

CONSTITUCIÓN, DERECHOS FUNDAMENTALES, INTELIGENCIA ARTIFICIAL Y ALGORITMOS

CONSTITUTION, FUNDAMENTAL RIGHTS, ARTIFICIAL INTELLIGENCE AND ALGORITHMS

César Landa Arroyo*

Miembro del Consejo Consultivo de THĒMIS
Pontificia Universidad Católica del Perú
Universidad Nacional Mayor de San Marcos

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

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

KEYWORDS: *Constitution; fundamental rights, technology; artificial intelligence; algorithms.*

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

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

PALABRAS CLAVE: *Constitución; derechos fundamentales; tecnología; inteligencia artificial; algoritmos.*

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

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

A la Generación Bicentenario

I. INTRODUCCIÓN

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

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

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

Todo ello se basa, en particular, en el desarrollo de la inteligencia artificial, la cual permite que un algoritmo se exprese en un lenguaje de programación para así realizar actividades registradas y procesadas por máquinas inteligentes (computadoras). Es decir, una máquina reemplaza las funciones cognitivas de los funcionarios del Estado

o los empleados de las empresas, maximizando sus objetivos y tareas. Así, en este proceso, las máquinas inteligentes sustituyen las capacidades humanas para percibir, razonar, decidir, aprender y resolver problemas, realizando una interpretación adecuada de los datos captados y procesados.

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

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

II. CONSTITUCIÓN E INTELIGENCIA ARTIFICIAL

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

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

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

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

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

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

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

(iv) una base de datos, en la cual se indexan todos los contenidos (Posicionamiento MX, 2014).

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

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

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

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

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

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

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

III. DERECHOS FUNDAMENTALES Y ALGORITMOS

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

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

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

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

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

A. Debido proceso

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

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

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

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

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

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

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

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

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

B. Derecho a un recurso efectivo

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

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

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

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

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

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

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

sonales. Ante ello, la ANTAIP concluyó que la difusión de aquella información mediante el motor de búsqueda debía cesar.

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

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

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

C. Privacidad y datos personales

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

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

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

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

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

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

Un algoritmo sesgado que discrimina sistemáticamente a un grupo en la sociedad –por ejemplo, en función de la edad, orientación sexual, raza, género o posición socioeconómica–, puede generar afectaciones considerables tanto en términos del acceso a los derechos de los usuarios o clientes afectados por estas decisiones, como también para la sociedad en su conjunto. Al respecto, se

podría argumentar que toda persona debe tener derecho a tener acceso a su perfil digital, en una versión ‘neutral’ de sus resultados de búsqueda.

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

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

D. Libertad de expresión

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

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

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

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

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

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

nar las incitaciones al odio; en consecuencia, se requiere de la armonización de la legislación europea (Valero, 2017).

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

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

E. Derecho a elecciones libres

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

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

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

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

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

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

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

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

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

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

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

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

F. Libertad de asociación y reunión

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

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

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

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

G. Derecho a la igualdad y prohibición de discriminación

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

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

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

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

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

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

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

H. Derecho al trabajo y acceso a los servicios públicos

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

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

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

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

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

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

IV. CONCLUSIONES

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

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

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

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

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

REFERENCIAS

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

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

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

Collosa, A. (8 de febrero de 2021). Algoritmos, sesgos y discriminación en su uso: A propósito de recientes sentencias sobre el tema. *Centro Interamericano de Administraciones Tributarias*

(CIAT). <https://www.ciat.org/ciatblog-algoritmos-sesgos-y-discriminacion-en-su-uso-a-proposito-de-recientes-sentencias-sobre-el-tema>

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

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

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

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

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

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

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

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

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

- Innerarity, D. (2020). El impacto de la inteligencia artificial en la democracia. *Revista de las Cortes Generales*, (109), 87-103. <https://doi.org/10.33426/rcg/2020/109/1526>.
- Landa, C. (2019). Contenido esencial del derecho fundamental al Internet: Teoría y praxis. En C. Landa (ed.), *Libro de Homenaje del Área de Derecho Constitucional por los 100 años de la Facultad de Derecho de la Pontificia Universidad Católica del Perú*. Pontificia Universidad Católica del Perú.
- (2021). *El derecho fundamental a la igualdad y no discriminación en la jurisprudencia del Tribunal Constitucional del Perú*. Tribunal Constitucional del Perú.
- López, S. (25 de noviembre de 2019). Facebook y el fin de la libertad de expresión. *El Juego de la Suprema Corte*. <https://eljuegodelacorte.nexos.com.mx/?p=10573>
- López Takeyas, B. (2007). *Introducción a la Inteligencia Artificial*. Instituto Tecnológico de Nuevo Laredo. <http://itnuevolaredo.edu.mx/takeyas/Articulos/Inteligencia%20Artificial/ARTICULO%20Introduccion%20a%20la%20Inteligencia%20Artificial.pdf>.
- Magallón Rosa, R. (4 de mayo de 2018). Leyes ‘fake news’: El problema para la libertad de información de no legislar. *Telos Fundación Telefónica*. <https://telos.fundaciontelefonica.com/las-leyes-las-fake-news-problema-la-libertad-informacion-no-legislar/>.
- Medrano, H. (28 de noviembre de 2020). La historia de un “hashtag” en los días más intensos. “Generación del bicentenario” fue la frase más usada en Twitter en protestas. *Grupo de Diarios América*. <http://gda.com/detalle-de-la-noticia/?article=4247897>.
- Navas, S., Górriz, C., Camacho, S., Robert, S., Castells, M., & Borge, I. (2017). *Inteligencia artificial, Tecnología, Derecho*. Tirant lo Blanch.
- Ortega, M. (2015). *Prestadores de servicios de Internet y alojamiento de contenidos ilícitos*. Editorial Reus.
- Palma Ortigosa, A. (2019). Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos. *Revista General de Derecho Administrativo*, (50).
- Ponce, J., & Torres, A. (2014). Introducción y Antecedentes de la Inteligencia Artificial. En *Inteligencia Artificial*. Iniciativa Latinoamericana de Libros de Texto Abiertos. <http://dx.doi.org/10.13140/2.1.3720.0960>
- Posicionamiento MX (23 de mayo de 2014). ¿Cómo funcionan los motores de búsqueda?. *Posicionamiento MX*. <https://www.posicionamiento.mx/blog/seo/como-funcionan-los-motores-de-busqueda>.
- Roig, A. (2020). *Las garantías frente a las decisiones automatizadas: Del Reglamento General de Protección de Datos a la gobernanza algorítmica*. J.M. Bosch. <https://doi.org/10.2307/j.ctv1dv0v54>.
- Roose, K. (7 de enero de 2021). The President Is Losing His Platforms. *The New York Times*. <https://www.nytimes.com/2021/01/07/technology/trump-social-media.html>.
- Sainz, M., Arroyo, L., & Castaño, C. (2020). *Mujeres y digitalización. De las brechas a los algoritmos*. Red.es. Ministerio de Asuntos Económicos y Transformación Digital (coords.). DOI: 10.30923/MujDigBreAlg-2020.
- Sánchez, A. (2016). *Reflexiones de un replicante legal*. Thomson Reuters Aranzadi.
- Tene, O., & Polonetsky, J. (2012). To Track or “Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising. *Consortium on Law and Values in Health, Environment & the Life Sciences*, 13(1).
- Tufekci, Z., York, J., Wagner, B., & Kalthuener, F. (2015). *The Ethics of Algorithms: From Radical Content to Self-Driving Cars*. European University Viadrina Frankfurt. <https://cihr.eu/publication-the-ethics-of-algorithms/>.
- Ureña, L., & De Buenaga, M. (1999). Utilizando WordNet para Complementar la Información de Entrenamiento en la Identificación del Significado de las Palabras. *Inteligencia Artificial*, 3(7).
- Valero, A. (10 de enero de 2017). ¿La libertad de expresión en manos de un algoritmo? [Entrada de blog] *Al revés y al Derecho*. <http://blogs.infolibre.es/alrevesyalderecho/?p=4805>
- Wagner, B. (2016). *Global Free Expression: Governing the Boundaries of Internet Content*. Springer International Publishing.
- Xu, B. (2019). Algorithm regulation under the framework of human rights protection. *The Journal of Human Rights*, 18(4).

LEGISLACIÓN, JURISPRUDENCIA Y OTROS DOCUMENTOS LEGALES

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

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

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

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

Directiva 2020/1828 del Parlamento Europeo y del Consejo de 25 de noviembre de 2020 relativa a las acciones de representación para la protección de los intereses colectivos de los con-

sumidores, y por la que se deroga la Directiva 2009/22/CE, 2020 O.J. (L409)1 (UE).

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

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

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

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