose así en un sector fuertemente regulado.

2.2. La delimitación originaria del sector audiovisual: El régimen jurídico de los servicios de comunicación audiovisual

Por lo que respecta a los servicios audiovisuales, estos contaban con una larga trayectoria de intervención a nivel europeo en desarrollo de la política en sector audiovisual, conforme a la que se habían adoptado medidas que inicialmente alcanzaban a los medios de transmisión (redes y servicios) centrándose en el concepto de "actividad de radiodifusión televisiva", que era la referencia sobre la que se disponía su normativa en la Directiva 89/552/CEE (de televisión sin fronteras)⁹.

Tradicionalmente, los servicios audiovisuales eran fácilmente identificables ya que se caracterizaban por la tecnología de transmisión en un solo sentido de forma simultánea

7 Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

8 Que será sustituida en breve por una nueva Ley General de Telecomunicaciones que transpondrá el contenido del Código Europeo de Comunicaciones Electrónicas.

9 En la Directiva 89/552/CEE del Consejo, de 3 de octubre de 1989, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados Miembros relativas al ejercicio de actividades de radiodifusión televisiva, se definía la radiodifusión televisiva como la emisión primaria, con o sin hilo, por tierra o por satélite, codificada o no, de programas televisados destinados al público (art. 1 a).

a una multiplicidad de usuarios (punto-multipunto), que era la forma de transmisión a través de las redes de radiodifusión analógica, tanto de la televisión como de la radio. Por esta razón, se identificaban coloquialmente como "medios de difusión", ya que permitían la comunicación de contenidos a gran escala. Esto los convertía en medios de comunicación de masas y justificaba que estuvieran sometidos a un régimen jurídico específico y distinto del régimen de las telecomunicaciones, ya que estas permitían una comunicación interactiva punto a punto, que era como inicialmente se caracterizaban los servicios tradicionales como la telefonía vocal o el telégrafo.

La convergencia derivada del avance tecnológico llevó a que los contenidos audiovisuales pudiesen transmitirse a través de distintos tipos de redes y que esas mismas redes pudiesen transmitir cualquier tipo de contenidos, haciendo que fuese cada vez más difícil la distinción de los servicios audiovisuales de los servicios de comunicaciones electrónicas y de los servicios de la sociedad de la información. Esto es lo que condujo a la integración de las redes de radiodifusión sonora y televisiva, en cuanto sistemas de transmisión, en las redes de comunicaciones electrónicas, perdiendo así su caracterización como un servicio de telecomunicaciones singular al que habían estado sujetas durante el proceso de liberalización. De esa manera, quedan sujetas al régimen común de las comunicaciones electrónicas.

De forma paralela a lo que había ocurrido en el ámbito de las comunicaciones electrónicas, se fue modificando la definición de la actividad de radiodifusión televisiva incorporando a su contenido otras formas de difusión más allá de la televisión analógica, como la digital, la emisión en directo en tiempo real por Internet (*live streaming*), la difusión web (*webcasting*) y el vídeo casi bajo demanda, hasta que, finalmente, se incorporaron los servicios audiovisuales a petición bajo una nueva definición de los "servicios de comunicación audiovisual" que introdujo la Directiva 2007/65/CE de modificación de la Directiva de televisión sin fronteras.

A partir de este cambio, los servicios de comunicación audiovisual pasan a definirse como aquellos cuya responsabilidad editorial corresponde a un prestador del servicio de comunicación y cuya principal finalidad es proporcionar programas, con objeto de informar, entretenér o educar al público en general, a través de redes de comunicaciones electrónicas, independientemente de si es o no bajo demanda, e incluyendo comunicaciones comerciales¹⁰.

La definición de servicios de comunicación audiovisual se centra en la consideración de que estos servicios son medios de comunicación de masas, es decir, que están destinados a una parte significativa del público en general y que puedan tener un claro impacto sobre él en el ejercicio de su función de informar, entretenér y educar al público general, así como de emitir comunicaciones audiovisuales comerciales¹¹.

Por lo tanto, quedan excluidos de los servicios de comunicación audiovisual aquellos que impliquen actividades que no sean fundamentalmente económicas, ni entren en competencia con la radiodifusión televisiva, ni los servicios cuyo principal objeto no sea

10 Artículo 1 a) de la Directiva 89/552/CEE, modificada por la Directiva 2007/65/CE. Esta es la definición de los servicios de comunicación audiovisual que se incorpora en España a través de la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual, a los que añade como modalidades del servicio de comunicación audiovisual, los servicios de comunicación audiovisual televisiva y radiofónica; ya sean estos lineales, a petición, en movilidad; sean de cobertura estatal; se emitan en abierto o codificado; y sean de acceso gratuito o de pago (artículo 2.2 a 2.5 de la LGCA).

11 Directiva 2007/65/CE, Considerandos 16 y 18.

proporcionar programas, es decir, aquellos cuyo contenido audiovisual sea meramente incidental y no constituya la finalidad principal, situación en la que encajan multitud de servicios de sociedad de la información¹².

Asimismo, quedan excluidas las redes y servicios de comunicaciones electrónicas utilizados para el transporte y difusión de la señal de los servicios de comunicación audiovisual, sus recursos asociados y los equipos técnicos necesarios para la recepción de la comunicación audiovisual, en tanto su régimen es el propio de las telecomunicaciones¹³.

De esta manera queda delimitado el ámbito propio de los servicios de comunicación audiovisual que, en tanto que medios de comunicación de masas, quedan sometidos a un régimen jurídico muy característico ya que responde a la tutela del derecho fundamental a la libre de comunicación y a la promoción de principios democráticos esenciales como son el pluralismo de los medios de comunicación, la imparcialidad, la diversidad cultural y lingüística, la integración social, la protección de los consumidores y la protección de los menores.

En efecto, el régimen de los servicios de comunicación audiovisual, que en España se contiene en la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual – que se completa con normativa a nivel autonómico–, tiene un fundamento completamente distinto al de las telecomunicaciones, lo que determina una modelo de intervención pública mucho más intenso lo que se manifiesta en la exigencia de licencias de comunicación audiovisual para el desarrollo de la actividad y el sometimiento a un control sobre los contenidos emitidos para garantizar el respeto de los derechos reconocidos.

2.3. La delimitación originaria de los servicios de sociedad de la información: El régimen jurídico de los servicios de la sociedad de la información

El último de los ámbitos en surgir dentro del sector digital ha sido precisamente aquel que más lo caracteriza, ya que son todos aquellos servicios prestados a distancia a través de comunicaciones electrónicas y que han ido multiplicándose a partir del acceso a Internet. Se trata de los tradicionales servicios de la tecnología de la información y comunicación (servicios TIC), que en el ámbito de la Unión Europea han sido identificados como servicios de la sociedad de la información y que se corresponden con lo que últimamente se denominan como servicios digitales.

La cantidad y variedad de estos servicios hacer imposible enumerarlos, ya que incluyen desde una simple página web de comercio electrónico hasta complejas plataformas de compras (Amazon, eBay, Aliexpress), videos (Netflix, HBO, Amazon Prime), música (Spotify, Last.fm, Soundcloud), información, opinión o tendencias (desde periódicos hasta los canales de influencers), juegos (Xbox, Playstation, Roblox), pasando por aplicaciones de videollamadas y mensajes (Skype, Whatsapp) y servicios en la nube (GoogleDrive, Dropbox, iCloud) y un largo etc. Se trata de servicios que, en muchos casos, supone una disrupción no solo técnica sino jurídica, ya que proporcionan funcionalidades que pueden ser sustitutivas de los servicios de telecomunicaciones y audiovisuales, así como de otros servicios con una regulación específica como el transporte, el alojamiento, etc. sin estar sujetos a la misma, operando así por encima de dichos regímenes jurídicos,

12 Se trata, por ejemplo, de imágenes y sonidos que pueden formar parte de una plataforma de venta online como Amazon o Zara, o de archivos de imagen y/o sonido que se transmite a través de un servicio de mensajería instantánea como Whatsapp.

13 También se excluye a las personas físicas o jurídicas que únicamente difundan o transporten la señal de programas audiovisuales cuya responsabilidad editorial corresponde a terceros, en tanto estaría fuera de su control el contenido difundido (artículo 3.2 a) y b) LGCA)

lo que lleva a calificarlos como servicios over the top (OTTs).

En el ámbito de la UE, los servicios de sociedad de la información se definen como todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios, requisitos que deben concurrir con carácter acumulativo¹⁴. Esta definición se recoge a nivel interno en la normativa sobre servicios de la sociedad de la información de cada uno de los Estados miembros, en el caso de España, en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI)¹⁵. Se trata de una definición legal de carácter expansivo que abarca un enorme cantidad y variedad de servicios en constante transformación, se recurre a enumeraciones ejemplificativas en las que se incluyen servicios que ofrecen funcionalidades de forma directa y final a los usuarios, y servicios de intermediación que facilitan el acceso a otros servicios o a contenidos e información¹⁶.

El carácter innovador y la plasticidad de los servicios de la sociedad de la información que les permiten desarrollar funcionalidades asimilables a las propias de los servicios de telecomunicaciones y audiovisuales, ha planteado el problema de su distinción de estos servicios que están sometidos a un régimen jurídico específico y más exigente, y que se analizará en el siguiente apartado.

En todo caso, conforme a la definición tradicional de los servicios de telecomunicaciones, no pueden considerarse como tales los servicios de la información que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas¹⁷, y tampoco lo son los servicios de comunicación audiovisual¹⁸.

14 La definición de los servicios de la sociedad de la información procede de la Directiva 98/34/CE sobre servicios de la sociedad de la información, y ahora se recoge en el artículo 1, apartado 1, letra b), de la Directiva 2015/1535 que la sustituye, y a la que remite la Directiva 2000/31/CE sobre el comercio electrónico que desarrolla gran parte de su régimen jurídico.

15 La definición contenida en el apartado a) del Anexo de la LSSI se corresponde exactamente con la dada en la Directiva 98/34/CE y que ahora se recoge en la Directiva 2015/1535.

16 En la definición contenida en el Anexo a) de la LSSI y en la Exposición de Motivos de la misma se enumeran una serie de ejemplos, por una parte, de servicios que ofrecen funcionalidades de forma directa como son la contratación de bienes o servicios por vía electrónica; la organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales; la gestión de compras en la red por grupos de personas; el envío de comunicaciones comerciales; el suministro de información por vía telemática (como el que efectúan los periódicos o revistas que pueden encontrarse en la red). Asimismo se añaden a la definición los denominados servicios de intermediación, que son aquellos por los que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información, como son las actividades de intermediación relativas a la provisión de acceso a la red, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como cualquier otro servicio que se preste a petición individual de los usuarios (descarga de archivos de vídeo o audio...).

17 Tal y como se indica en el art. 1.2 LGTel 2014, ya que la clave es que las actividades en línea de que se trate no sean medio de transmisión, es decir, que no se encarguen específicamente del transporte de señales, lo que excluye aquellos servicios de comunicación entre usuarios como WhatsApp, Skype, etc. que son interfaces y no habilitan a la transmisión de la señal.

18 Quedarían excluidos de la condición de servicios de la sociedad de la información que lleva a cabo la propia LSSI con respecto a los servicios prestados por medio de telefonía vocal,

Esto implica que aquellos servicios que respondan a la definición de los servicios de la sociedad de la información, pero también encajen en la definición más específica de los servicios de comunicaciones electrónicas o audiovisuales, quedarán sometidos al régimen jurídico de éstos últimos. En todo caso, un mismo operador puede desarrollar simultáneamente distintos servicios siempre que cuente con los títulos habilitantes correspondientes y se someta a la normativa específica¹⁹.

Por último, debe tenerse en cuenta que el régimen de los servicios de la sociedad de la información tienen como fundamento esencial la protección de los intereses de los consumidores que son sus usuarios, por lo que, a diferencia del régimen de los servicios de comunicaciones electrónicas y de los servicios audiovisuales, se basa un libre desarrollo de la prestación de estos servicios con respecto a los que no se exige ningún título habilitante y simplemente se imponen unas obligaciones genéricas (de identificación del prestador, información, etc.) para facilitar a los usuarios ejercer sus derechos y se delimitan una serie de responsabilidades para garantizar dichos derechos. Por lo tanto, se trata de un régimen jurídico que contiene una intervención pública mínima en comparación con el propio de los servicios de comunicaciones electrónicas y, sobre todo, de los de comunicación audiovisual.

3. LAS INSUFICIENCIAS EN LA DELIMITACIÓN DE LOS SECTORES DEL ENTORNO DIGITAL ANTE EL EMPUJE DE LOS SERVICIOS DIGITALES OVER THE TOP (OTT)

3.1. El surgimiento de los servicios Over the Top (OTT) y su incidencia en la tradicional articulación jurídica de los sectores económicos

Como se ha podido comprobar, la articulación del entorno digital se ha basado en la configuración de distintos sectores –como son las telecomunicaciones (o comunicaciones electrónicas), el audiovisual y los servicios de la sociedad de la información–, que quedan sujetos a un regímenes jurídicos diferenciados con importantes asimetrías en la intensidad y características de la intervención administrativa desplegada en cada uno de ellos.

Se establece así, desde principios de siglo, una ordenación estanca para cada uno de estos sectores que, en aquel momento, se podían distinguir con claridad, pero cuyas fronteras quedaron rápidamente superadas por los avances tecnológicos que desbordaban las definiciones legales en que se basaba la delimitación de estos sectores.

En efecto, el desarrollo vertiginoso de los servicios en línea prestado a través de Internet durante las dos últimas décadas, impulsado por la mejora en la capacidad y velocidad de conexión y por los avances en la programación informática, ha dado lugar a la aparición de un sinfín de nuevas aplicaciones que dejaron obsoletas las definiciones en que se basaba la delimitación de los distintos sectores en que se articulaba el entorno digital.

fax o télex; el intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan; los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta); los servicios de radiodifusión sonora; el teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas

19 Por ejemplo, un proveedor de servicios de Internet, puede ofrecer tanto un servicio de comunicaciones electrónicas, tal como el acceso a Internet, como servicios de la sociedad de la información, tales como el suministro de contenidos en forma de páginas de Internet, tal y como se indicaba en el considerando 10 de la Directiva Marco.

La manifestación de estos cambios se refleja en los denominados servicios over the top (OTT), que son servicios prestados sobre Internet y se ofrecen directamente a los usuarios finales por terceros que utilizan las redes y servicios de comunicaciones electrónicas, sin necesidad de ningún hardware específico²⁰. Pero lo verdaderamente característico de los servicios OTTs es que son servicios que no encajaban en la tradicional definición de los servicios de comunicaciones electrónicas o los audiovisuales, pero prestaban las mismas funcionalidades, compitiendo en el mercado con éstos desde un régimen jurídico distinto y mucho menos exigente como es el propio de los servicios de la sociedad de la información.

Así, frente a los servicios de comunicaciones electrónicas, van surgiendo servicios OTT de mensajería instantánea que permite el envío de texto, imágenes y videos (como Whatsapp, Telegram, Line, etc.) que sustituyen servicio de telecomunicaciones similares (como los mensajes de SMS o MMS). También van extendiéndose servicios de audio o videollamada (como el propio WhatsApp, Skype, Zoom, etc.) que, cada vez más, sustituyen a los tradicionales servicios de telefonía vocal. En la medida en que todos estos servicios dependen del servicio de acceso a Internet, los demás servicios de telecomunicaciones van siendo abandonados progresivamente a favor del servicio de banda ancha fija o móvil, que es lo único y fundamental que necesitan los usuarios en esa convergencia al todo IP.

Por otra parte, respecto a los servicios de comunicación audiovisual, estos servicios OTT van concentrando cada vez una mayor audiencia en las nuevas formas de consumo de contenidos audiovisuales que superan a los tradicionales canales difusión a través de los servicios de radio y televisión. Se trata de plataformas de video bajo demanda en streaming como Netflix, HBO, Amazon Prime que no son meros difusores sino creadores de contenidos y, por tanto, actores plenos del sector audiovisual, así como plataformas de intercambios de videos o de retransmisión en directo o en diferido como Youtube, Vimeo o Twitch.

Por último, aunque no suele identificarse como servicios OTT, también han surgido innumerables servicios prestados a través de Internet (servicios de la sociedad de la información) que están alterando todos los sectores económicos ya que surgen como instrumentos que modifican el esquema de los mercados de bienes y de servicios. Estos aparecen ofreciendo funcionalidades complementarias a los actores de esos mercados (como los comparadores de productos o las plataformas de prestadores de servicios) o como actores alternativos (distribución de productos -como medicamentos- o de prestación de servicios -apps de seguros-). Esta incidencia tiene un mayor alcance en aquellos sectores que se encuentran sometidos a una mayor intervención pública, pues los nuevos servicios ofrecidos en línea son sustitutivos de los ya existentes, pero no están sujetos a las limitaciones y exigencias propias de la regulación de ese sector –por lo que operan en la misma lógica que los servicios OTT–, como se ha puesto de manifiesto en el caso del sector del transporte de pasajeros (con iniciativas como Uber) o en el de los alojamientos (como AirBnB).

Como se puede comprobar, el desafío de los nuevos servicios prestados a través de Internet es común para la articulación jurídica de los sectores del entorno digital como para el resto de sectores económicos, en tanto desbordan las definiciones legales de

20 Al respecto se puede consultar el "Report on OTT Services" del BEREC [BoR (16) 35] de 29 de enero de y, asimismo, "Caracterización del uso de algunos servicios over the top en España (servicios de comunicaciones y servicios audiovisuales)", Documento de Trabajo nº 4 de la CNMC, diciembre 2014.

modo que no les resulta aplicable el régimen jurídico específico previsto para cada sector, a pesar de que actúan como actores relevantes de los mismos. Este desequilibrio ha sido denunciado por los operadores tradicionales de los correspondientes sectores (comunicaciones electrónicas, audiovisual, transportes, alojamiento, etc.) que reclamaban el denominado *level playing field* para competir en pie de igualdad con estos servicios digitales que se benefician de las insuficiencias en la articulación del régimen jurídico, estudiando las obligaciones, exigencias y cargas previstas en el mismo.

Sin duda, el ámbito donde este desequilibrio entre los OTT y los operadores tradicionales se manifiesta de forma más acentuada es con respecto a los operadores de telecomunicaciones. Esto, ya que los OTT aprovechan sus redes y servicios –en muchos casos con un consumo masivo de datos– para ofrecer servicios sustitutivos a los que ofrecen estos mismos operadores, pero sin tener que desplegar y mantener sus propias redes y servicios, ni tener que afrontar el coste de su uso ya que lo abona el usuario final. El planteamiento de los operadores de telecomunicaciones con respecto a los OTT es que, si sus servicios son sustitutivos de los servicios de comunicaciones electrónicas, deberían quedar sujetos a una misma regulación y responder a las mismas obligaciones que estos²¹.

De hecho, ante la falta de respuesta por parte de los legisladores responsables para equilibrar esta situación (*level playing field*), los operadores tradicionales de telecomunicaciones recurrieron al único recurso a su alcance para incidir en la actividad de estos servicios OTT, que era la gestión del tráfico de la red, modulando la velocidad en función del tipo de servicio utilizado, lo que motivó el reconocimiento del principio de la neutralidad de la red. En efecto, ante la creciente amenaza de que los operadores de telecomunicaciones pudiesen manipular el flujo de datos por sus redes para hacer frente al desafío de los OTT, el Reglamento (UE) 2015/2120 (internet abierta) consagró el principio de neutralidad de la red, al garantizar un tratamiento equitativo y no discriminatorio del tráfico en la prestación de servicios de acceso a internet y los derechos relacionados de los usuarios finales. De este modo, los operadores OTT quedaron blindados frente a cualquier posible acción de los operadores de telecomunicaciones, independientemente que sus servicios puedan suponer un consumo masivo de ancha de banda, como es el caso de las plataformas audiovisuales.

3.2. La respuesta jurisprudencial ante las insuficiencias en la delimitación de los sectores económicos

A pesar del desafío que suponía la aparición de los nuevos servicios prestados por Internet para la articulación jurídica de los distintos sectores tanto dentro del entorno digital como en la economía, en general, las definiciones legales sobre las que establecía la delimitación de cada uno de estos sectores han permanecido inalteradas casi dos décadas, desde los inicios de siglo²².

21 De este modo, por ejemplo, consideran que los OTTs deben abonar las tasas de telecomunicaciones o responder a las obligaciones de servicio público, contribuyendo a la financiación del servicio universal, facilitando el acceso a servicios de emergencia a través de 112 y respetando las exigencias de calidad de los servicios.

22 En efecto, si bien la Directiva Marco y el resto del Paquete Telecom de 2002 fue modificada por la Directiva 2009/140, sin embargo, no se modificaron las definiciones de los servicios de comunicación electrónica. Otro tanto sucedió con los servicios de comunicación audiovisual una vez que fueron introducidos en la Directiva 2007/65/CE y a la que sustituyó la Directiva 2010/13/UE sobre servicios de comunicación audiovisual. Tampoco se modificó la definición de los servicios de la sociedad de la información asentada en la Directiva 98/34/CE que fue sustituida por la Directiva 2015/1535.

Ante la renuncia por parte del legislador europeo de abordar los cambios que estaban introduciendo los servicios OTT, fue la jurisprudencia del Tribunal de Justicia de la Unión Europea (TJUE) la que vino a concretar y aclarar las dudas que se han ido planteando al respecto en cada caso. En este sentido, si bien los pronunciamientos del TJUE no han sido muy numerosos, sí han sido relevantes ya que han sido tenidos en cuenta posteriormente por el legislador europeo a la hora de definir los distintos tipos de servicios del ámbito digital.

Por una parte, el TJUE ha tenido ocasión de pronunciarse sobre la distinción entre los servicios de comunicaciones electrónicas y aquellos servicios de sociedad de la información que se utilizan para comunicarse, como es el caso del correo electrónico o aplicaciones de audio o videollamadas a través de Internet. Se trata de sentencias muy casuísticas, con las que no se pretende establecer criterios generales, sino que analizan las características de cada servicio llegando a conclusiones divergentes en función de las mismas.

Así, el servicio de correo electrónico prestado por Google (Gmail) fue excluido de la consideración de servicio de comunicación de comunicación electrónica siendo considerado un servicio sociedad de la información. La cuestión no era tan evidente ya que el proveedor del servicio de correo electrónico en Internet efectúa una transmisión de señales, pero el Tribunal consideró no era su actividad principal y que no tenía responsabilidad dicha transmisión (STJUE de 13 de septiembre de 2019, C-193/18). Resulta relevante esta interpretación del TJUE, ya que posteriormente se modificaría la definición de los servicios de comunicaciones electrónicas para incluir este tipo de servicios de la sociedad de la información.

Por el contrario, un servicio de llamadas de Skype (STJUE de 5 de junio de 2019, C-142/18) directamente a teléfonos fijos o móviles, es considerado parte de los servicios de comunicaciones electrónicas, por lo que debe someterse a su régimen jurídico. La clave aquí es la funcionalidad adicional (denominada SkypeOut) que permite al usuario llamar a un número fijo o móvil gracias a acuerdos con operadores de telecomunicaciones encargados de terminar la llamada. En este criterio ha sido recogido en la nueva definición de los servicios de comunicaciones electrónicas que distingue entre los servicios de comunicaciones interpersonales que utilizan números servicios de comunicaciones interpersonales que utilizan numeración y aquellos que no lo hacen.

Por otra parte, el TJUE también se ha pronunciado sobre la distinción entre los servicios de comunicaciones electrónicas y los servicios audiovisuales, llevando a cabo una interpretación expansiva del alcance de los primeros al incluir todos servicios que sirven para la transmisión de la señal de radio y televisión.

Así, con respecto a un operador de cable (STJUE de 7 de noviembre de 2013, C-518/11), que facturaba tanto por los costes de transmisión como por los derechos de autor por la difusión del contenido de las obras, fue considerado un operador de comunicaciones electrónicas en la medida que su actividad principal consistía en la transmisión de la señal por cable hasta el terminal de recepción del consumidor final. En el mismo sentido calificó un servicio de conexión vía satélite que ofrecía esencialmente contenidos televisivos de acceso condicional como servicio de comunicaciones electrónicas (STJUE de 30 de abril de 2014, C-475/12). Se confirma así la relevancia de la actividad de transmisión independientemente de lo transmitido, incluidos los contenidos radiofónicos o televisivos.

Por el contrario, el TJUE deja fuera de la consideración de servicios de comunicación audiovisual la oferta de contenidos audiovisuales a través de Internet, similar a la que

llevan a cabo multitud de plataformas de video bajo demanda (STJUE de 13 de diciembre de 2018, C-298/17). En concreto el Tribunal considera que una empresa que ofrece el visionado de programas de televisión en flujo continuo y en directo en Internet no debe ser calificada como operador de comunicaciones electrónicas, ya que una cosa es la transmisión y otra el contenido de los servicios prestados a través de las redes y servicios de comunicaciones electrónicas.

Por último, el TJUE también ha entrado la distinción de los servicios de sociedad de la información y otros servicios ajenos al entorno digital, pero sobre los que incide de forma decisiva, como son los servicios de transporte o alojamiento. En este sentido ha interpretado que los servicios de sociedad de la información dejan de serlo, y pasan a ser considerado otro tipo de servicio (de transporte, alojamiento, etc.), en función de las características del servicio de intermediación que cumplen y de cómo se insertan y afecta a la estructura de prestación del servicio final para el que realizan la intermediación. Conforme a la jurisprudencia, esto sucede cuando ese servicio de intermediación forme parte integrante de un servicio global cuyo elemento principal sea un servicio al que corresponda otra calificación jurídica (servicio de transporte, de alojamiento, etc.) (STJUE de 19 de diciembre de 2019, C-390/18).

Así, en el TJUE consideró que un servicio de intermediación para la prestación de servicio de transporte de vehículos de turismo con conductor (VTC) como Uber no era un simple servicio de la sociedad de la información, en tanto el prestador crea una oferta de servicios de transporte urbano, que hace accesible concretamente mediante herramientas informáticas, y organiza el funcionamiento general de la misma en favor de las personas que deseen recurrir a esta oferta, por lo que el servicio de intermediación prestado debe considerarse parte integrante de un servicio global cuyo elemento principal es un servicio de transporte y, por lo tanto, pasa a ser considerado un servicio de transporte y a someterse a la normativa de los mismos (STJUE de 20 de diciembre de 2017, C-434/15).

Por el contrario, en el caso de un servicio de intermediación para la prestación de transporte de taxi (una app para reservar taxis autorizados) fue considerado como servicio de sociedad de la información ya que, por sus características, al limitarse a poner en contacto a los consumidores con los taxistas autorizados sin influir en ninguna condición del servicio (precio, calidad, etc.), no debía considerarse como parte integrante del servicio de transporte urbano (STJUE de 3 de diciembre de 2020, C-62/19).

Como se puede comprobar, la jurisprudencia del TJUE, por razón de su carácter limitado y fragmentario, no podía ser la solución al desbordamiento que estaban provocando la aparición de nuevos servicios prestados a través de Internet que superaban las tradicionales definiciones sobre las que se había articulado el régimen jurídico de los distintos sectores tanto dentro del entorno digital como en la economía en general, por lo que fue necesario un replanteamiento de dichas definiciones y de los regímenes jurídicos aplicable en estos sectores.

4. LA NUEVA DELIMITACIÓN DE LOS SECTORES DEL ENTORNO DIGITAL: LA AMPLIACIÓN DE LAS DEFINICIONES Y LA ADAPTACIÓN DE LOS REGÍMENES JURÍDICOS SECTORIALES

La intensificación de la transformación digital derivada del uso masivo y generalizado de servicios prestados a través de Internet hicieron insostenible la tradicional delimitación de sectores del entorno digital, basada en unas definiciones de los servicios de telecomunicaciones, audiovisual y sociedad de la información que se habían dado casi dos décadas atrás, y que estaban siendo constantemente superadas por nuevos servicios

que permitían actuar en distintos sectores sin tener que someterse a su respectivo régimen jurídico, actuando por encima de estos, operando sometidos exclusivamente bajo laxo régimen propio de los servicios de la sociedad de la información.

Frente a este desafío, a lo largo de la última década, se desarrolló un intenso debate sobre cuál debía ser la solución para regular estos nuevos servicios OTTs. En este, se planteaba desde someterlos en igualdad de condiciones al régimen jurídico de aquellos servicios que afectase, a crear un régimen jurídico exclusivo y autónomo para esta categoría de servicios o incluso mantener la misma situación actual que les permitiese desarrollarse y evolucionar libremente.

La solución escogida es una tercera vía que implica incluir a estos nuevos servicios prestados por Internet que actúan como servicios OTTs a través de la ampliación de la definición de los servicios a los que afectan (comunicaciones, audiovisual) y, simultáneamente, adaptar el régimen jurídico aplicable para darles un tratamiento específico y asimétrico, distinto y menos gravoso que el resto de los tradicionales operadores de estos servicios.

4.1. La nueva definición de los servicios de comunicación electrónica y la adaptación de su régimen jurídico

Así, puede apreciarse en el Código Europeo de las Comunicaciones Electrónicas aprobado por la Directiva (UE) 2018/1972, la apertura hacia una definición más amplia sobre los servicios de comunicaciones electrónicas, pues se incluyen servicios de la sociedad de la información que habían quedado, hasta ese momento, fuera de dicha consideración, justificándolo en el hecho de que son servicios sustitutivos, por lo que se hace necesario garantizar que los usuarios finales y sus derechos estén eficaz y equitativamente protegidos cuando utilicen servicios de función equivalente²³.

Por lo tanto, se abandona la vinculación de las redes y servicios de comunicaciones electrónicas al «transporte de señales» –aunque se sigue utilizando como criterio– y se establece una definición que incluye otros servicios que permiten la comunicación, sin llevar a cabo el transporte o la transmisión. Se amplía así la definición de los servicios de comunicaciones electrónicas, pero se introducen tres categorías con regímenes específicos y asimétricos, los cuales deberán identificarse a partir de un recorrido por las normas que, en cada caso, les resultan aplicables²⁴: servicios de acceso a internet, los servicios de comunicaciones interpersonales, y los servicios que consisten total o principalmente en el transporte de señales.

Debe tenerse en cuenta que este cambio en la definición no ha supuesto la absorción de los servicios de comunicación audiovisual y los servicios de la sociedad de la información que siguen existiendo como categoría con su respectivo régimen jurídico, si bien mucho de los segundos van a pasar a ser considerados servicios de comunicaciones electrónicas

-
- 23 Desde la perspectiva del usuario final, no hace al caso si un proveedor transporta las señales él mismo o si la comunicación se ofrece mediante un servicio de acceso a internet, por lo que debe garantizarse dicha comunicación como tal independientemente de cómo se produzca. Esto se debe a la evolución tecnológica y de los mercados que ha hecho que las redes se dirijan a la tecnología del protocolo de internet (IP), y ha posibilitado que los usuarios finales escojan entre una serie de proveedores de servicios vocales competidores, independientemente de la tecnología que se utilice (considerando 13).
 - 24 Se pretende así eliminar las ambigüedades observadas en la aplicación de la definición de los servicios de comunicaciones electrónicas y permitir una aplicación particularizada, disposición por disposición, de los derechos y obligaciones específicos que comprende el marco a los diferentes tipos de servicios (considerando 11).

en la medida que encajen en la definición que se hace de cada una las categorías de servicios de comunicaciones electrónicas y, específicamente, en los denominados servicios de comunicaciones interpersonales²⁵.

En efecto, dentro de las nuevas categorías de servicios de comunicaciones electrónica destacan los servicios de comunicaciones interpersonales, que se definen como los prestados por lo general a cambio de una remuneración que permite un intercambio de información directo, interpersonal e interactivo a través de redes de comunicaciones electrónicas entre un número finito de personas, en el que el iniciador de la comunicación o participante en ella determina el receptor o receptores y no incluye servicios que permiten la comunicación interpersonal e interactiva como una mera posibilidad secundaria que va intrínsecamente unida a otro servicio²⁶.

Dentro de los servicios de comunicaciones interpersonales se distinguen entre aquellos basados en numeración –entre los que se encuentran los servicios de comunicaciones vocales y que se caracterizan ya que los usuarios finales tienen asignados para garantizar la conectividad y que entren en contacto–, y los independientes de la numeración, que son la verdadera novedad, ya que supone la inclusión de un gran número de servicios que, hasta entonces, eran considerados como simples servicios de la sociedad de la información.

Lo relevante de todas estas nuevas categorías es que quedan sometidas a un tratamiento jurídico diferenciado en cada una de ellas, lo que resulta especialmente notable en el caso de los servicios de comunicaciones interpersonales sin numeración que quedan sometidas a obligaciones mucho menos exigentes, ya que estos últimos solo deben estar sujetos a obligaciones cuando el interés público exija la aplicación de obligaciones reglamentarias específicas a todos los tipos de servicios de comunicaciones interpersonales, con independencia de que utilicen números para la prestación de su servicio²⁷.

4.2. La nueva definición de los servicios de comunicación audiovisual y la adaptación de su régimen jurídico

Este modelo conforme al que se amplía la definición de los servicios sometidos a un régimen jurídico específico, pero se adapta su contenido para ajustarlo a las características de cada servicio, no es privativo de las comunicaciones electrónicas, sino que se ha extendido igualmente a los servicios audiovisuales en términos muy similares.

En efecto, la Directiva (UE) 2018/1808 de servicios de comunicación audiovisual²⁸ viene a modificar su definición por razón de la convergencia de la televisión y los servicios de

25 Por lo tanto, dentro de los OTT, los servicios prestados por proveedores de contenidos como Netflix, HBO, Amazon Prime, Spotify y demás, seguirán quedando fuera de la consideración de los servicios de comunicaciones electrónicas, pero los servicios de mensajería, audio o videollamada (desde el Gmail hasta WhatsApp) pasan a ser considerados como tales, dentro de la categoría de servicios de comunicación personal, aunque se someten a un régimen diferenciado mucho menos intenso que el propio de los operadores tradicionales de telecomunicaciones.

26 Características que deben cumplirse todos de forma acumulativa (artículo 2.5 CECE).

27 Se considera justificado dar un trato diferente a los servicios de comunicaciones interpersonales basados en numeración, ya que participan en un ecosistema interoperable garantizado públicamente y, por consiguiente, también se benefician de él (considerando 17 CECE).

28 Directiva (UE) 2018/1808 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, por la que se modifica la Directiva 2010/13/UE sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la

internet gracias a los avances técnicos que ofrecen nuevos servicios que modifican los hábitos de los ciudadanos, que van abandonando los contenidos televisivos tradicionales a través de la pantalla de televisión por nuevos tipos de contenidos, como los vídeos cortos o el contenido generado por los usuarios, al margen de los servicios de vídeo a petición. Se procura así ajustar el marco jurídico actualizado para adaptarse a la evolución del mercado y permitir un equilibrio entre el acceso a los servicios de contenidos en línea, la protección del consumidor y la competencia.

Sin embargo, en este caso la estrategia es algo diferente ya que no se utiliza una única definición de servicios de comunicación audiovisual bajo la que se establecen distintas categorías de estos servicios que quedan sometidos a condiciones específicas, sino que junto a estos se introduce los denominados servicios de intercambio de vídeos a través de plataforma o plataforma de intercambio de vídeos que quedan sometidos a su propio régimen jurídico, lo que a efectos prácticos es casi lo mismo.

La definición de los servicios de comunicación audiovisual también se ajusta, ya que se parte de la tradicional identificación de estos servicios como aquellos cuya finalidad consiste en ofrecer programas al público en general, bajo la responsabilidad editorial de un prestador de servicios de comunicación, con objeto de informar, entretenér o educar, a través de redes de comunicaciones electrónicas, pero se especifica que debe ser su finalidad principal propia o de una de sus partes disociables²⁹.

No obstante, lo verdaderamente novedoso es la inclusión en la normativa audiovisual de los "servicios de intercambio de vídeos a través de plataforma" o "plataformas de intercambio de vídeos" que son definidos como aquellos cuya finalidad principal propia o de una de sus partes disociables o cuya funcionalidad esencial consiste en ofrecer al público en general programas, vídeos generados por usuarios o ambas cosas, sobre los que no tiene responsabilidad editorial el prestador de la plataforma, con objeto de informar, entretenér o educar, a través de redes de comunicaciones electrónicas, y cuya organización determina el prestador de la plataforma de intercambio de vídeos, entre otros medios con algoritmos automáticos, en particular mediante la presentación, el etiquetado y la secuenciación³⁰.

En todo caso, estos servicios y plataformas de intercambios de videos quedan sometidos a un régimen jurídico específico que se construye sobre el régimen propio de los servicios de comunicación audiovisual, aunque limitando y modulando el alcance de muchas de las obligaciones, requisitos y exigencias dispuestos para estos últimos, sometiéndolos así

prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual), habida cuenta de la evolución de las realidades del mercado.

- 29 Conforme a la nueva redacción del artículo 1.1 a) de la Directiva 2010/13/UE. Se cumple el requisito del objetivo principal si el servicio tiene una forma y contenido audiovisuales disociables de la actividad principal del prestador de servicios, como las partes autónomas de los periódicos en línea que ofrecen programas audiovisuales o vídeos generados por usuarios, cuando dichas partes puedan considerarse disociables de su actividad principal. Por el contrario, se trata de un mero complemento indisociable de la actividad principal cuando exista una conexión importante entre la oferta audiovisual y la actividad principal, como facilitar noticias por escrito [considerando 3 de la Directiva (UE) 2018/1808]
- 30 Conforme a la nueva redacción del artículo 1.1 a) bis de la Directiva 2010/13/UE. Lo que se justifica en tanto se ponen a disposición contenidos audiovisuales y se han convertido en un importante medio para compartir información, entretenér y educar, y compiten por la misma audiencia e ingresos que los servicios de comunicación audiovisual, además de tener un impacto considerable, ya que ofrecen a los usuarios la posibilidad de conformar las opiniones de otros usuarios e influir en ellas.

un marco jurídico mucho más flexible.

4.3. La nueva definición de los servicios de intermediación y de los servicios básicos de plataforma y su nuevo régimen jurídico

El último frente desde el que se está llevando a cabo la nueva delimitación de los sectores que componen el entorno digital afecta a los propios servicios de la sociedad de la información, ya que, aunque se mantiene la misma definición fijada originalmente, se ha propuesto establecer un régimen jurídico propio para los servicios de intermediación y también para los servicios básicos de plataforma, que son las dos categorías de servicios de la sociedad de la información que más han alterado la tradicional configuración de los sectores del entorno digital.

Por una parte, la definición de los servicios de sociedad de la información se va a ver completada con los servicios de intermediación que vienen configurados por la propuesta de Reglamento sobre servicios digitales³¹ y que se aplica a aquellos servicios intermediación que no constituyen parte integral de otro servicio que no es un servicio intermediado (servicio de transporte, de alojamiento) según se especifica en la jurisprudencia del TJUE, ya que de lo contrario pasaría a regirse por la normativa propia de ese servicio principal.

Dentro de los servicios de intermediación destacan los servicios de alojamiento de datos tales como servicios en nube y de alojamiento web que quedan sometidos a obligaciones comunes³². Los servicios de alojamiento incluyen, a su vez, plataformas online que reúnen a vendedores y consumidores (como mercados online, tiendas de aplicaciones, plataformas de economía colaborativa y plataformas de redes sociales) que se someten a obligaciones adicionales³³. En cuanto a las plataformas online muy grandes plantean especiales riesgos y para las que contemplan normas específicas cuando que llegan al 10% de los 450 millones de usuarios europeos³⁴.

Por otra parte, la tradicional definición de los servicios de la sociedad de la información también se va a ver completada con el régimen específico para los servicios básicos de plataforma que actúan como guardianes de acceso (*gatekeepers*) que se contiene en la propuesta de Reglamento sobre mercados digitales³⁵, y que afecta a determinados servicios que disfrutan de dicha posición (servicios de intermediación, motores de búsqueda, redes sociales, plataformas de intercambio de vídeos, comunicaciones interpersonales independientes de la numeración, sistemas operativos, servicios de computación en

31 Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE (COM/2020/825 fin).

32 Informes de transparencia, condiciones de servicio conformes a los derechos fundamentales, cooperación con las administraciones nacionales; puntos de contacto y representante legal; notificación y adopción de medidas y obligación de informar a los usuarios.

33 Mecanismos de reclamación y recurso y de resolución extrajudicial de litigios, alertadores fiables, medidas contra las notificaciones y contra notificaciones abusivas, comprobación de las credenciales de terceros proveedores, transparencia de la publicidad online para los usuarios, denuncia de infracciones penales.

34 Obligaciones sobre gestión de riesgos y responsables del cumplimiento, auditoría externa de riesgos y rendición pública de cuentas, transparencia de los sistemas de recomendación y posibilidades de elección de los usuarios para el acceso a la información, intercambio de datos con administraciones e investigadores, códigos de conducta, cooperación en materia de respuesta a las crisis.

35 Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre mercados disputables y equitativos en el sector digital (Ley de Mercados Digitales) COM/2020/842 final

nube, servicios de publicidad). Cuando estas plataformas básicas sean considerados guardianes de acceso³⁶, quedan sometidos a una serie de obligaciones y de restricciones para garantizar que no abusen de su posición y faciliten la libre competencia³⁷.

5. CONCLUSIÓN

El empuje de los nuevos servicios digitales prestados a través de Internet está desbordando la estructura de los tradicionales régímenes jurídicos de los sectores de referencia del entorno digital como son las telecomunicaciones, el audiovisual y de los propios servicios de la sociedad de la información en los que aquellos se enmarcan. Se hace imprescindible así equilibrar la situación en que se encuentran estos servicios que actúan como actores relevantes en todos los mercados del entorno digital, pero desarrollan su actividad al margen del correspondiente régimen jurídico al que se encuentran sometidos los operadores tradicionales.

La opción escogida en el ámbito de la Unión Europea ha sido ampliar la definición legal que delimita estos sectores para incorporar estos nuevos servicios al régimen jurídico de las telecomunicaciones y del audiovisual, a la vez que se adapta su contenido distinguiendo distintas categorías de servicios que se someten a unos derechos y obligaciones específicos y distintos de los propios de los operadores tradicionales de estos sectores. A esto se suma la propuesta regulatoria de los propios servicios digitales que introducen nuevos límites y obligaciones para aquellos que tengan una mayor repercusión sobre los ciudadanos por su volumen de impacto (servicios digitales básicos) o su carácter estratégico (guardianes de acceso).

Con este novedoso planteamiento se consigue un importante avance, que va a permitir superar el tradicional problema de los servicios OTT y su falta sometimiento al régimen jurídico de referencia junto a los demás operadores del sector. Sin embargo, la solución no es, ni mucho menos definitiva, ya que se limita a trasladar el debate a la determinación del alcance de las obligaciones y requisitos que corresponda a estos servicios como operadores del sector de referencia.

En todo caso no se deben desdeñar los logros de esta estrategia ya que, por lo pronto, permite incorporar servicios equivalentes bajo un mismo marco jurídico, avanzando así en el *level playing field* y evitando así el debate binario entre aplicación o no aplicación de un bloque normativo completo, además de trasladar la cuestión a un contexto más flexible como es la determinación de los derechos y obligaciones que corresponden a unos y otros operadores dentro de un mismo marco normativo, bajo el principio de imponer obligaciones similares a servicios semejantes.

Esta será la clave para mantener el equilibrio y la eficacia en la ordenación de los

36 Las plataformas básicas son considerados guardianes de acceso cuando tiene una posición económica fuerte, un impacto significativo en el mercado interior y actividades en muchos países de la UE; tiene una sólida posición de intermediadora, con una amplia base de usuarios y un gran número de empresas; y tiene (o está a punto de tener) una posición arraigada y duradera en el mercado.

37 Así deberán permitir a terceros interactuar con sus propios servicios, permitir que sus empresas usuarias accedan a los datos que generan al utilizar la plataforma del guardián de acceso, ofrecer a las empresas que publicitan en su plataforma las herramientas y la información necesarias para que anunciantes y editores lleven a cabo su propia verificación independiente de los anuncios alojados por el guardián de acceso, permitir que sus empresas usuarias promocionen sus ofertas y celebren contratos con sus clientes fuera de la plataforma del guardián de acceso.

distintos sectores que integran el entorno digital y requiere un análisis muy detallado del contenido exacto del régimen jurídico que le corresponde a cada categoría de servicios porque, aunque todos sean a partir de ahora operadores de un mismo sector, su estatuto no será exactamente el mismo para todos ellos.

6. BIBLIOGRAFÍA

- Aguado-Guadalupe, G. y Bernaola, I. (2019). «El nuevo marco regulador europeo de los servicios audiovisuales bajo petición y de intercambio de vídeo. Su repercusión en el mercado español de plataformas», *Index.Comunicación*, 9(3), 13-34.
- Andrés Segovia, Belén. (2020). La convergencia de las telecomunicaciones, los medios de comunicación y las tecnologías de la Información. Aranzadi.
- Echebarría Sáenz, Marina. (2021). "Restricciones de acceso al mercado y plataformas digitales: el caso Amazon como ejemplo", *Revista de Estudios Europeos*, No 78, julio-diciembre, 154-182.
- Fernández, Lionel. El Código Europeo de las Comunicaciones Electrónicas: Una auténtica reforma de la regulación de las telecomunicaciones. *Revista General de Derecho de los Sectores Regulados*, 2-9.
- García Castillejo, Ángel. (2017). La regulación del sector audiovisual. De la radio y la televisión a los servicios sobre la red (OTT)», en Edgar González López (Dir.), *El ecosistema digital y las autoridades de regulación de los sectores audiovisual y TIC*, 1075-1116.
- Malaret García, Elisenda. (2015). «Los servicios excluidos del ámbito de aplicación de la legislación de telecomunicaciones: Los servicios de la Sociedad de la Información y los Servicios de Comunicación Audiovisual», en T. Quadra-Salcedo (Dir.), J. Vida (coordinador), *Derecho de las telecomunicaciones*, Aranzadi, Cizur Menor, 2015, págs. 104-137.
- Quadra-Salcedo Fernández del Castillo, Tomás. (2004). «Comentario a las disposiciones generales de la LGT», en E. García de Enterría y T. de la Quadra-Salcedo (Dirs.): *Comentarios a la Ley General de telecomunicaciones. Ley 32/2003, de 3 de noviembre*, Madrid, Thomson/Civitas.
- Rodríguez de las Heras Ballell, Teresa. (2020). "Los servicios de la sociedad de la información en una Economía de Plataformas: Caso Uber. La segunda generación de la economía digital en la Unión Europea", en Albert Ruda González; Carmen Jerez Delgado (dirs.), *Estudios sobre Jurisprudencia Europea: materiales del III Encuentro anual del Centro Español del European Law Institute Vol. 2*, 69-85.
- Vida Fernández, José (2016), «Las garantías para el acceso a una internet abierta en el reglamento (UE) 2015/2120: una batalla perdida para la neutralidad de la red», *Revista General de Derecho Europeo*, núm. 40, 96-124.

7. ANEXO DE NORMATIVA Y JURISPRUDENCIA

Normativa

- Directiva 89/552/CEE del Consejo, de 3 de octubre de 1989, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados Miembros relativas al ejercicio de actividades de radiodifusión televisiva

Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas.

Directiva 2002/77/CE de la Comisión, de 16 de septiembre de 2002, relativa a la competencia en los mercados de redes y servicios de comunicaciones electrónicas.

Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de equipos radioeléctricos terminales (Directiva RED)

Reglamento (UE) 2015/2120 del Parlamento Europeo y del Consejo de 25 de noviembre de 2015 por el que se establecen medidas en relación con el acceso a una internet abierta

Directiva 2014/61/UE del Parlamento Europeo y del Consejo, de 15 de mayo de 2014 , relativa a medidas para reducir el coste del despliegue de las redes de comunicaciones electrónicas de alta velocidad (BBcost)

Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.

Jurisprudencia

Sentencia del Tribunal de Justicia Europea de 7 de noviembre de 2013, *UPC Nederland*, asunto C-518/11.

Sentencia del Tribunal de Justicia Europea de 30 de abril de 2014, *UPC DTH Sàrl*, asunto C-475/12.

Sentencia del Tribunal de Justicia Europea de 20 de diciembre de 2017, *Asociación Profesional Elite Taxi*, C-434/15, apartados 38 a 44.

Sentencia del Tribunal de Justicia Europea de 13 de diciembre de 2018, *France Télévisions SA y Playmédia*, asunto C-298/17.

Sentencia del Tribunal de Justicia Europea de 5 de junio de 2019, *Skype vs. IBDP*, asunto C-142/18.

Sentencia del Tribunal de Justicia Europea de 13 de septiembre de 2019, *Google vs Alemania*, asunto C-193/18.

Sentencia del Tribunal de Justicia Europea de 19 de diciembre de 2019, *Airbnb Ireland*, C-390/18, apartado 50 y jurisprudencia citada.

Sentencia del Tribunal de Justicia Europea de 3 de diciembre de 2020, *Star Taxi App*, C-62/19, apartado 55.

Consejo de Egresados

A

1. Acosta Álvarez, Gloria María
2. Aguilar Obregón, Alan Kenny
3. Aguirre Alván, Rossana Lisset
4. Alberto Chagua, Luz Milagros
5. Alvarado Ordoñez, Ángela
6. Ancieta Sánchez, Wendy Valeria
7. Angulo Carvallo, Ana Cecilia
8. Arroyo García, Renato Mario
9. Arroyo Tocto, Victor
10. Ataupillco Calderón, Saly Eveling
11. Azerrad Urrutia, Cecilia

B

12. Balbuena Pérez, Humberto Manuel
13. Bar Infantes, Ricardo José
14. Barbieri Rodríguez, Carla Pamela
15. Bayro Valenza, Claudia Livia
16. Bellota Zapata, Jose Carlos
17. Benavides Mendoza, Elmer Alberto
18. Benvenuto Millones, Víctor Andrés
19. Bernal Alcalá, María Elena
20. Bringas Aceijas, José Gonzalo
21. Bonnett Escobar, Francisco Roberto
22. Briceño Barboza, Sofía
23. Brocq Montalva, Gonzalo

C

24. Caballero Beraún, Luis de Jesús
25. Caballero Alvarado, Victor Raúl
26. Cabrera León, Jennifer Elizabeth
27. Cacnahuaray Huillcahuari, Lucy
28. Caicedo Safra, Paola
29. Camones Avendaño, Gabriella Lorenza
30. Campos Kou, Alexandra Cecilia
31. Cano Nuñez, Patricia M.
32. Carbonell Bonilla, Teresa de Jesús
33. Cárdenas Hurtado, Renato
34. Carretera Estrada, Nacory
35. Carrillo García, Giuliana Vanessa
36. Castañeda Panduro, Cinthia Irene
37. Castañeda Cáceda, Jaime
38. Castillo Meza, Miguel Antonio
39. Castillo Chávez, Christian Daniel
40. Castro Ausejo, Sheila

41. Caycho Bravo, Diana
42. Celis Velásquez, Samantha
43. Chaupis Sosa, Daniela Anyela
44. Chávez Granda, Julissa
45. Chávez Manrique De Lara, Katherine Stefany
46. Chávez Gutiérrez, Wendy Elizabeth
47. Chinchay Yacunta, Juan José
48. Ciriaco Bellido, Carlos
49. Común Túpac, Virginia
50. Cordero Maldonado, Lorena del Pilar
51. Córdova Pineda, Daniel Alberto
52. Coronado Robles, Jacquelyn Elvira
53. Coronel Meza, Marco Antonio
54. Coronel Pardavé, Natalia
55. Cuadros Gómez, Henry
56. Cubas Sáenz, Alessandra Patricia
57. Cuyutupa Luque, Jorge Carlos

D

58. Dávila Llacrahuanga, Luis Antonio
59. Delgado Peralta, Wilmer Alexander
60. Delgado de la Flor Dondero, Cinthya
61. Díaz Montalvo, Jorge Armando
62. Díaz Berrú, Katherine Elizabeth
63. Díaz Kong, Alejandra Sarai
64. Dongo Torres, José Carlos
65. Durán Vargas, Michael

E

66. Echevarría Carrasco, Katherine Fiorella
67. Egúsquiza Cerrón, Pierina Fiorella
68. Escobedo Del Carpio, Rocío
69. Espinoza Unda, Marcelo Daniel

F

70. Farfán Sousa, Ronnie Aldo
71. Fernández Buitrón, José
72. Fernández Rojas, Paolo Junior
73. Figueroa Zárate, Elisa Angelina
74. Flores Menéndez, Fiorella Patricia
75. Fuentes Garrido, Claudia Alejandra

76. Fustamante Fuentes, Sandra
Gianina
77. Fung Romero, Cindy Meylan

G

78. Gálvez Paiba, Mónica Patricia
79. Gamarra Barrantes, Lily Carolina
80. Garaycott Ortiz, Richie Orlando
81. Gómez Bellota, Edson Américo
82. Guardia Muguruza, Lorena
83. Guerrero Gallegos, Luis Enrique
84. Guerrero Zambrano, Luis Fernando
85. Gurreonero Aguado, Leyla Fiorella
86. Gutiérrez Avendaño, Michel Fabricio
87. Gutiérrez Suarez, Sara
88. Guzmán Alarcón, Alisson Lisette

H

89. Herencia Chuquihuanga, Amaru Ernesto
90. Hernández Gonzales-Mugaburú, Andrea
91. Hinostroza Sobrevilla, Luis Martín
92. Huapaya Nava, Mario
93. Humala Marín, Lineth Estefani

J

94. Jaime Zamora, Carlos Martín
95. Jiménez Chávez, Cinthia Paola
96. Jiménez Alemán, José Alonso
97. Jiménez Aquiño, Carmen Alejandra

K

98. King Kee Handabaka, Alberto Orlando
99. Kuroki Távara, Kioshy Alfredo

L

100. Lafitte Lamas, Samara Annel
101. Landa Farfán, Luis Arturo
102. Lanegra Ramírez, Óscar José
103. La Rosa Salas, Mayra Alejandra
104. León Cabezudo, Liz
105. León Vargas, Víctor

106. Leyva Chacón, Teresa Elena Otilia
107. Limaco Chahua, Ayme Denisse
108. Límaco Medina, Daniel Gustavo
109. Llanos Vergara, Juan Antonio
110. Lolay Huamanyauri, Ingrid Vanessa
111. Lolay Huamanyauri, Yoselin
112. López Matzukaka, Jaime

M

113. Macassi Zavala, Juan Pablo
114. Magni Chinchay, Martín José
115. Mancada Alcántara, Enrique Alberto
116. Manrique Chávez, Renoir Katia
117. Mantilla Acosta, Bertha
118. Mantilla Acosta, Carla Elizabeth
119. Martínez del Águila, Shane Starsky Mathias
120. Miranda Cabrera, Marycielo Lisbeth
121. Mayhuasca Torres, Pamela
122. Mayorca Munive, Gonzalo
123. Melgar Córdova, Eduardo R.
124. Mendiola Florez, David Enrique
125. Mendoza Jesus, Jenny Estephany
126. Mendoza Luna, José Luis Leoncio
127. Mendoza Guerra, Juan Pablo
128. Mendoza Guerra, Víctor Andrés
129. Merodio Mejía, Lourdes Inés
130. Mogrovejo Rivera, Milagros María
131. Montoro Rodriguez, Daniela
132. Montenegro Monteza, Favio Martín
133. Montes Huamán, Tania Lorena
134. Montes Huamán, Tatiana
135. Mora Paniagua, Carol Julissa
136. Morote Tipe, Leyla Kerly
137. Muñoz Toalino, Luis Alberto

N

138. Navarrete Delgado, Cinthya Rosario
139. Nieto Donayre, Silvana de los Ángeles
140. Noriega Egas, Carmen Rocío

O

141. Ochoa Richard, Fiorella Giannina
142. Ocón Soto, Luis
143. Olaechea Barbieri, Vilma Karina

144. Olavide Cuba, Ana Zoraida
145. Oliva Castro, Marisol
146. Ordoñez Zenteno, César Augusto
147. Orellana Maldonado, Sybila Antonella
148. Ormeño Monroe, Renato Aníbal
149. Ortiz Fernández, Andrea María
150. Otero Valencia, Jackeline Paola

P

151. Palacios Arzapalo, Gladys Giovana
152. Pancca Mamani, Erika Fabiola
153. Pantoja Acuña, Paola Janet
154. Paredes Marroquin, Juan Alberto
155. Paredes Gutiérrez, Marcela Inés
156. Pastrana Espinal, Graziella Fiorella
157. Patiño Muñoz, Manuel Alberto
158. Paz Aparicio, Leonardo Daniel
159. Pereira Pinedo, Erika Mercedes
160. Pereyra Pachas, Allison Dayane
161. Pérez Huamani, Claudia
162. Pizarro Breña, Crizia María
163. Porcel Cornejo, Tely Bladimir
164. Poves Montero, Joyce Pamela
165. Prada Trujillo, Hans Herbert
166. Pretel Tinoco, Patricia Teresa
167. Prudencia Gallegos, Luz Gudelia
168. Puicón Che, Carlos Daniel

Q

169. Quiñones Quiñones, Adan Arturo Alexander
170. Quispe Andía, Mónica Fiorela
171. Quispe Ramírez, Rosa Elvira
172. Quispe Trejo, Mayra Alejandra
173. Quisquia Cárdenas, Stephanie Marissa

R

174. Ramírez Arias, Diego Jesús
175. Ramo Quispe, Adriana
176. Ramos Torres, Tamara Victoria
177. Ramos Lopinta, Elvia María
178. Rímac Narro, José Luis
179. River Vela, Diana
180. Rivera Rojas, Carlos Mariano
181. Rivero Moscoso, Ángel Renán
182. Rodríguez Carrillo, Karen Stefanie
183. Rodríguez Ríos, Sandra Milagros

184. Rodríguez Salinas, Sergio Enrique
185. Rodríguez Yupanqui, Sofía
186. Rodríguez Zumaeta, Ricardo Santiago
187. Román Palomino, Karin Nilda
188. Romano Vergara, Natalia Alessandra
189. Romo Quisé, Adriana
190. Ruiz Quispe, Diana Elsa
191. Ruiz Ramos, Elva Irene

S

192. Saavedra Gutiérrez, Tomás Jaime Arturo
193. Sacsa Tello, Eva Yushara
194. Salas Fernández, Andrés Edgardo
195. Salazar Mesías, Gary Octavio
196. Salazar Tarazona, Christian Michel
197. Salazar Vallejo, Renzo Javier
198. Salazar Verdi, Sandy Carmen
199. Salinas Lau, Javier Augusto
200. Salvatierra Sinche, Jordano Antonio
201. Sanchez Yaringaño, Gadwyn
202. Sánchez Povis, Lucio
203. Santillán Espinoza, Jessica Victoria
204. Santos Loyola, Carlos
205. Scapa Passalacqua, Daphne
206. Seminario Córdova, Renzo Jean Pierre
207. Shimabukuro Tokashiki, Néstor Raúl
208. Silva Jáuregui, Claudia Giuliana
209. Silvestre Bermúdez, Julia Katty
210. Sinche Salvatierra, Isis Milagros
211. Sinche Salvatierra, Jordano Antonio
212. Solis Curi, Erika Patricia
213. Soto Huerta, Alexander Palermo
214. Suárez Blanco, Walter Gabriel
215. Suca Concha, Alejandro

T

216. Tam Mendiola, Marcia
217. Tantalean Leóng, Mónica Gabriela
218. Tena Mucha, Marely Luceta
219. Toledo Asenjo, Cesar
220. Tomaylla Catacora, Juan Victor
221. Torres Gamboa, Gerardo Santos
222. Torres Otoya, Franco Aníbal Abel
223. Trujillo Castañeda, Pamela
224. Tullume Carrión, Giovanna Elizabeth

U

- 225. Ulffe Carrera, Jessica De Luren
- 226. Ulloa Zegarra, Sylvia Karina
- 227. Umezagua Makikado, Angie Carolina
- 228. Uribe Almeida, María Pía
- 229. Urrutia Aliano, Luis Eduardo

V

- 230. Valencia Sáenz, Krystal del Carmen
- 231. Valdez Reyes, Laura Rosa
- 232. Vargas Antonio, Héctor Diego
- 233. Vargas Tacuri, Victor David
- 234. Vásquez Flores, Luis Ángel
- 235. Vega Gutiérrez, Jesús Andrés
- 236. Velásquez Ipanaqué, Claudia Katherine
- 237. Velazco Yábar, Alessandro Carlo André
- 238. Vera Torrejón, José Antonio
- 239. Vergaray De La Cruz, Marta Yolanda
- 240. Vigil Martínez, Lourdes María Esther
- 241. Vilca Pulgar, Ericka Elizabeth
- 242. Vilela García, Luis Fernando
- 243. Villa Castillo, Rosa María
- 244. Villegas Vega, Paul Nicolás
- 245. Villegas Vega, Pedro
- 246. Villegas Calderón, César Pool

W

- 247. Wong Vargas, Christian Fernando

Z

- 248. Zambrano Olivera, Elisa Pamela
- 249. Zúñiga Díaz, Giuliana Gabriela