Derechos digitales en Iberoamérica:
situación y perspectivas

Fundación Carolina y Telefónica

Derechos digitales en Iberoamérica:
situación y perspectivas

Fundación Carolina
Telefónica

Renata Ávila
Janaina Costa
Celia Fernández-Aller
J. Carlos Lara Gálvez
Santiago Nardini
Camilla Roveri
María Mercedes Serrano Pérez
Carlos Affonso Souza

PRÓLOGO DE
Trinidad Jiménez y José Antonio Sanahuja

Fundación Carolina

Fundación Carolina, marzo 2023

Fundación Carolina
Pza. del Marqués de Salamanca, 8
4ª Planta. 28006 Madrid - España
www.fundacioncarolina.es
@Red_Carolina

ILUSTRACIÓN DE PORTADA:
Sebastián Guzmán
(exbecario de la Fundación Carolina)

REALIZACIÓN GRÁFICA:
Calamar Edición & Diseño

ISBN: 978-84-09-49022-6
Depósito Legal: M-8241-2023

Con la colaboración de

Telefónica

Índice

Prólogo

Trinidad Jiménez
José Antonio Sanahuja[*]

Telefónica y Fundación Carolina presentan, con este volumen, los resultados de la segunda edición de su programa de estudios "Digitalización inclusiva y sostenible en América Latina". Se trata de una línea de actividad centrada en la investigación y el análisis que, en esta oportunidad —y tras el enfoque multidimensional con el que se inauguró el programa—, ha querido detenerse a examinar la situación de los derechos digitales en Iberoamérica. Bajo la lógica de una transformación digital que, según defendemos ambas instituciones, debe acompasarse con una transición medioambientalmente sostenible y socialmente justa, es necesario valorar y analizar posibles acciones normativas que respondan a los retos éticos, económicos y de cohesión social que la digitalización suscita.

Así, de hecho, se ha venido entendiendo en tiempos recientes desde la Unión Europea —haciendo valer su marchamo de "potencia reguladora", según la expresión de Anu Bradford— y, no cabe olvidar, también desde la experiencia singular de varios países de la región latinoamericana. Ello se refleja, por parte de la UE, en la aprobación en 2016 del Reglamento General de Protección de Datos (RGPD), secundada en 2022 por la Ley de Servicios Digitales, la Ley de Mercados Digitales, y la Declaración Europea sobre los Derechos y Principios Digitales, entre otras iniciativas. En este plano, merece recordarse la Carta de Derechos Digitales que, ya en julio de 2021, presentó el Gobierno de España para dotar de un marco de referencia al desarrollo regulatorio y al diseño de políticas públicas en dicho ámbito. Por su parte, en América Latina, hay que des-

* Trinidad Jiménez es directora de Estrategia Global de Asuntos Públicos en Telefónica. José Antonio Sanahuja es director de la Fundación Carolina.

tacar el precedente que supuso la adopción en 2014 del Marco Civil de Internet en Brasil, así como los debates legislativos, igualmente pioneros, por incorporar la protección de los "neuroderechos" en Chile, o el lanzamiento de estrategias nacionales para regular la inteligencia artificial (IA) en países como Argentina, Uruguay o Perú. A todo ello hay que agregar la aprobación, en marzo de 2023, de la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales en la XXVIII Cumbre Iberoamericana de jefes y jefas de Estado y de Gobierno en República Dominicana.

Estos hitos plasman la convergencia, en clave democrática, de respeto a los derechos humanos y al imperio de la ley, que desde un punto de vista histórico unen a Europa y América Latina. Justamente, a partir de este vínculo humanista —en un contexto de incertidumbre económica, auge de rivalidades geopolíticas y conflictividad bélica—, la UE y la Comunidad de Estados Latinoamericanos y Caribeños (CELAC) han incluido entre sus prioridades el establecimiento de una Alianza Digital que intensifique sus relaciones institucionales y tecnológicas[1]. Dentro de ellas —además del impulso en infraestructuras, conectividad, seguridad cibernética o alfabetización digital— la dimensión regulatoria ocupa un importante lugar, pero todavía incipiente; de ahí la pertinencia de articular un proyecto de estudio que ofreciera un panorama de situación actualizado sobre los derechos digitales en Iberoamérica.

Para ello, acudimos a una de las mayores especialistas en la materia, la profesora de la Universidad Politécnica de Madrid, Celia Fernández-Aller —copartícipe en la redacción de la citada Carta española—, cuyo perfil jurídico incorpora un amplio bagaje en estudios sobre desarrollo y cooperación internacional. Bajo su coordinación académica, se gestó un equipo multidisciplinar de colaboradores/as que, partiendo de los puntos nodales que aglutina esta nueva generación de derechos —la protección de la privacidad, el uso ético de la IA, la libertad de expresión, las brechas digitales o la apertura digital de las Administraciones públicas a la participación cívica— ha hecho posible el presente volumen.

Este se inicia con un estudio sobre la protección de los datos personales en defensa de la dignidad individual, firmado por la profesora de Derecho Constitucional de la Universidad de Castilla-La Mancha, María Mercedes Serrano. En él se da cuenta de cómo, en el espacio digital, la información a la que acceden

[1] Véanse el Comunicado y la Hoja de Ruta lanzados tras la reunión ministerial UE-CELAC, de 27 de octubre de 2022: https://www.consilium.europa.eu/media/59827/celac-eu-fmm-joint-communique.pdf y https://www.consilium.europa.eu/media/59838/hoja-de-ruta-celac-ue-2022-2023-final.pdf

los sectores público y privado, aun en su propósito de proveer mejores servicios e incrementar el bienestar, puede generar riesgos sobre los derechos fundamentales de la ciudadanía. De este modo, el capítulo aborda los impactos planteados por las tecnologías en la privacidad, e introduce una visión pormenorizada sobre las distintas políticas en protección de datos puestas en marcha en la región. A continuación, la coordinadora del proyecto, junto a sus ayudantes, Camilla Roveri y Santiago Nardini, analiza el uso ético de la IA y las "neurotecnologías", haciendo hincapié en la exigencia de que incorporen el enfoque de derechos humanos en su diseño, desarrollo e implementación, esto es, poniendo a las personas en el centro de las propuestas. El capítulo contempla una detenida reflexión sobre los desafíos conceptuales que la innovación tecnológica ejerce sobre las corrientes del pensamiento y los modelos de convivencia social, y profundiza asimismo en el papel de los derechos digitales relacionados con la IA, identificando buenas prácticas de políticas en ejercicio, que equilibran respeto ético y aplicaciones de tecnología avanzada.

El tercer capítulo, suscrito por el codirector ejecutivo de la organización Derechos Digitales de Chile, J. Carlos Lara, examina la acuciante cuestión de la libertad de pensamiento y el derecho a una información veraz ante la desinformación y las *fake news*, recordando cómo la expansión de las posibilidades de comunicación representa una de las consecuencias más evidentes del enorme crecimiento del acceso a internet. Pues bien, debido precisamente a la ampliación de las capacidades para ejercer dichas libertades, ha aumentado de igual forma la aparición de expresiones legalmente ilícitas o socialmente dañinas. Sin perjuicio de la necesidad de afrontar tales retos, el texto no deja de subrayar las circunstancias de un contexto regional que, ya en el mundo analógico, a menudo oprime el desarrollo de la libertad de expresión y que puede verse extendido, e incluso exacerbado, en el entorno digital. Seguidamente, el artículo de Carlos Affonso Souza y Janaina Costa, del prestigioso Instituto de Tecnología y Sociedad de Río, expone el modo en el que se han articulado en América Latina diversas políticas digitales por medio de mecanismos de participación cívica, y demuestra que estos modelos —aun con todas sus dificultades técnicas— aportan más soluciones y mejores conocimientos a los dilemas que implica la digitalización, incrementando además la confianza de las sociedades sobre la labor de sus gobiernos. A su vez, el texto revisa el surgimiento de declaraciones de derechos digitales en varios países, con especial énfasis en la experiencia sudamericana que plasman los casos de Brasil y Perú, y subraya la importancia de hacer un uso adecuado de tecnologías modernas para que la gestión pública

gane en eficiencia y calidad democrática. Por último, Renata Ávila, CEO de Open Knowledge Foundation, cierra el volumen abordando los efectos de la brecha digital: estos, en primera instancia, afectan negativamente a los colectivos más vulnerables, pero además pueden incrementar el grado de desigualdad entre países y regiones. Para afrontar esta situación, su texto postula que las nuevas normativas no pueden limitarse a proteger los derechos humanos y fundamentales (de privacidad, expresión, igualdad, etc.), sino que deben extenderse a derechos como los de competencia o de protección a los consumidores. Por lo demás, la autora sostiene que los países latinoamericanos, en lugar de implementar políticas aisladas, han de coordinar sus esfuerzos para construir una verdadera agenda regional, más autónoma, que incluso pueda contribuir a alumbrar una nueva arquitectura digital.

Una vez cerrada esta segunda edición, el programa de "Digitalización inclusiva y sostenible" ha quedado consolidado, de modo que Telefónica y Fundación Carolina continúan su trabajo conjunto, abriendo líneas de investigación orientadas a generar conocimiento experto sobre un proceso de transformación productivo y cultural, en su sentido más amplio, que no ha hecho más que empezar. Las novedades y ritmos de innovación —tan vertiginosos como en ocasiones ininteligibles, entre los que ya se cuentan los sistemas de aprendizaje profundo como ChatGPT, la evolución del metaverso o las amenazas del *deep fake*—, nos obligan a identificar y desentrañar constantemente las claves tecnológicas que están delineando un futuro todavía por definir. Pero de lo que no cabe duda es de que, en esta tarea, las alianzas público-privadas resultan imprescindibles, y que el porvenir de los principios e instituciones democráticos pasa por que los lazos euro-latinoamericanos sigan estrechándose, poniendo los intereses de la ciudadanía y sus derechos en el centro de estas cuestiones.

1. La protección de los datos personales en defensa de la dignidad individual ante los riesgos de pérdida de privacidad

*María Mercedes Serrano Pérez**

1. Introducción

La cuarta revolución industrial tiene en la tecnología, y su introducción y extensión en la sociedad, sus señas de identidad más identificativas. La tecnología ha revolucionado la vida y las relaciones sociales. Se emplea el concepto *sociedad digital* para identificar la sociedad que se desenvuelve en su labor rutinaria con apoyo de la tecnología digital y utiliza grandes volúmenes de datos para desarrollar sus múltiples tareas. La digitalización social ha de contribuir a "fortalecer las instituciones democráticas, mejorar la productividad, estrechar las disparidades sociales y de género, formar en competencias tecnológicas, y garantizar la sostenibilidad medioambiental" (Fundación Carolina y Telefónica, 2021: 6). Algunos de los procesos tecnológicos en los que nos vemos envueltos a diario emplean datos personales, por ejemplo, los procesos de inteligencia artificial (IA), aunque quepa remarcar que muchas aplicaciones de la IA no usan datos personales. Por otra parte, todos o casi todos los trámites administrativos de relación de la Administración con los ciudadanos se realizan de modo telemático. Utilizamos la tecnología y el tratamiento de datos personales buscando un beneficio individual y/o colectivo. En este contexto tecnológico, tanto los po-

* Profesora doctora de Derecho Constitucional en la Universidad de Castilla-La Mancha (UCLM).

deres privados como el poder público pueden acceder a un conocimiento de informaciones personales cuyo tratamiento ha de tender siempre a mejorar la calidad de vida de los ciudadanos. Pero el uso de la tecnología puede también convertirse en una amenaza para la dignidad de la persona y el ejercicio de sus derechos fundamentales. El tratamiento de la información personal puede perjudicar el ejercicio de nuestras libertades y nuestro modelo de vida.

La actividad tecnológica no es un fenómeno transitorio y excepcional sino permanente, a veces intrusivo e irreversible en cuanto a sus logros. La finalidad de los avances tecnológicos de mejorar la vida de los ciudadanos propicia que su aplicación y su utilización en todos los sectores sociales se incremente y convierta la tecnología en una herramienta imprescindible en la sociedad digital. Precisamente, la omnipresencia tecnológica y su necesaria permanencia entre nosotros demandan una regulación jurídica adecuada para que —por la afectación de los adelantos técnicos a todos los elementos de la sociedad y por su incidencia directa en la persona— no pueda provocar, como un posible efecto secundario, la vulneración de los derechos de los individuos. Ello porque también los derechos se ven sacudidos por la revolución tecnológica y requieren, para mantener su esfera de protección, una reconstrucción desde el enfoque de la tecnología. El derecho, por tanto, ha de intervenir para extender de manera igualitaria el uso de la tecnología, dotarla de accesibilidad y al tiempo proteger a los ciudadanos de las posibles amenazas que puede representar para los derechos del individuo. La Constitución española recoge esta mediación legal en su art. 18.4 en relación con la informática, aunque con una insatisfactoria redacción, pero eleva dicha previsión, no lo olvidemos, a categoría de derecho fundamental. También la ética debe estar presente en los procesos tecnológicos, puesto que los nuevos desarrollos y aplicaciones pueden plantear retos relevantes que deben evaluarse y analizarse para construir un futuro alienado con nuestros valores. Además, en la labor de extender el empleo de la tecnología y facilitar su accesibilidad, el poder público y el poder privado deberían actuar y planificar estrategias comunes y convergentes, teniendo siempre en cuenta a las personas y a sus derechos fundamentales.

La privacidad en el entorno digital adquiere una dimensión especial cuando situamos a la persona frente al uso de las tecnologías. La privacidad reconoce el derecho de los ciudadanos a controlar sus informaciones personales y decidir acerca del uso de los datos que se refieren al individuo. Alcanza igualmente la protección de todos los aspectos de la vida privada que en el entorno tecnológico adquieren una nueva dimensión (Naciones Unidas, 2018): la iden-

tidad digital, la seudonimización, la elaboración de perfiles, etc. La protección también alcanza a los metadatos por la información que pueden aportar. Los riesgos a gran escala para la protección de los datos personales podrían provenir, entre otras, del Big Data y de los procesos de IA cuando en algunos casos utilizan datos personales para ofrecer el resultado solicitado. La seudonimización de los datos no garantiza de forma total la protección de la persona, pues la reidentificación es casi siempre posible, aunque es un proceso complejo. El único impedimento real a la identificación podría provenir —además de la intervención legal y de la aplicación de criterios éticos— de una imposibilidad motivada por criterios económicos o temporales y sobre todo técnicos, que en algunos casos también podrían ser derribados.

El derecho a la privacidad es un derecho que pertenece a la persona. Todos los individuos tenemos presencia digital, mayor o menor, pues nuestra vida y actividades se ven reflejadas y almacenadas en forma digital. El Estado recoge y trata los datos de los ciudadanos para desempeñar la actividad pública que tiene atribuida, pero también los poderes privados recaban datos para ofrecer servicios y captar clientes. Además, la privacidad en el entorno digital no solo ofrece una vertiente individual, sino que desde la perspectiva colectiva el dato adquiere un valor y una dimensión que no pueden ser obviados por las normas reguladoras. Junto a su valía para el conjunto de la sociedad, el dato personal incorpora un valor económico que influye poderosamente en la actividad económica y empresarial.

La extensión y generalización de la tecnología será posible siempre y cuando el poder público asuma como obligación del Estado determinadas exigencias que vienen de la mano del Estado social digital y que obligan al poder público a actuar para intentar eliminar los obstáculos que puedan quebrar la igualdad real, desde una perspectiva tecnológica. A modo de ejemplo: en la sociedad digital la extensión de la digitalización a todos los sectores sociales y la capacitación digital deben formar parte de la educación obligatoria a través de la incorporación de contenidos digitales al sistema educativo. En este sentido, las cartas de derechos digitales ponen el acento tanto en los derechos surgidos al amparo de los avances tecnológicos, como en una adaptación de los derechos clásicos a la nueva realidad.

Junto a ello, el poder público debe asumir la obligación de extender la cultura de la protección de datos a los ciudadanos, a las empresas y a la propia Administración, así como emprender acciones para facilitar el control de los datos personales en manos ajenas, también en poder del Estado. Y es que el Estado dispone —a través del tratamiento de la información personal— de una potencial vía para invadir el espacio individual cuya protección corresponde al ser humano por

medio del reconocimiento de los derechos fundamentales de la personalidad. Pero también las empresas y entes privados almacenan y manejan datos personales, y pueden provocar agresiones a los derechos fundamentales. Por tanto, proteger la privacidad es esencial para la protección de los derechos fundamentales, tanto dentro como fuera de internet. El ciudadano no puede volverse vulnerable ante la convivencia irreversible, necesaria y deseable con la tecnológica.

En una sociedad cada vez más digitalizada y con una necesidad más evidente de aceptar el tratamiento de sus datos de forma natural, el individuo no puede quedar alejado y a veces despreocupado de la protección y del cuidado de sus informaciones personales.

2. La protección de la privacidad y la protección de datos en la cuarta revolución industrial

La vida privada y la intimidad de la persona quedan protegidas en una sociedad analógica a través del derecho a la vida privada. El objeto del derecho es proteger del conocimiento ajeno los actos privados o íntimos a través de facultades que impiden o corrigen una injerencia externa no deseada. La vida privada protege, dentro de un círculo imaginario que traza el titular del derecho, los actos que veta así a la indiscreción de terceros. Las acciones de tutela del derecho a la vida privada o a la intimidad actúan impidiendo las injerencias no deseadas, tanto del resto de ciudadanos como de los poderes públicos. La vida privada es más amplia que la intimidad.

La sociedad digital ha extendido la tecnología a todos los sectores sociales y su reto es ponerla al alcance de toda la sociedad para que pueda cumplir su finalidad real de mejorar la vida de los ciudadanos. Para que la tecnología pueda lograr dicho objetivo necesita, en una gran mayoría de sus intervenciones (educación, salud, ocio, trabajo, comercio, etc.), realizar tratamientos de datos de carácter personal. El tratamiento de datos de carácter personal resulta imprescindible en la sociedad digital datalizada.

Los datos de carácter personal recogen en forma de informaciones facetas de nuestra vida que nos pertenecen y que en la sociedad digital son tratadas a través de procedimientos tecnológicos, esto es, son objeto de tratamiento. El tratamiento de la información personal puede lesionar el derecho a la vida privada, a la intimidad o incluso dañar el ejercicio del resto de los derechos de la persona, si no se somete a reglas jurídicas. Por ello, proteger los datos persona-

les que son objeto de tratamiento es el modo de proteger la libertad de la persona y el ejercicio de sus derechos en la sociedad tecnológica. Pero el derecho a la protección de los datos personales no tutela solamente los datos que guardan relación con la vida privada, sino cualquier información que pertenezca al círculo de la intimidad o no, o al círculo de la vida privada. Se protegen los datos personales, con independencia de su carácter privado o íntimo. Incluso los datos ya publicados o los datos que son objeto de intercambio público también han de ser objeto de amparo y protección.

Proteger los datos personales en la cuarta revolución industrial, la que viene de la mano de la sociedad digital, es proteger a la persona ante un uso incorrecto de la tecnología. La relación entre el ser humano y la tecnología ha de ser armónica y amable.

3. Los impactos positivos y negativos de la tecnología en los derechos de las personas

La tecnología ha impactado en el ejercicio de los derechos fundamentales. La vida de la persona se proyecta ahora en forma de datos que reflejan la salud del sujeto, sus gustos, trabajo, preferencias, relaciones, estudios, etc. Toda esa información forma parte de contextos digitales, cuyas posibilidades de transmisión y tratamiento superan los límites del tiempo y del espacio, lo que obliga a protegerse frente a las amenazas que podría generar la acumulación de la información. Almacenar todos estos datos personales puede constituir un riesgo para la persona por la posible pérdida de control sobre ellos, esto es, por la pérdida de dominio sobre la propia vida. Si a la capacidad de almacenar información unimos su tratamiento para obtener resultados, la vida privada necesita una protección reforzada o específica ante la utilización de la tecnología en lo que atañe a los datos personales. La posible amenaza se puede proyectar sobre el conjunto de los derechos del individuo. Las personas pueden encontrarse desprotegidas ante el empleo masivo de la tecnología que maneja información personal.

La capacidad de penetración de la tecnología es inmensa y supera la limitación que presentaban los instrumentos analógicos hasta ahora existentes y empleados en cualquier campo. Precisamente dicha capacidad tiene efectos beneficiosos, pues mejora la calidad de vida de las personas y ofrece más y mejores servicios a los ciudadanos (biotecnología, telecomunicaciones, IA, economía, etc.). Pero el manejo de una gran cantidad de información personal

también incrementa la facilidad —tanto del sector público como de las empresas— para vigilar a los ciudadanos, analizar y predecir su comportamiento e incluso manipularlo. Las consecuencias de las aplicaciones de la tecnología "inciden directamente en la conducta de la persona, en su individualidad y en la sociedad en su conjunto, pero también en la democracia y el mercado, así como en la capacidad de los individuos y sociedad para elegir y decidir. También por supuesto en los derechos fundamentales" (De la Quadra-Salcedo Fernández del Castillo, 2019: 2).

Tanto el Estado como el sector empresarial utilizan cada vez con mayor frecuencia datos biométricos en el ámbito laboral, como la voz, la huella dactiloscópica, la geometría facial etc., que tienen la consideración de datos personales. La recogida y tratamiento de datos biométricos puede facilitar labores legales de vigilancia y seguridad. Pero el tratamiento de estos datos también puede resultar un peligro si se emplearan para fines distintos de los legítimos para los que fueron recogidos y tratados, porque aportarían información relevante de las personas.

La acumulación de datos personales puede ofrecer, en determinados casos, un perfil de la personalidad del sujeto. La elaboración de un perfil es el resultado de la aplicación de la IA y está regulada por las normas de protección de datos. La legislación sobre protección de datos proscribe que una persona pueda ser objeto de una decisión automatizada basada exclusivamente en la elaboración de perfiles, de manera que produzca efectos jurídicos o le afecte significativamente.

La IA puede utilizar datos personales en alguno de sus procedimientos. Su empleo obliga a someter estos procesos a la normativa de protección de datos para no provocar daños en los derechos de la persona. El sujeto puede sufrir las consecuencias derivadas de la intervención de la IA sin llegar a conocer, en algunos casos, el origen del perjuicio debido a la opacidad que rodea estos sistemas. Algunos dispositivos basados en inteligencia artificial recogen de manera masiva datos personales de forma imperceptible para nosotros, por tanto, sin nuestro conocimiento ni consentimiento (Fernández-Aller y Serrano Pérez, 2022).

El impacto negativo del empleo de datos personales en los derechos de los individuos puede provenir también de la falta de transparencia de los tratamientos de datos, así como de la quiebra de las medidas técnicas de seguridad que han de reunir los tratamientos.

En todo caso, los avances tecnológicos en el tratamiento de la información incorporan también medidas de protección para los derechos de las personas que las normas recogen cada vez con mayor precisión. Supone un adelanto importante la consideración de la protección de datos como derecho fundamental,

pero, junto a ello, debemos elaborar normas garantistas para el sujeto que regulen de manera minuciosa tanto los derechos y principios como las medidas de seguridad, intervención de las autoridades de control, mecanismos de defensa, etc.; todo el contenido material que asegure una auténtica protección frente al progreso tecnológico, sin renunciar tampoco a sus bondades (Murillo de la Cueva, 2009: 133). De nuevo incidimos en la necesidad de colaboración entre el sector público y el privado en este ámbito.

4. Las políticas públicas de los Estados para responder a los retos que plantea la tecnología

El reto principal del poder público se bifurca en una doble dirección. Por una parte, el poder público debe desplegar actuaciones para regular el uso de la tecnología y hacerlo teniendo en cuenta el respeto a los derechos de la persona, esto es, el legislador debe elaborar normas que busquen equilibrar la tecnología y el ejercicio de los derechos de la ciudadanía. Proteger el ejercicio de los derechos de los sujetos, su libertad y dignidad son pilares esenciales en un Estado de derecho y en una sociedad democrática. Por otro lado, las acciones deben dirigirse a extender el uso de la tecnología a todos los ciudadanos en condiciones de igualdad. El acceso universal a internet, la neutralidad en la red, etc., son derechos digitales que ahora obligan al Estado a actuar en esa dirección, a incorporar acciones para asegurar la digitalización social. Y el sector privado asume un papel relevante y responsable en esta nueva realidad.

La generalización de la tecnología ha de llevarse a cabo fomentando la educación digital tanto en competencias digitales como en un uso responsable de la misma y al tiempo extender la cultura de la protección de datos a todos los niveles educativos y a todos los ciudadanos. En la sociedad digital todos los ciudadanos tenemos que ser vigilantes de nuestra información personal porque también puede comprometer el ejercicio de los derechos de los demás.

La regulación del uso de la tecnología de modo respetuoso con los derechos de los ciudadanos demanda leyes que respondan a estándares y principios internacionales. En Europa, el Reglamento General de Protección de Datos (RGPD) está cumpliendo la misión de crear un espacio europeo de datos con legislaciones uniformes. El deseo de Europa de convertirse en líder tecnológico y de importar los principios de protección de datos de su normativa se hace realidad en las legislaciones de América Latina, donde las más recientes reformas legis-

lativas y la nueva oleada de normas de protección de datos se están elaborando bajo la clara influencia de la legislación europea.

La actividad pública desarrollada en dichas coordenadas —y que es necesaria para hacer frente al reto informático— exige un determinado modelo de organización jurídico constitucional que afecta a los poderes del Estado y a las reglas por las que se rige la actuación de dichos poderes. La estructura jurídica organizativa que mejor puede regular e impulsar la tecnología y proteger los derechos de los ciudadanos es la que ofrece el Estado social y democrático de derecho, por varias razones que sintéticamente señalamos:

· La constitución de estos Estados se ha convertido en la norma suprema de los ordenamientos jurídicos y tiene carácter normativo, es decir, tiene eficacia directa. Entre sus contenidos incluye un conjunto de derechos que son inherentes a la persona y que tienen carácter fundamental. También recoge los instrumentos que permiten proteger estos derechos y que constituyen el sistema de garantías establecido para restaurarlo en caso de lesión. Entre los derechos fundamentales se encuentra el derecho a la vida privada y el derecho a la protección de datos de carácter personal. La inclusión de este último en las constituciones y en la parte de los derechos fundamentales constituye un signo evidente de su relevancia y de la necesidad de tutelarlo frente a las posibles agresiones de la tecnología.

· La existencia de leyes que desarrollen el derecho a la protección de datos aporta seguridad jurídica a los ciudadanos, a los poderes públicos y al sector privado, y traslada principios y criterios recogidos en normas superiores. Estas normas crean autoridades de protección de datos que velan por el cumplimiento de la legislación y establecen las condiciones de actuación de la tecnología.

· Las obligaciones sociales del Estado para extender la digitalización a todos los ciudadanos —sin distinción y de forma igualitaria para no generar desigualdades significativas— se incorporan al modelo de Estado actual. Las prestaciones digitales enfocadas hacia la tecnología quedan asumidas por el Estado social digital que ahora se ve obligado a intentar remover los obstáculos que, provenientes de la tecnología, pueden impedir la implantación de la igualdad real, por ejemplo, con el reconocimiento del derecho universal a internet, el derecho a la educación digital, etc.

Como decimos, en primer lugar, la normativa sobre protección de datos a elaborar por el legislador ha de proporcionar seguridad y ha de enmarcarse en un contexto global de utilización de los datos personales y de criterios seguros para responder a los nuevos retos planteados por el uso de la tecnología. Además, la aceptación de estándares comunes facilita la libre circulación de datos, lo que a su vez fomenta y consolida el crecimiento económico y las relaciones entre países. Junto a la normativa aplicable hay que destacar la autorregulación desarrollada por el sector privado, básicamente mediante la elaboración de códigos de conducta y principios de actuación dentro del marco legal vigente. Estos códigos y principios, promovidos desde la legislación europea, facilitan el cumplimiento de las leyes de protección de datos y constituyen herramientas válidas para garantizar los derechos de los ciudadanos y reforzar la seguridad de los tratamientos.

Las políticas públicas que se adopten para facilitar la protección de la privacidad han de ser transparentes y ser conocidas por los ciudadanos. Y, también, eficaces y eficientes.

Por ejemplo, en Chile, el Consejo para la Transparencia y la Universidad Adolfo Ibáñez lideran un programa que pretende afianzar la transparencia en operaciones de algoritmos en procesos de decisiones que manejan datos personales. La finalidad del Consejo es:

> velar por el derecho de cualquier persona a acceder a información que está en poder de instituciones públicas, lo que incluye transparentar en base a qué antecedentes y cómo toman las decisiones en el sector público, incluso cuando utilicen sistemas de decisiones automatizadas o semiautomatizadas, los cuales muchas veces pueden resultar opacos, desconocidos o complejos para una mayoría[1].

La iniciativa se enmarca dentro de la Ley de Transparencia que garantiza el acceso de los ciudadanos a la información pública. Dentro de la finalidad de transparencia, en Chile también destacan los intentos de reforzar la protección de datos frente a las técnicas de videovigilancia o reconocimiento facial[2]. La primera de ellas con

[1] Se constata que el 80% de los sistemas algorítmicos que usa el Estado no ofrece información ni sobre el funcionamiento ni sobre el origen de los datos, lo que puede resultar contrario al derecho a la protección de datos personales. Disponible en: https://www.consejotransparencia.cl/consejo-para-la-transparencia-y-universidad-adolfo-ibanez-lideran-piloto-en-organismos-publicos-para-inedita-normativa-en-transparencia-algoritmica-de-america-latina/ (consultado el 7 de noviembre de 2022).

[2] La protección de datos personales en contextos de avanzado desarrollo tecnológico, con énfasis en videovigilancia y tecnología de reconocimiento facial empleada por el sector público. Estudios de

fines de seguridad, mientras que la segunda, además de la seguridad, tiene una finalidad de controlar la asistencia laboral, las finanzas, el transporte, etc.

Dentro de la estructura estatal para abordar una protección de los ciudadanos frente al manejo de los datos personales queremos destacar la existencia de autoridades de control nacionales e internacionales, con la competencia general de velar por la aplicación de las normas sobre protección de datos y su correcto cumplimiento, lo que incluye la protección de los derechos de los ciudadanos. También tienen potestad sancionatoria.

Las autoridades nacionales de control deben adoptar, como labor constante exigida además desde la normativa en vigor, la tarea de extender la cultura de la protección de datos a la ciudadanía. Para ello pueden servirse de diferentes herramientas como seminarios, jornadas, participación en congresos y elaboración de guías dirigidas tanto al sector público (a las distintas Administraciones públicas) como al sector privado. Los actos de carácter más divulgativo y reflexivo deberían contar con expertos tanto nacionales como internacionales con el fin de poder conocer, compartir y armonizar los esfuerzos que se realizan en los diferentes países, ya sea de la región o europeos.

Las guías deberían ser prácticas e indicar todos los pasos a seguir en la aplicación de las medidas técnicas y de seguridad dirigidas a garantizar un tratamiento legal de datos que protejan los derechos de los ciudadanos. Eso por lo que respecta al tratamiento de datos por parte de la Administración pública y de las empresas; estas últimas asumen también una labor destacada en la difusión de la cultura de la protección de datos y en la aproximación de la misma al ámbito laboral. Sería una buena solución adoptar guías sectoriales, en especial en el sector público, de manera que el tratamiento de datos por parte de las distintas Administraciones públicas fuera objeto de un análisis y estudio particular. Es obvio que los principios generales y los derechos son de aplicación con independencia del sector, pero pueden existir matices, por ejemplo, el tratamiento de datos de salud, en educación, laborales, que las diferentes guías pueden abordar mejor si se dirigen especialmente a las distintas Administraciones públicas. La parte más teórica de las guías debe ser explicada con sencillez, transparencia y claridad. Se deberían elaborar también guías destinadas a los ciudadanos, cuyo contenido sea dar a conocer tanto los riesgos que conlleva el

---

transparencia. Disponible en: https://www.consejotransparencia.cl/wp-content/uploads/2022/01/La-proteccio%CC%81n-de-datos-personales-en-contextos-de-avanzado-desarrollo-tecnolo%CC%81gico-con-e%CC%81nfasis-en-videovigilancia-y-tecnologi%CC%81a-de-reconocimiento-facial-empleada-por-el-sector-pu%CC%81blico-1.pdf.

adelanto tecnológico como la forma de ser precavidos frente a la potencial amenaza. Por supuesto, las guías deberían desarrollar de manera sencilla el derecho a la protección de datos, y las facultades o derechos que hacen posible su defensa: cómo ejercitar los derechos de acceso, rectificación, cancelación, oposición, etc. Las guías deben ser claras en sus contenidos, de manera que puedan ser entendidas por todos los ciudadanos con independencia del nivel de estudio y del nivel de conocimiento de la materia (debe evitar la posibilidad de generar brechas digitales). De esta manera el ciudadano podrá ser más proactivo y cuidadoso con sus informaciones personales.

5. El derecho a la protección de datos: concepto, contenido esencial y naturaleza jurídica

El derecho a la protección de datos personales constituye un derecho fundamental que, arraigado en el tronco común de la vida privada, proyecta su esfera de control en la tecnología (Rallo Lombarte, 2009: 18; Murillo de la Cueva, 2009: 134). Sin ser este el lugar idóneo para disertar conceptual y materialmente acerca de la diferenciación entre ambos derechos, recordemos que la vida privada es más extensa en sus contenidos que la intimidad y se identifica con la idea de privacidad (Pendás, 1995; Del Castillo Vázquez, 2007). Este último término, especialmente, parece abarcar la necesaria protección del individuo cuando desea hacer efectivo el control sobre aspectos de su vida en el contexto tecnológico.

La privacidad así entendida coincide con el derecho a la protección de datos concebido como el derecho del individuo a ejercer un control sobre sus informaciones personales cuando están en poder de un tercero, ya sea este el Estado o un particular. El derecho a la protección de datos ha de facilitar a la persona saber en todo momento quién tiene los datos personales, qué uso va a hacer de ellos, y poder rectificarlos o cancelarlos según la voluntad del sujeto.

La finalidad del derecho a la protección de datos, a la privacidad, es proteger la dignidad del ser humano, pues el uso de los datos puede afectar al derecho a la intimidad, al derecho a la libertad de expresión, al derecho al trabajo, a la igualdad, etc., en definitiva, al conjunto de derechos de la persona.

Los derechos fundamentales disfrutan de un contenido esencial que identifica al propio derecho y lo diferencia de los demás. Dicho contenido esencial está formado por el conjunto de acciones que el sujeto puede ejercitar para defender los intereses que el derecho protege.

El contenido esencial del derecho a la protección de datos está formado por las facultades que se dirigen a permitir que la persona pueda seguir ejerciendo un control sobre sus datos personales. Y se concretan en derechos clásicos que forman parte del propio derecho a la protección de datos, y son el derecho de acceso, el derecho de rectificación, el derecho de cancelación, el derecho al olvido, el derecho de oposición, el derecho a la limitación del tratamiento y un principio esencial de la protección de datos que es el consentimiento del individuo por el que autoriza el tratamiento de los datos (Polo Roca, 2020). Es verdad que el consentimiento está excepcionado en las circunstancias previstas en las leyes, que legitiman el tratamiento de datos al margen de la valoración de la voluntad del sujeto. La garantía de protección del individuo en estos casos en los que el consentimiento no es la base que valida un tratamiento de datos, viene asegurada por los principios que han de regir el tratamiento de los datos y el ejercicio de los derechos propios del contenido esencial del derecho, además, obviamente, de su previsión en una norma. En caso contrario, suprimido el consentimiento para el tratamiento de los datos y eliminada la posibilidad de ejercitar los derechos, la persona perdería el control sobre sus datos personales y se dañaría su dignidad y el ejercicio del resto de sus derechos. Se lesionaría el derecho a la protección de datos de carácter personal.

Si convenimos que el derecho a la protección de datos es un derecho de naturaleza fundamental recogido en las constituciones de los Estados, estamos otorgándole el máximo nivel de protección. Este alto nivel se proyecta en una intervención del legislador para elaborar las normas que desarrollan el derecho, y que regulan el ejercicio de las facultades intrínsecas al mismo, y en una protección reforzada a través de la actuación de los órganos judiciales para restaurar la integridad del derecho vulnerado y devolver al particular a su situación inicial de disfrute del derecho, esto es, de control de sus informaciones personales. La protección tan elevada de la que disfruta este derecho está en correspondencia con su conexión con la personalidad y con la dignidad del ser humano. No olvidemos que conocer los datos personales que revelan cómo es el individuo, nos aporta una información relativa a su esencia, a lo que piensa, hace, decide, etc.; en el fondo revela aspectos de su personalidad que han de quedar bajo el control de la persona misma.

5.1. Los elementos básicos que definen el contenido del derecho

Los elementos básicos que componen el derecho a la protección de datos personales son las facultades o derechos que facilitan el control. Y tanto los principios del tratamiento como las medidas técnicas de seguridad constituyen

también pilares esenciales en el tratamiento de datos personales. Dentro de los principios encontramos:

· Principio de licitud, transparencia y lealtad, según el cual los datos deben ser tratados de forma lícita, transparente y leal.

· Principio de finalidad: la finalidad/es del tratamiento debe ser determinada, explícita y legítima. Los datos personales no pueden ser utilizados posteriormente con finalidades incompatibles con las iniciales.

· Principio de minimización de datos, conseguido a través de medidas técnicas y organizativas que aseguren que solo van a ser objeto de tratamiento los datos estrictamente necesarios para cumplir los fines específicos ya precisados en la recogida.

· Principio de conservación limitada, según el cual los datos no pueden conservarse por más tiempo del necesario para cumplir con las finalidades perseguidas. Así, alcanzadas las finalidades del tratamiento, los datos deben ser eliminados o bloqueados (restringida su utilización), o anonimizados para no identificar a la persona y hacer peligrar el derecho a la protección de datos.

· Principio de exactitud, por el que se obliga al responsable del tratamiento a vigilar la exactitud de los datos de manera que respondan con veracidad a la situación real del sujeto y, en caso de encontrar alguna inexactitud, el responsable mismo deberá proceder a su rectificación.

· Principio de seguridad: exige adoptar todas las medidas técnicas y organizativas para garantizar la integridad de la información, su disponibilidad, de manera que solo sean accesibles a quienes legítimamente pueden tratar dichos datos y su confidencialidad.

Dentro de la regulación de la protección de datos en Latinoamérica destaca, como elemento regional común y propio, la existencia del *habeas data*, que es un procedimiento instado para conocer las informaciones personales o de interés general que obran en registros públicos. El *habeas data* no viene de la mano de la revolución tecnológica, pues ya estaba incluido en las constituciones latinas antes de la digitalización de las sociedades, aunque es cierto que se robustece en su finalidad cuando se dirige a la protección de los datos personales y, a

partir de la extensión de la digitalización, adquiere una dimensión más amplia. El *habeas data* no solo da acceso al conocimiento de las informaciones personales, esto es, el derecho de acceso en versión europea, sino que a través de él se puede solicitar también la rectificación de los datos considerados erróneos o parcialmente incorrectos. El sujeto puede acudir directamente ante los tribunales de justicia presentando un *habeas data*, sin necesidad de agotar antes la vía administrativa. En realidad, funciona como un proceso de aplicación inmediata porque va dirigido a la protección de un elemento propio de garantía del derecho fundamental a la información en un primer momento, y al derecho a la protección de datos más adelante, por lo que su presentación inicia un procedimiento de cuasiurgencia en la tramitación y en la resolución.

La identificación del *habeas data* con el derecho de acceso se advierte también en las características de uno y otro. En ambos casos se trata de un derecho personalísimo cuyo ejercicio se atribuye al titular de la información y que solo podría ser denegado para salvaguardar un derecho o interés de otra persona o el interés público, a juicio de la Administración.

Con bastante precisión en su enunciación, el art. 70 de la Constitución de la República Dominicana lo define como el derecho que tiene toda persona:

> a una acción judicial para conocer de la existencia y acceder a los datos que de ella consten en registros o bancos de datos públicos o privados y, en caso de falsedad o discriminación, exigir la suspensión, rectificación, actualización y confidencialidad de aquéllos, conforme a la ley. No podrá afectarse el secreto de las fuentes de información periodística.

Por su parte, el art. LXXII de la Constitución de Brasil reconoce el *habeas data* en el título de los derechos y garantías fundamentales, afirmando que se concederá *habeas data*: "a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimientos secreto, judicial o administrativo" (del tenor expreso de la Constitución, parece quedar al margen de la acción del *habeas data* el control sobre el almacenamiento privado de datos). Estos dos ejemplos constituyen una muestra del instrumento de protección de los datos de carácter personal que es similar en toda la región latinoamericana. En este sentido podemos hablar de una regulación uniforme, y una práctica sólida y consolidada del ejercicio del *habeas data*.

Respecto de los derechos y de forma sintética, debemos señalar lo siguiente:

· Derecho de acceso: atribuye al sujeto titular del derecho la facultad de solicitar al responsable del tratamiento de datos, que le informe si está tratando sus datos de carácter personal y le proporcione información relativa a los fines del tratamiento, los datos que está tratando, los destinatarios, el plazo de conservación o los criterios para el mantenimiento de los datos, la posibilidad de ejercitar el resto de derechos, así como a presentar una reclamación ante la autoridad de control y la existencia de decisiones automatizadas (entre otras).

· Derecho de rectificación: según el cual el sujeto tiene derecho a solicitar la corrección de los datos (por incompletos, inexactos o erróneos) que no respondan con exactitud a la situación real de la persona sin ninguna demora. En la solicitud de rectificación hay que acompañar los documentos que justifiquen la corrección pedida.

· Derecho de oposición: como se intuye por su denominación, es el derecho de la persona a oponerse a un tratamiento de datos solamente en los supuestos recogidos por la ley.

· Derecho de supresión: facultad de solicitar la supresión de los datos en los casos contemplados en la norma, entre ellos, el cumplimiento de los fines que motivaron su tratamiento, o si los datos han sido tratados de forma ilícita, si retiramos el consentimiento otorgado en un momento anterior, entre otras circunstancias. El derecho de supresión encuentra una modalidad particular en el llamado derecho al olvido, que se ejercita ante los motores de búsqueda y que obliga al responsable del buscador a suprimir los enlaces que relacionen el nombre de una persona con sus informaciones personales.

· Derecho a la limitación del tratamiento de los datos personales del sujeto con las peculiaridades y bajo las condiciones que indican las leyes.

Ninguno de los derechos reseñados es derecho absoluto, por lo que admiten restricciones y modulaciones para preservar otros bienes o derechos constitucionales dignos de protección, o para preservar los intereses o derechos de otra persona diferente del sujeto.

5.2. Formas de reclamación de la exigibilidad del derecho

En un Estado de derecho, la forma más adecuada de reclamar la protección de un derecho fundamental —como la protección de datos— es acudir ante los órganos judiciales reclamando su intervención para obtener una sentencia, de obligado cumplimiento, en la que se restaure al particular en el disfrute de su derecho. El inicio de un procedimiento de *habeas data* es un instrumento eficaz para la defensa del derecho allí donde está previsto. Así, los tribunales ordinarios ejercen el papel de defensores naturales de los derechos de la persona.

Junto a la intervención de los órganos del poder judicial, los ordenamientos que han decidido la creación de un órgano independiente que vela por la aplicación de la normativa de protección de los datos personales le han atribuido la facultad de intervenir para ofrecer una tutela adecuada a los ciudadanos que la demanden.

Las acciones ante los órganos de control deben ser fáciles de cumplimentar, identificadas con el nombre y apellidos del sujeto perjudicado, hechos, razones y petición que se dirige al órgano de control, órgano que ha incurrido en una presunta lesión del derecho a la protección de datos y la firma del sujeto que interpone la reclamación de manera que quede identificado de forma clara.

6. Ejemplos de regulaciones de América Latina

La regulación de la protección de datos constituye una de las intervenciones jurídicas pioneras en materia tecnológica. Dos son los modelos legislativos que podemos encontrar en materia de protección de datos. En primer lugar, el modelo europeo, con una trayectoria ya dilatada y asentada en principios generalizados de la protección de datos. La actividad legislativa europea en relación con la digitalización se enmarca en la Estrategia Digital Europea. Este modelo legislativo europeo de protección de datos personales se ha extendido a los países latinoamericanos con clara influencia en sus normas sobre la materia. En segundo lugar, el modelo estadounidense, con una diferencia en cuanto a las medidas de protección de los datos.

Dentro de la región destacan las iniciativas globales para iniciar una mejora de las legislaciones en materia de protección de datos personales. Así, la estrategia acordada en 2016 de la Red Iberoamericana de Datos Personales de 2020 consistente en "Impulsar y contribuir al fortalecimiento y adecuación de los

procesos regulatorios en la región, mediante la elaboración de directrices que sirvan de parámetros para futuras regulaciones o para revisión de las existentes en materia de protección de datos personales". Igualmente, el 20 de junio de 2017 se aprobaron los Estándares de Protección de Datos Personales para los Estados Iberoamericanos[3]. Este documento elabora unas directrices orientadoras para la elaboración de regulaciones de protección de datos en aquellos países que no cuenten con ella o para la revisión de las ya existentes. De esta manera, el objetivo de armonizar las regulaciones de la zona está presente en esta iniciativa con base en cuatro pilares esenciales:

· Conjunto de principios y derechos comunes.

· Garantizar el efectivo ejercicio y la tutela del derecho a la protección de datos personales mediante reglas comunes que aseguren el debido tratamiento de los datos personales.

· Facilitar el flujo transfronterizo de datos personales entre los Estados latinoamericanos y más allá de las fronteras.

· Favorecer la cooperación internacional entre las autoridades de control de los Estados latinoamericanos con otras autoridades de control no pertenecientes a la región, así como autoridades y organismos internacionales en la materia.

Obviamente, conseguidos los objetivos primero y segundo, se allana el camino para la consolidación del tercer y cuarto objetivo, que requieren para su robustecimiento la existencia de normas y legislaciones uniformes que aseguren una protección semejante del derecho a la protección de datos personales. Hay que subrayar que el texto señala expresamente como referencias de los estándares tanto la adopción de textos latinoamericanos como otros instrumentos internacionales, tales como las directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la OCDE, así como el convenio 108 del Consejo de Europa y su Protocolo de perfeccionamiento y el RGPD, que, como ya hemos reiterado, constituye un referente sólido y fuerte en el ámbito del derecho a la protección de datos y de la libre circulación de los mismos.

[3] Véase: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

El modelo europeo vigente, el RGPD, es el modelo que, por medio, tanto de la influencia española como europea en Latinoamérica, ha calado de manera profunda en las legislaciones sobre la materia. En realidad, la seguridad que aportan las reglas europeas facilita la solidez de las relaciones económicas entre las empresas latinoamericanas y las europeas, al tiempo que refuerza la confianza de los ciudadanos europeos en relación con los servicios que ofrezcan las empresas latinoamericanas. De hecho, bajo la perspectiva latinoamericana, el objetivo principal del RGPD es "dar el control a los ciudadanos y residentes respecto a sus datos personales y simplificar el entorno regulador de los negocios internacionales, unificando la regulación dentro de la Unión Europea"[4]. Junto a esa vertiente empresarial, el RGPD constituye un marco fuerte de tutela del derecho a la protección de datos personales.

Dentro del panorama legislativo regional sudamericano podemos distinguir entre dos modelos diferentes. Por un lado, observamos la existencia de un modelo donde existe una ley general que recoge los elementos principales de la protección de datos. Por otro, asistimos a un patrón legislativo en el que destaca una multiplicidad de leyes que plasman de manera sectorial aspectos de la protección de datos. Frente a esta última modalidad —que puede provocar dispersión normativa, falta de seguridad jurídica y dificultades en orden a su aplicación—, preferimos la existencia de una norma general, que además es la política legislativa que se está imponiendo entre las modificaciones de leyes de los últimos años. Esto no obsta para, a partir de ella, poder especificar sectorialmente, si fuera más acorde con una mejor aplicación de la norma, aspectos particulares de la protección de datos en los diferentes ámbitos, esto es, crediticio, de salud, etc. En casi todos los países se compatibilizan estos dos modelos regulatorios, principalmente por la anticipación temporal de las normas dirigidas a regular determinados sectores frente a la elaboración de la norma general, más tardía en su aparición. Aunque, como decimos, la tendencia es la reordenación en una norma general.

La mayor garantía para la protección de los datos personales consiste en su reconocimiento como derecho a nivel constitucional. Hay que indicar la peculiaridad que comparte toda la región latinoamericana, que contempla en sus constituciones el reconocimiento del *habeas data* como una acción judicial para

[4] Tal y como queda reflejado en Chile: https://www.consejotransparencia.cl/wp-content/ uploads/ 2022/01/La-proteccio%CC%81n-de-datos-personales-en-contextos-de-avanzado-desarrollo-tecnolo%CC%81gico-con-e%CC%81nfasis-en-videovigilancia-y-tecnologi%CC%81a-de-reconocimiento-facial-empleada-por-el-sector-publico-1.pdf (consultado el 7 de noviembre de 2022).

poder ejercer el control sobre los datos a través del ejercicio de los derechos que forman el contenido esencial de la protección de datos. Dicho reconocimiento está recogido en las constituciones de la República Dominicana (art. 44.2) y *habeas data* art. 70; Constitución de Brasil, *habeas data* en LXXII; la Constitución chilena (19 nº 4), con una ley de 1999 (Ley 19.628), adoptada en un contexto de protección de datos diferente al actual; y la Constitución de la República de Colombia (art. 15). La Ley 1581, de 17 de octubre de 2012, se funda en el art. 15 sobre conocer, rectificar las informaciones sobre la persona, así como el derecho a la información. En Ecuador, la Constitución reconoce el derecho a la protección de datos en el art. 66.19, así como el *habeas data*, sin dicha denominación, en el art. 92, como una acción ante el responsable de los archivos donde se almacenan datos manuales o electrónicos, tanto para conocer como para rectificar, eliminar o anular. Habla incluso de datos sensibles.

En cuanto al panorama legislativo, destacamos las legislaciones siguientes:

Brasil

Ley de Brasil 13.709 de 14 de agosto de 2018 (redacción por la Ley 13.853 de 2019, que entró en vigor en agosto de 2020), especialmente precisa en su objeto de aludir a los medios digitales, y prever el tratamiento de estos datos con el objeto de proteger "los derechos fundamentales de libertad e intimidad y el libre desarrollo de la personalidad de la persona física" (art. 1). La protección se articula frente al tratamiento realizado por una persona física o una persona jurídica, ya sea pública o privada. A nuestro modo de ver, la terminología empleada por la ley de protección de datos resulta novedosa, pues expresamente alude a la protección de datos como una disciplina que se basa en el respeto a la "privacidad, autodeterminación informativa, libertad de expresión, información, comunicación y opinión, inviolabilidad de la intimidad, el honor y la imagen, desarrollo económico y tecnológico e innovación, libre empresa, libre competencia y protección del consumidor y los derechos humanos, el libre desarrollo de la personalidad, la dignidad y el ejercicio de la ciudadanía por las personas físicas". Pese a este llamativo precepto, el resto de la ley se ajusta a los estándares ya asentados a nivel internacional sobre el derecho a la protección de datos.

El art. 55ª de la Ley de 2018 crea la Autoridad Nacional de Protección de Datos (ANPD), como autoridad especial, con autonomía técnica y equidad propia. El Consejo de Administración de la ANPD es el máximo órgano de dirección, y sus miembros son elegidos por el presidente y nombrados por la Autoridad Na-

cional previa aprobación del Senado Federal. La Autoridad Nacional brasileña podrá solicitar en cualquier momento, a los órganos y entidades del poder público que realicen operaciones para el tratamiento de datos personales, la información específica sobre el alcance y naturaleza de los datos y demás detalles del tratamiento realizado, y podrá emitir un dictamen técnico complementario para asegurar el cumplimiento de esta ley. La ANPD está integrada, entre otros, por el Consejo Nacional de Protección de Datos Personales y Privacidad formado por representantes de los órganos democráticos y de justicia, así como por miembros de la sociedad civil y de las entidades científicas, tecnológicas y empresariales. Es el órgano que propone las líneas principales para la elaboración de la Política Nacional de Protección de Datos Personales, difunde el conocimiento de la protección de datos personales y la privacidad, sugiere las acciones a llevar a cabo por la ANPD y elabora los informes anuales que evalúan la implementación de las acciones de la Política Nacional de Protección de Datos Personales y Privacidad. Quizá la dependencia del órgano del presidente de la República merma su autonomía. Con carácter general podemos afirmar que la última modificación de la ley de protección de datos de Brasil sigue el modelo de protección de datos del Reglamento europeo.

Chile

Chile se encuentra a la vanguardia en cuanto a protección de datos, con un proyecto de ley actualmente en la Cámara sobre la protección y el tratamiento de datos personales y la creación de la Agencia de Protección de Datos Personales que modifica la Ley 19.628[5]. El proyecto de ley señala de forma explícita —entre sus objetivos— modernizar y actualizar el marco normativo de protección de datos, y constituye un texto que muestra la influencia de la legislación europea en esta materia. En Chile existe una gran dispersión normativa tanto general como sectorial. Por otra parte, hay que destacar la actividad realizada por el Consejo para la Transparencia, cuya implicación en materia de protección de datos es significativa. El proyecto de ley es un texto que muestra la influencia de la legislación europea en esta materia. El Consejo para la Transparencia[6] tiene entre

[5] Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07m.

[6] El Consejo para la Transparencia dirige recomendaciones a los órganos de la Administración del Estado en virtud del art. 33, e y m de la Ley de Transparencia de la Función Pública y Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la Ley n° 20.285, con-

sus atribuciones la de velar por la aplicación correcta de la Ley de Protección de Datos 19.628, de protección de datos de carácter personal en ejercicio de la atribución que le confiere el artículo 33 m de la Ley de Transparencia de la Función Pública y de Acceso a la Información de la Administración del Estado, aprobada por el artículo primero de la Ley 20.285, de 2008 (en adelante, Ley de Transparencia). Dentro de esta atribución de velar por la aplicación de la ley, el Consejo para la Transparencia adoptó un acuerdo[7] en el que recomienda a la Administración del Estado cómo actuar para la defensa de los datos personales en poder de dicha Administración, por medio de una elevación de los estándares de protección de los datos que maneja el poder público. El texto recoge un conjunto de recomendaciones dirigidas a la Administración cuando trata datos de carácter personal. En realidad, el acuerdo reúne los elementos principales que ha de contemplar una norma general sobre protección de datos. El Consejo para la Transparencia ha formulado también recomendaciones respecto a la instalación de dispositivos de videovigilancia por parte de las municipalidades (a través de cámaras de videovigilancia, globos aerostáticos, drones, cualquier otro instrumento idóneo para la grabación y/o captación de imágenes con fines de seguridad), conforme a las disposiciones de la Ley 19.628. La implantación de estos dispositivos ha sido revisada por el Consejo, que ha formulado recomendaciones para el debido respeto y garantía de los datos personales de los individuos[8].

Uruguay

La Constitución de la República de Uruguay no recoge de forma explícita el derecho a la protección de datos personales, que queda al amparo de la cláusula general del art. 72, como reconoce el art. 1 de la Ley 18.331, de 11 de agosto de 2008, protección de datos y *habeas data*. La ley de 2008 crea el órgano de control (art. 31), desconcentrado de la Agencia para el Desarrollo del Gobierno de Gestión electrónica y la Sociedad de la Información y del Conocimiento, denominado Unidad Reguladora y de Control de Datos Personales, encargado de

sistentes en formular recomendaciones a los órganos de la Administración del Estado tendientes a perfeccionar la transparencia de su gestión y a facilitar el acceso a la información que posean, y en velar por el adecuado cumplimiento de la Ley n° 19.628, de protección de datos de carácter personal.

[7] https://www.bcn.cl/leychile/navegar?idNorma=1029588&idParte=0&idVersion=2011-09-14.

[8] Oficio nº 2309, de 23 de marzo, del Consejo para la Transparencia, que formula recomendaciones respecto de la instalación de dispositivos de videovigilancia por parte de las municipalidades según la Ley 19.628. Disponible en: https://www.portaltransparencia.cl/PortalPdT/documents/10179/62801/OF.+2309+VIDEOVIGILANCIA.pdf/d767f39b-add2-4d76-9a67-c6dbe6de3b2c?version=1.0.

custodiar el cumplimiento de la legislación de protección de datos personales y asegurar el respeto a sus principios, pero con una clara dependencia del ejecutivo en los nombramientos de sus miembros, pese a que la norma aclara que durante su mandato "no recibirán órdenes ni instrucciones en el plano técnico". El art. 37 recoge el *habeas data*. Uruguay ha aprobado también el Protocolo de enmienda del Convenio para la protección de las personas con respecto al tratamiento de datos personales, suscrito en Estrasburgo el 10 de octubre de 2018.

Paraguay

Paraguay dispone de una ley de 2014 de acceso a la información pública y transparencia gubernamental que no efectúa una protección de los datos de forma específica. Por ello, el proyecto de ley sobre protección de datos del año 2021 aspira a colmar la laguna legislativa existente en el país. La Ley 6534/2020 de protección de datos crediticios ha dejado sin efecto la Ley 1682/2001, por lo que los datos de carácter personal se encuentran en una situación de desprotección que intenta remediar el proyecto del año 2021. La pretensión del proyecto de ley es ofrecer una protección integral que supere la protección sectorial —y por tanto deficiente— en atención a la tutela de los derechos de las personas. El proyecto paraguayo remite en su texto a la legislación europea, señalando de forma explícita que: "Este marco se posiciona como un referente obligado y determinante para la elaboración de las legislaciones nacionales de protección de datos en Iberoamérica". El proyecto de ley aspira a adoptar los estándares de protección de datos europeos y convertir a Paraguay en un Estado con un nivel de protección adecuado que atraiga la inversión europea. Además, los estándares promovidos por la Unión Europea ayudan a facilitar el desarrollo de la economía digital y promueven la innovación, como reconoce el proyecto de ley.

Junto a este importante referente, Paraguay constata el empuje que la aprobación del proyecto de ley supondría para la firma del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, suscrito en el ámbito del Consejo de Europa por parte de Argentina y Uruguay.

Panamá

Panamá recoge en su art. 42 el derecho fundamental a la protección de datos con bastante precisión, señalando el objeto del derecho, así como algunos de

los derechos propios de su contenido esencial: el derecho de rectificación y de supresión. Igualmente, alude al consentimiento y al principio de finalidad.

La Ley 81, de 26 de marzo de 2019, sobre protección de datos personales regula el tratamiento de la información. La Ley 81 ha sido desarrollada a través del Decreto Ejecutivo nº 285, de 18 de mayo de 2021, que reconoce el nivel de protección de mínimos que recoge la ley y es compatible con los regímenes especiales de protección de datos. El art. 34 de la ley crea el Consejo General de Protección de Datos, organismo competente para consultar y asesorar en materia de protección de datos, entre otros, a la Autoridad Nacional de Transparencia y Acceso a la Información[9]; esta autoridad es el organismo rector en materia de protección de datos (art. 54 del Decreto Ejecutivo). A través de la Dirección de Protección de Datos Personales[10], la Autoridad de Control resolverá las quejas y peticiones presentadas. Corresponde a esta Dirección General la potestad sancionatoria ante los incumplimientos de la legislación sobre protección de datos (art. 58 del Decreto Ejecutivo, y art. 1 y 2 de la Resolución de 23 de abril de 2021).

Ecuador

Ecuador ha regulado la protección de datos a través de la Ley Orgánica de Protección de Datos Personales, de 26 de mayo de 2021. Se trata de un derecho reconocido en el art. 92 de la Norma Suprema ecuatoriana. La norma de Ecuador regula los datos crediticios y los datos de salud dentro del cuerpo de la ley, lo que evita la existencia de la dispersión normativa que se ha advertido en otros ordenamientos latinoamericanos. La norma refleja con acierto todas las cuestiones que en la normativa europea aparecen detalladas en el RGPD, aunque no se haga referencia explícita a ella en la ley ecuatoriana.

Costa Rica

Costa Rica ha llevado a cabo una reforma del art. 24 de la Constitución para recoger de forma explícita el derecho a la protección de datos personales y la inviolabilidad de los datos sensibles. Resulta de interés el texto que justifica la reforma, pues toma como referente la regulación europea de la protección de

[9] La Ley de 25 de abril de 2013 crea la Autoridad Nacional de Transparencia y Acceso a la Información.
[10] La Resolución nº ANTAI-DS-002-2021, de 23 de abril de 2021, por la que se crea la Dirección de Protección de Datos Personales dentro de la estructura organizativa de la Autoridad Nacional de Transparencia y Acceso a la Información.

datos, así como el Convenio 108+, y reconoce la necesidad de elevar el derecho a la protección de datos al máximo nivel dentro de las constituciones y como derecho autónomo de la intimidad o de la vida privada. La Ley 8968, de 7 de julio de 2011, de protección de datos personales de la persona, frente al tratamiento de sus datos personales vigente, habla de protección de la autodeterminación informativa, concepto ya en desuso. La ley resulta obsoleta en cuanto a los derechos incluidos en protección de datos, aunque refleja sus principios esenciales. La ley crea la Agencia de Protección de Datos de los Habitantes (Prodhab) (art. 15). El Reglamento a la Ley de Protección de Datos frente al Tratamiento de sus Datos Personales, nº 37554-JP, de 30 de octubre de 2012, desarrolla la ley. En la actualidad hay un proyecto de ley en tramitación (2022) que actualiza la normativa sobre protección de datos. El propio proyecto reconoce "la desactualización de la normativa vigente frente a los retos de la creciente digitalización" y alude expresamente a la intención de Costa Rica de adherirse al Convenio 108, así como también al 108+ y de este modo estar en consonancia con la regulación del RGPD.

La adhesión de Costa Rica a los documentos del Consejo de Europa haría al país atractivo para la inversión digital europea y "favorecería la exportación de servicios digitales desde Costa Rica al masivo mercado europeo". La influencia del RGPD se advierte en todo el texto del proyecto de ley. En cuanto a la Agencia de Protección de Datos el proyecto da una nueva perspectiva a este órgano configurándolo como una autoridad verdaderamente independiente que amplía sus potestades y sus funciones.

República Dominicana

La Ley nº 172-13, de 15 de diciembre de 2013, que tiene por objeto la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, contiene los principios generales que han de regir los tratamientos de datos tales como la finalidad, la calidad de los datos, el derecho a la información y el consentimiento, así como medidas de seguridad, deber de secreto y los derechos de los sujetos. Sin embargo, la mentalidad de legislador dominicano se enfoca a garantizar la actuación eficaz de las Sociedades de Información Crediticia (SIC), que utilizan información personal de carácter económico, asegurando al tiempo la protección de la privacidad, y señala la norma y los derechos de los titulares de los datos. Por tanto, la norma

se convierte, no tanto en una norma general, sino en una regulación sectorial que ha de aludir obligatoriamente a los principios generales de la protección de datos para su finalidad última que se concentra en las SIC. De hecho, el órgano de control del cumplimiento de la norma y de la observancia de los derechos del sujeto es la Superintendencia de Bancos, en una norma enfocada casi de manera exclusiva a la protección de los datos crediticios. Por tanto, en República Dominicana se precisa una actualización de la norma sobre protección de datos que generalice los principios de la protección de datos y se alinee con los estándares europeos y con las normas latinoamericanas que ya los han acogido.

Tabla 1. Puntos fuertes y débiles de las legislaciones latinoamericanas

País	Constitución	Legislación	Puntos fuertes	Puntos débiles
Argentina*	Art. 43	Ley 25.326, de 2 de noviembre de 2000 (Proyecto de ley de 2022)	Recoge elementos esenciales, pero necesitan una revisión que ya se ha iniciado	
Brasil	LXXII *habeas data*	Ley 13.709	Se ajusta a estándares internacionales y al RGPD	
Chile	Art. 19.4	Proyecto 2022	Se ajusta a estándares internacionales y al RGPD	
Colombia*	Art. 15	Ley 1581 de 17 de octubre de 2017	Recoge elementos esenciales, pero necesitan una revisión	
Paraguay	Arts. 33 y 135 *habeas data*	Proyecto 2021	El proyecto se ajusta a los estándares internacionales y al RGPD	Dispersión sectorial
Uruguay	No reconocimiento explícito	Ley 2008	Guías sobre protección de datos actualizadas	Obsoleta, aunque recoge los elementos principales

País	Constitución	Legislación	Puntos fuertes	Puntos débiles
Costa Rica	Art. 24 (no explícitamente)	Ley 2011	Se ajusta a estándares internacionales	
Ecuador		Ley 2021	Se ajusta a estándares internacionales y al RGPD	
Panamá	Arts. 29 y 42 (de forma diluida en otros derechos)	Ley 2019	Se ajusta a estándares internacionales y al RGPD	
República Dominicana	Arts. 44.2 y 70 *habeas data*	Ley 2013	Recoge elementos esenciales pero necesitan una revisión	Mejorable Ley de protección de datos crediticios

*Aunque no han sido objeto de desarrollo en el texto, se incluyen en el esquema las referencias de Argentina y de Colombia. Colombia destaca por la elaboración de un conjunto excelente de guías (Delegatura para la Protección de Datos Personales) que trasladan al ciudadano la necesidad de proteger los datos personales y favorecen la extensión de la cultura de la protección de datos en el país.

Cabe mencionar también la existencia de la Red Iberoamericana de Protección de Datos Personales (RIPD) cuyo Reglamento (San José, 30 de noviembre de 2018) constituye un valioso documento que recoge entre sus objetivos promover políticas que garanticen el derecho fundamental a la protección de datos personales, la edición y publicación de documentos de trabajo que permitan difundir los resultados obtenidos en las actividades desarrolladas por las diferentes instituciones públicas, extender la cultura de la protección de datos y llevar a cabo programas de capacitación entre sus miembros. El Reglamento recoge elementos organizativos y de funcionamiento de la RIPD.

7. Retos para la protección de datos

La elaboración de normas sobre protección de datos tiene efectos positivos en la sociedad. No solo porque la regulación de los datos es necesaria para proteger el derecho a la protección de datos y la privacidad del individuo en el siglo XXI.

Proteger la libertad y los derechos de las personas es motivo suficiente para legislar sobre cualquier materia, pero además la legislación sobre protección de datos sobre estándares comunes y normas internacionalmente aceptadas facilita las transferencias internacionales de datos, con lo que la economía digital y la economía en general se ven favorecidas, así como la innovación y la investigación.

En el ámbito de la protección de datos todavía quedan retos pendientes de resolver. Entre ellos podemos citar:

· Proteger los datos personales en los sistemas de IA, que se ocupan ya en buena parte de resolver actividades que antes desarrollaba el ser humano y que ahora se encomiendan a máquinas. En la medida en que en alguno de sus procesos empleen datos de carácter personal, estos no pueden permanecer al margen de la normativa vigente sobre la materia. No puede ignorarse que el individuo puede dejar de ejercer el control sobre sus datos personales introducidos en sistemas de IA ante la dificultad, primero de conocer que son objeto de tratamiento, y después de cómo ejercer los derechos sobre los mismos (Fernández-Aller y Serrano Pérez, 2022: 308).

· Promover la sensibilización de los responsables de tratamiento tanto del sector público como del sector privado sobre las obligaciones que les incumben como responsables de tratamientos de datos a través de cursos, jornadas de formación, etc. Insistir en la responsabilidad proactiva de los responsables del tratamiento, así como en el conocimiento de los documentos a elaborar antes de iniciar un tratamiento, las medidas de seguridad, etc.

· Fomentar la elaboración de códigos de conducta sectoriales para facilitar la aplicación de las normas de protección de datos, y dar a conocer los derechos y deberes de todos los sujetos implicados. La elaboración de códigos de conducta sectoriales sobre la base de estándares comunes, suficientemente consolidados, facilitará un espacio compartido de intercambio seguro de datos personales.

· Asesorar a los poderes del Estado, principalmente al legislador, en la elaboración de las medidas legislativas adecuadas para la protección de los derechos y libertades de los ciudadanos en la sociedad digital, en especial, de normas con estándares de protección elevados que tutelen debidamente los datos de carácter personal. Esta labor de asesoramiento en una materia compleja como la pro-

tección de datos deberían llevarla a cabo personas expertas. Las normas deben ser claras y generar confianza y tranquilidad entre la ciudadanía.

· Elaborar normas que terminen con la dispersión existente (en aquellos países en que exista tal dispersión), que es confusa, contradictoria y carente de seguridad jurídica para los ciudadanos y los sujetos privados y públicos.

· Creación de autoridades de control de protección de datos independientes y con capacidad para informar, adoptar resoluciones, sancionar y realizar una labor divulgativa de los derechos de los ciudadanos y de los deberes de los responsables de tratamiento.

· Reforzar las medidas de seguridad. Hay que evaluar los riesgos del tratamiento para los derechos del sujeto, gestionarlos y saber responder a ellos. Las medidas técnicas han de asegurar que los tratamientos de datos solo van a ser accesibles para quienes están autorizados a conocer la información personal, de acuerdo con la finalidad perseguida y no para cualquier persona.

· Extender la cultura de la protección de datos a través de guías, recomendaciones e información, con el fin de trasladar a la ciudadanía la necesidad de velar por sus informaciones personales. La generalización de la educación digital a todos los niveles y en todos sus aspectos constituye una excelente herramienta para formar al ciudadano en la sociedad digital. Dicha formación alcanza no solo a la protección de datos, sino a todos los aspectos que la persona ha de conocer y utilizar en un mundo digitalizado. Hay que evitar o corregir las probables brechas digitales que puedan surgir.

· Invertir en la digitalización de la sociedad y en la educación. Europa prevé una importante inversión económica para situar al viejo continente como líder en tecnologías. La tecnología y su implantación ha de constituir un elemento más del Estado social que ahora se ha transformado en Estado social digital. El Estado ha de intervenir de forma activa para la transformación digital y eliminar los obstáculos que impidan la igualdad material también desde la perspectiva tecnológica. La inversión económica en tecnología generará a su vez crecimiento económico. No podemos olvidar el valor económico del dato personal (también del no personal).

En conclusión, en los próximos años será necesario insistir en el reconocimiento del derecho a la protección de datos en la región, con un nivel equiparable al europeo, tal y como se ha venido haciendo en algunos países. Más ahora que Estados Unidos está haciendo esfuerzos por regular con más firmeza los asuntos de privacidad. Además, hará falta una institucionalidad suficiente, que permita una gobernanza de las nuevas tecnologías, como la IA. Sin un marco jurídico fuerte, la privacidad de la ciudadanía de Iberoamérica no podrá protegerse suficientemente, en un contexto en el que el modelo de generación de valor a partir del dato personal es la base de la economía digital. Proteger la privacidad es clave en el siglo XXI si queremos que las personas conserven su soberanía y su autonomía a la hora de tomar decisiones (políticas, económicas y de cualquier otro tipo); y en este sentido también es preciso que las personas que interactúan en el nuevo espacio digital lo hagan de manera responsable e informada, con el fin de asegurar un entorno de confianza para el conjunto de la ciudadanía.

Referencias bibliográficas

Casas Baamonde, M. E. (coord.) (2020): *El derecho a la protección de datos en la sociedad digital*, Fundación Ramón Areces.

De la Quadra-Salcedo Fernández del Castillo, T. (2019): "Derechos fundamentales, democracia y mercado en la edad digital", *Derecho Digital e Innovación*, nº 1, enero-marzo, pp. 1-19.

Del Castillo Vázquez, I. C. (2007): "Transparencia, acceso a la documentación administrativa y protección de datos personales", *Foro*, nº 6, pp. 231-254.

Fernández Aller, M.ª C. y Serrano Pérez, M.ª M. (2022): "¿Es posible una inteligencia artificial respetuosa con la protección de datos?", *Doxa, Cuadernos de Filosofía del Derecho*, nº 45, pp. 307-336.

Fundación Carolina y Telefónica (2021): *La transición digital: retos y oportunidades para Iberoamérica*, Madrid.

García Mahamut, R. (2018): "El derecho fundamental a la protección de datos. El Reglamento (UE) 2016/679 como elemento definidor del contenido esencial del artículo 18.4 de la Constitución", *Corts. Anuario de derecho parlamentario*, nº extra-31, pp. 59-80.

López Garrido, D.; Serrano Pérez, M.ª M. y Fernández-Aller, C. (2017): *Derechos y obligaciones de los ciudadanos/as en la sociedad digital*, Documentos de trabajo, Fundación Alternativas, nº 195.

Murillo de la Cueva, P. (2009): "La protección de datos personales en el horizonte del 2010", *Anuario de la Facultad de Derecho*, nº 2, pp. 131-142.

— (2022): "Aspectos de la actualidad del derecho fundamental a la protección de datos de carácter personal", *La Ley. Privacidad*, nº 11.

Naciones Unidas (2018): "El derecho a la privacidad en la era digital. Informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos", A/HRC/39/29. Disponible en: https://documents-dds-ny.un.org/doc/ UNDOC/ GEN/G18/239/61/PDF/G1823961.pdf?OpenElement.

Pendás, B. (1995): "Introducción a la obra *The right to privacy*, de S. Warren y L. Brandeis", Cuadernos Cívitas, Madrid.

Polo Roca, A. (2020): "El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado", *Revista de Derecho Político*, nº 108, pp. 165-194.

Rallo Lombarte, A. (2009): "La protección de datos en España", *Anuario de la Facultad de Derecho*, nº 2, pp. 15-30.

Rebollo Delgado, L. (2018): *Protección de datos en Europa: origen, evolución y regulación actual*, Dykinson.

Red Iberoamericana de Protección de Datos (2020): *Estrategia RIDP 2021-2025*. Disponible en: https://www.redipd.org/es/documentos/estrategia-ripd-2021-2025.

Serrano Pérez, M.ª M. y Fernández Aller, M.ª C. (2021): "Derecho constitucional e inteligencia artificial", en F. Lledó Yagüe (coord.): *La robótica y la inteligencia artificial en la nueva era de la revolución industrial 4.0*, Dykinson, pp. 487-544.

Legislación

Argentina: Ley 25.326, de 2 de noviembre de 2000, de Protección de Datos.

Brasil: Ley 13.709, de 14 de agosto de 2018 (modificada por la Ley 13.853 de 2019).

Chile: Ley 19.628 de protección de datos de carácter personal (proyecto de ley de septiembre de 2022 que actualiza y moderniza la Ley 19.628 en tramitación).

Colombia: Ley 1581 de 17 de octubre de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Costa Rica: Ley 8968 de 7 de julio de 2011, de protección de datos personales (proyecto de ley de 2022 en tramitación).

Ecuador: Ley orgánica de protección de datos, de 21 de mayo de 2021.

Panamá: Ley 81, de 26 de marzo de 2019, sobre protección de datos personales.
Paraguay: Ley 6534/2020 de protección de datos personales crediticios (proyecto de ley de 2021 en tramitación).
República Dominicana: Ley nº 172-13, de 13 de diciembre de 2013, de protección de datos.
Uruguay: Ley 18.331 de 11 de agosto de 2008, de protección de datos.
Reglamento de la Red Iberoamericana de Protección de Datos, aprobado el 30 de noviembre de 2018 en San José (Costa Rica).

2. El uso ético de la inteligencia artificial y las neurotecnologías

Celia Fernández-Aller
Camilla Roveri
*Santiago Nardini**

1. Contexto ético, social y tecnológico de la inteligencia artificial y las neurotecnologías

1.1. Contexto ético, social y tecnológico de la inteligencia artificial

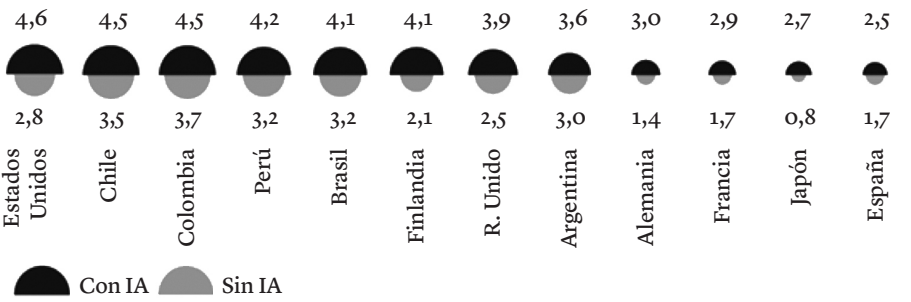
Sin duda la inteligencia artificial (IA) es clave en la cuarta revolución industrial que vivimos. Durante la Tercera Revolución Industrial lo digital no estaba en el centro de la actividad económica, pero progresivamente ha llegado a extenderse de tal forma, que no solo ocupa el centro, sino que invade la mayor parte de ella (Thoughtworks, 2021). La IA (Tegmark, 2017) está detrás de muchas de nuestras actividades cotidianas, como las búsquedas en internet, los asistentes de navegación, los traductores, los sistemas de apoyo a la concesión de créditos o de ayudas públicas, entre otros.

* Celia Fernández-Aller es profesora contratada doctora en la Universidad Politécnica de Madrid (UPM) en el área de Ética y Derecho. Su línea de investigación es el enfoque de derechos humanos en los proyectos tecnológicos, especialmente en torno a la privacidad. Pertenece al grupo de investigación en Organizaciones Sostenibles (GIOS) y al Centro de Innovación en Tecnología para el Desarrollo Humano de la UPM. Ha sido profesora visitante en la Universidad Centroamericana de El Salvador y en la Universidad de Bristol. Formó parte del grupo de especialistas que redactaron la Carta de Derechos Digitales en España. Camilla Roveri es máster en Estrategias y Tecnologías para el Desarrollo de la UPM y la Universidad Complutense de Madrid (UCM). Contratada en el Máster on AL for Public Servicer (AI4GOV). Ha sido becaria en la AI for Good Foundation. Santiago Nardini es máster en Estrategias y Tecnologías para el Desarrollo de la UPM y la UCM. Formó parte del equipo investigador del estudio "Can Venture Capital be a Digital Governance Promoter?" de la Universidad Politécnica de Madrid junto con el Banco Interamericano de Desarrollo.

Algunas estimaciones prevén que la IA podría contribuir a la economía global hasta llegar a los 15,7 trillones de dólares en 2030, más que la productividad de China e India juntas (PWC, 2018). Sorprenden algunas cifras relativas al peso de las *startups* basadas en IA de EE.UU., donde consiguieron cerca de 38 billones de dólares en financiamiento en 2020, mientras en Asia fueron 25 billones y en Europa 8 billones (*The Age of AI*, 2021).

En el ámbito latinoamericano, un estudio del Banco Interamericano de Desarrollo (BID) resalta que la IA puede facilitar las negociaciones comerciales y agregar un punto de crecimiento económico adicional a las economías de la zona. Casi la mitad de ese aumento se generaría por mejoras de la productividad, al permitir a los trabajadores dedicarse más a tareas en las que aportan más valor agregado (Béliz, 2018). El informe también advierte que la irrupción de la IA traerá importantes retos éticos y en el mercado del empleo. En la Figura 1 podemos apreciar las estimaciones económicas de lo que podría suponer la IA en algunos países de América Latina y del mundo.

Figura 1. Variación estimada del PIB en 2035



Fuente: Béliz, 2018: 10.

Tal y como reconoce Oliver (2020: 25), la creadora del primer algoritmo destinado a ser procesado por una máquina fue la matemática Ada Byron (Lovelace), que propuso en el siglo XIX el uso de la máquina analítica de Babbage para resolver problemas complejos, convencida de que las máquinas deberían servir para algo más que para hacer cálculos matemáticos. Nunca llegó a construirse por motivos técnicos y políticos, pero la semilla estaba plantada.

En el siglo XX, el matemático e informático Alan Turing, considerado el padre de la IA, habló de su prueba, que permitía identificar si un sistema es inteligente o no, en un artículo publicado en 1950. En 1956 tuvo lugar la conven-

ción de Dartmouth, un encuentro en el que los mejores expertos en informática definieron la IA como la "disciplina dentro de la Ingeniería que se ocupa del diseño de sistemas inteligentes".

Simplificando mucho y en aras de la comprensión del concepto, la Unión Europea (UE) ha dado diferentes definiciones de los sistemas inteligentes, como esta:

> sistemas software (en algunos casos también hardware) diseñados por humanos que, dado un objetivo complejo, actúan tanto física como digitalmente a través de la obtención de datos, ya sean estructurados o no, interpretando, razonando o procesando la información derivada de estos datos, y decidiendo la mejor acción a tomar para lograr el objetivo deseado (Grupo de Expertos de la Unión Europea, 2019).

En definitiva, la IA es la ciencia que estudia y crea sistemas artificiales inteligentes. Un ejemplo de IA en sistemas *hardware* serían los incluidos en los robots autónomos. Un ejemplo de IA formada solo por *software* serían los asistentes virtuales o *chatbots*.

La transformación digital se entiende como algo imprescindible para la consecución de la Agenda 2030 de los Objetivos de Desarrollo Sostenible (ODS). Junto a ella, las otras grandes transformaciones necesarias afectan a la educación, el género y la lucha contra la desigualdad, la salud, el bienestar y el equilibrio demográfico; la descarbonización energética, la garantía de alimentos, la tierra, el agua y los océanos saludables, y la transformación de las ciudades y comunidades (Sachs *et al.*, 2019).

1.1.1. Impactos positivos y negativos de la IA

Una tecnología clave dentro de la transformación digital es la IA, que, como sucede con otras, tiene impactos positivos y negativos en los derechos de las personas. Broussard (2018) explica cómo la IA podría ser utilizada para resolver problemas endémicos en nuestras sociedades, como la falta de transparencia en el financiamiento de las campañas políticas. La IA también puede ser útil en la formulación de políticas públicas basadas en evidencia empírica en la etapa de identificación de la intervención más apropiada, en la implementación de un programa y en la medición de los impactos deseados.

Igualmente, la literatura ha señalado la relevante contribución de la IA en el campo de la salud, no solo como apoyo al diagnóstico médico, sino en el ám-

bito de los exoesqueletos, prótesis con inteligencia y otros dispositivos que mejoran las capacidades cognitivas. Además, la IA tiene aplicaciones con impacto en el clima y la energía (sistemas de monitorización predictiva), en la agricultura sostenible, en la movilidad, en las políticas de asilo y migración, en las de ayuda humanitaria o en el sistema judicial, entre otros.

A su vez, resulta interesante destacar el papel que podría tener la IA en la garantía del derecho a la educación. Se ha trabajado mucho en la educación para formar a la población en torno a la IA, pero poco en cómo esta contribuye a mejorar y potenciar la educación (Schiff, 2022: 528), es decir, en el uso de la IA en relación a herramientas de enseñanza y aprendizaje, calificación de tareas automáticas, apoyo fuera del aula, y evaluación adaptativa (que se adapta al nivel del estudiante). Los países que han incluido este potencial de la IA en sus estrategias educativas son China, India, Italia, Kenia, Malta, Singapur, Corea del Sur, España y Estados Unidos. Y los países que las tienen más desarrolladas son India, Kenia, Singapur y España (Schiff, 2022: 536).

Otros impactos positivos se dan en el ámbito de la industria —generando por ejemplo más eficiencia en los procesos de fabricación— o en el de la agricultura, por citar solo algunos.

Algunos autores (Vinuesa *et al.,* 2020: 2) han llevado a cabo estudios centrados en la contribución positiva y negativa de la IA en los ODS, llegando a establecer una cuantificación de las mismas: en un 79% las positivas y en un 35% las negativas. Tal y como reconocen los autores, los resultados deben matizarse teniendo en cuenta las siguientes consideraciones:

a) Por un lado, el propio interés puede sesgar a la comunidad de investigadores y a la industria hacia la publicación de resultados positivos. Es esperable que los proyectos de IA con más potencial de maximizar beneficios vayan a ser financiados, mientras que se relegarán los que no puedan rentabilizarse con inmediatez. En este sentido, Benkler afirma que:

> La industria se ha movilizado para dar forma a la ciencia, la ética y las leyes de la inteligencia artificial. El 10 de mayo están previstas las cartas de intención a la National Science Foundation (NSF) de EE.UU. para un nuevo programa de financiación de proyectos sobre la imparcialidad en la inteligencia artificial, en colaboración con Amazon. En abril, tras la publicación por la Comisión Europea de las Directrices Éticas para una Inteligencia Artificial confiable, un académico miembro del grupo de expertos que las elaboró calificó su creación de "lavado de ética" dominado por la industria. En marzo, Google creó un consejo de ética

de la IA, que se disolvió una semana después en medio de la polémica. En enero, Facebook invirtió 7,5 millones de dólares en un centro sobre ética e IA en la Universidad Técnica de Múnich (Alemania) (Benkler, 2019).

Son muchas las voces que se han pronunciado en este sentido (Pratkusha, Kalluri, Crawford, Calo, Köbis, Bonnefon, Rahwan, Banks, etc.), alertando sobre cómo la financiación puede condicionar los resultados de la investigación científica. Sin embargo, esta preocupación debe convivir con la necesaria alianza de actores que ha de facilitar la Agenda 2030, sin la cual será difícil que se consiga. Lamentablemente, no estamos ni siquiera en la senda que nos llevaría a su plena realización (World Inequality Lab, 2022).

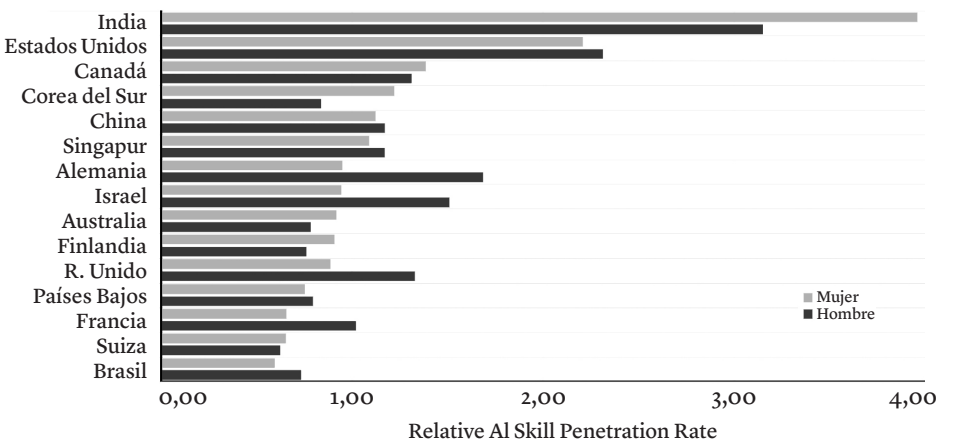
b) Por otro lado, aunque se están llevando a cabo algunos estudios de impacto de la IA en derechos humanos (Consejo de Europa, 2022; Fjeld *et al*., 2020; Agencia de los Derechos Fundamentales de la Unión Europea, 2022), se necesita la paciencia del medio y largo plazo para poder conocer en profundidad los efectos positivos y negativos que tendrá el uso generalizado de algoritmos en el derecho a la igualdad, la justicia, la salud, la educación, la participación democrática, la identidad digital, la libertad de expresión e información, o el trabajo, entre otros.

Entre las investigaciones llevadas a cabo, un informe del Parlamento Europeo destacó la distribución desigual de los beneficios de la tecnología en la sociedad y la posible explotación de los trabajadores, las nuevas cuestiones relacionadas con los derechos a la privacidad y a los datos, y las repercusiones negativas para la democracia (European Parliament, 2020; Véliz, 2021). Por su parte, la Agencia de los Derechos Fundamentales de la UE (FRA, por sus siglas en inglés) señala que muchos derechos fundamentales podrían verse afectados por el uso de la IA (FRA, 2020), como la dignidad humana, la libertad de asociación, y aspectos relativos a la negociación colectiva y a unas condiciones de trabajo justas y equitativas.

La literatura ha destacado también que la IA puede generar, en determinados casos, discriminación como consecuencia de su uso, por ejemplo, porque, entre otras cosas, los datos con los que se entrenan los algoritmos estén sesgados. Tenemos que adaptar nuestros principios y valores éticos a las demandas de las tecnologías. Pero debemos prestar atención también a los sesgos que implícitamente incluimos en los desarrollos tecnológicos. Es innumerable la literatura que hay acerca de los sesgos algorítmicos (Cotino Hueso, 2022; Allen, Wallach y Smit, 2017, entre otros). Y no debemos olvidar el sesgo de género en la IA, sobre el que hay mucha reflexión avanzada (Gebru, 2020; Ortiz de Zárate-Alcarazo,

2021). Este sesgo puede tener diferentes significados, tanto desde el punto de vista de las decisiones que toman los algoritmos como de la falta de presencia femenina en el ámbito profesional de la IA. En este sentido, resulta muy clarificador el gráfico siguiente (Figura 2), que apunta a diferencias de género muy relevantes precisamente en los países que lideran la revolución digital:

Figura 2. Tasa de penetración de las destrezas en el uso de IA



Fuente: Stanford University (2022): *Artificial Intelligence Index Report*: 150.

Además, en ocasiones la IA está afectando a la privacidad de las personas, por cuanto utiliza cantidades masivas de datos —también datos personales—, y toma decisiones que afectan a este derecho. Esto puede suceder porque es complejo solicitar el consentimiento al interesado para el uso de sus datos personales, al no conocerse exactamente el alcance ni el tipo de decisión que se va a tomar. Se trata de una cuestión relevante, y por este motivo el capítulo primero de este libro se dedica a ello. No preocupa tanto el hecho de que se genere valor a partir de nuestra información personal, cuanto de las consecuencias que tiene el hecho de que las tecnologías permitan perfilar a la ciudadanía e influir sobre ella sin las garantías y valores que tanto tiempo ha costado conseguir (el debido proceso, la salud, la educación, la intimidad personal, la democracia como sistema de organización de las personas, que —con todas sus imperfecciones— tiene la misión de alejar los fantasmas del totalitarismo y la injusticia)[1].

[1] Esta charla TED es imprescindible para comprender la realidad que torpemente se intenta describir en nuestro texto: https://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy. Esta noticia nos da idea de hasta qué punto el asunto es grave: https://elpais.

La IA también puede colisionar en determinados casos con el derecho a la libertad de expresión, pues parte de la ciudadanía puede temer represalias si ejercita este derecho en una situación en la que la IA se utilice para vigilar o controlar el uso de una tecnología por parte de las personas.

Un asunto que no cabe olvidar son los impactos de la IA en el derecho a un medioambiente sano. Muchas voces reclaman el derecho a una digitalización sostenible y esta exige un uso óptimo de la energía. El consumo actual de los aparatos electrónicos y la infraestructura que comunica, almacena y procesa los datos, supone entre un 5% y un 9% del total de la energía eléctrica producida y alrededor de un 2% de las emisiones de efecto invernadero[2].

Pero, además, la digitalización —incluida la que está originando la IA— ha de tener el objetivo de la sostenibilidad ambiental. Para ello, se ha de dirigir específicamente a sectores como la eficiencia energética en edificios —control automático de demanda— y transporte —*car sharing*, movilidad conectada, optimización de carga para transporte terrestre—, entre otros (Salgado Criado *et al.*, 2021). Esto supone considerar la infraestructura digital como bien común y reivindicar la soberanía digital para poder establecer democráticamente las prioridades de los desarrollos y las aplicaciones en aquellas áreas donde hay más urgencia[3]. Tal y como establece Ortega (2021):

> usamos el concepto de bien común, colectivo o público en una acepción no jurídica, sino económica, como la del premio Nobel Elinor Ostrom, que se refiere al carácter de uso y no de la propiedad. Desde esta perspectiva, son bienes o servicios de uso público, aunque no sean de propiedad pública por lo que el hecho de que sean suministrados por empresas privadas no tiene por qué afectar a la denominación.

El despliegue de la IA requiere el manejo de grandes volúmenes de datos, que actualmente se realiza en centros de procesamiento de datos. Las Administraciones necesitan disponer de un sistema público de custodia para el procesamiento de datos. Las instituciones y organizaciones sociales también deben

---

com/tecnologia/2023-01-11/las-grandes-tecnologicas-denunciadas-por-provocar-la-crisis-de-salud-mental-de-los-jovenes-en-ee-uu.html

[2] Ver: https://www.enerdata.net/search/node/expected%20world%20energy%20consumption%20increase%20from%20digitalization/.

[3] En el contexto actual, el Foro Económico Mundial recuerda la voluntad de Europa de mantener su soberanía digital. Véase: https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/.

tener acceso a los datos para su uso público. Los datos abiertos implican la interoperabilidad y la interconexión de diversas fuentes de datos. También requiere diseñar servicios que optimicen el uso y la accesibilidad de estos, garantizando al mismo tiempo la seguridad y la privacidad adecuadas (Fernández-Aller *et al.*, 2021). Estas preocupaciones están contenidas asimismo en la Estrategia Europea de Datos[4].

En definitiva, es necesaria una reflexión serena para valorar los impactos de manera más global y, en concreto, sobre los derechos de las personas. El marco de protección de los derechos es anterior al de los ODS y es exigible, por lo que cualquier análisis debe completarse con esta mirada.

1.1.2. Ética de la IA

La actual revolución digital se caracteriza por la aceleración del cambio tecnológico, de consecuencias impredecibles. Algunos autores (Lasalle, 2019) anuncian distopías como el "colapso de la democracia liberal" tal y como la entendemos hoy día. Los retos que plantea la IA son de tal calado que tanto la comunidad científica como la de la ingeniería, las organizaciones empresariales y las gubernamentales o sociales, llevan años planteando la necesidad de afrontar los escenarios de incertidumbre y vacíos legales que origina el diseño, el desarrollo y la implementación de la IA, a partir de la ética (entendida como disciplina encargada de reflexionar acerca de los valores compartidos por la humanidad que nos harán ciudadanos más libres, más dignos, mejores).

La ética tiene que ver con un proceso, con la toma de decisiones y con los criterios y valores que se incorporan en ese proceso (Villas y Camacho, 2022). Lo complejo del tema es que a lo largo del tiempo ha habido distintas visiones de lo que es la ética[5]. Además, los consensos acerca de cuáles son los principios

[4] European Commission (2020): *A European Strategy for Data*. Disponible en: https://ec. europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy.

[5] Un repaso rápido por las distintas teorías éticas obligaría a considerar: a) La ética *consecuencialista o utilitarista* (J. S. Mill y J. Benthan), que es el enfoque más utilizado en el mundo empresarial. Su objetivo es encontrar la solución que produzca un mayor beneficio para mayor número de afectados. b) Para superar las posibles limitaciones del utilitarismo, Rawls propone la *ética de la justicia*, a través de un contrato social mediante el que las personas deben establecer las condiciones en que están dispuestas a vivir en sociedad. c) Por otro lado, la *ética del deber racional o deontológica* (Kant) pone el foco, no en las consecuencias, sino en ciertos principios y normas a los que se llega a través del uso de la razón. Este enfoque parte de que la razón que compartimos nos hace personas, con dignidad propia. Debemos hacernos tres preguntas a la hora de decidir: i) si nuestra acción es universalizable; ii) si nos sentiríamos cómodos haciendo pública nuestra decisión-acción, y iii) si estamos tratando a

éticos deseables no son una receta fácil de aplicar a casos concretos. Pensemos, por ejemplo, para cada uno de los retos que plantea la IA, quién tendría que responsabilizarse de una decisión que tome un robot cuidador; la solución habrá que sopesarla con cautela, y difícilmente será la misma para casos diversos.

En todo caso, y conscientes de la multitud de áreas de preocupación en torno a los impactos negativos de la IA en los derechos de las personas —y partiendo de las dificultades para exigir obligaciones legales en actividades que trascienden fronteras—, se hace necesario impulsar un desarrollo de la IA de forma responsable, integrando, al menos, los principios éticos en torno a los que hay consenso: transparencia, justicia, no maleficencia, responsabilidad y privacidad (Jobin *et al*., 2019).

La ética tiene un papel clave en el desarrollo de la IA. Así, en la Unión Europea se ha constituido un *Grupo de expertos de alto nivel sobre Inteligencia Artificial* que ha definido la IA fiable como aquella que es: i) lícita, es decir, que cumple la legislación aplicable; ii) ética, de modo que se garantice el respeto a los principios y valores éticos; y iii) robusta, tanto desde el punto de vista técnico como social, a fin de asegurar que los sistemas de IA, incluso si las intenciones son buenas, no provoquen daños accidentales.

La IA confiable debe cumplir los siguientes requisitos:

· Intervención y supervisión humanas. Los sistemas de IA deben facilitar sociedades equitativas, apoyando la intervención humana y los derechos fundamentales, y no disminuir, limitar o desorientar la autonomía humana.

· Robustez y seguridad. La fiabilidad requiere que los algoritmos sean suficientemente seguros, fiables y sólidos para resolver errores o incoherencias durante todas las fases del ciclo de vida útil de los sistemas de IA.

---

los demás como fines en sí mismos, y no solo como medios. d) La *ética dialógica* (Habermas) sostiene que lo éticamente adecuado puede emerger de la comunicación con otros, en lugar del razonamiento individual. Se anima al diálogo, a la argumentación y a la participación de afectados. e) La *ética de la virtud* (Aristóteles) propone que cada persona se sitúe en una función social para la que tenga buenas aptitudes y, una vez en ella, persiga la excelencia en las cualidades necesarias para desempeñar óptimamente esa función, que serían las virtudes propias de la función, incluyendo las cualidades morales (Villas y Camacho, 2022). Existen aún otras teorías éticas interesantes que exceden las limitaciones de este estudio. Nos parece esencial destacar la reivindicación de Gilligan para la incorporación de la experiencia femenina en la teoría moral, que la llevará a proponer una *ética del cuidado* que ponga el énfasis en las cuestiones de afecto y cuidado entre los seres humanos (Gilligan, 1982).

· Privacidad y gestión de datos. Los ciudadanos deben tener pleno control sobre sus propios datos, al tiempo que los datos que les conciernen no deben utilizarse para perjudicarles o discriminarles.

· Transparencia. Debe garantizarse la trazabilidad de los sistemas de IA.

· Diversidad, no discriminación y equidad. Los sistemas de IA deben tener en cuenta el conjunto de capacidades, competencias y necesidades humanas, y garantizar la accesibilidad.

Estos requisitos deben ser evaluados a lo largo de *todo el ciclo de vida* del sistema de IA de forma continua.

Hasta este momento, se han establecido códigos éticos[6] que permiten definir principios que orienten la resolución de los conflictos que origina el uso de la IA. Estos principios podrían servir para rellenar las lagunas legales que se produzcan, puesto que son muchas las consecuencias que la IA tiene en los derechos de las personas, y la regulación existente es, básicamente, la que ofrece el Reglamento General de Protección de Datos en Europa (art. 13 y 22, RGPD).

En cualquier caso, toda organización que utilice la IA para tomar decisiones deberá adoptar medidas adecuadas para salvaguardar los derechos y libertades, y los intereses legítimos del interesado, y al menos informar sobre la lógica aplicada. No se permite la utilización de decisiones individuales automatizadas, incluida la elaboración de perfiles, que produzcan efectos jurídicos en las personas o que les afecten de forma significativa, sin consentimiento de la persona involucrada. En otras palabras, existe el derecho a no ser sometido a una decisión basada exclusivamente en un tratamiento automatizado de datos personales, salvo excepciones (como el hecho de que una ley lo autorice, o la persona afectada haya dado su consentimiento o firmado un contrato). En estos dos últimos casos, existe el derecho a impugnar la decisión, expresar su punto de vista y exigir la intervención de una persona humana.

Como se ha dicho, quien utilice este tipo de tratamientos debe informar suficientemente acerca de la lógica aplicada. Sin embargo, no se han establecido

[6] Asilomar Principles (https://futureoflife.org/ai-principles/); Montreal Declaration for Responsible AI; IEEE Ethically Aligned Design v2 (https://ethicsinaction.ieee.org/); *Ethical Framework for a Good AI Society,* propuesto por el AI4People en diciembre de 2018; *Ethics Guidelines for Trustworthy AI del High-Level Expert Group on Artificial Intelligence* de la Comisión Europea de abril de 2019; UNESCO Recommendation; WWW Consortium has a great proposal on Ethics and Tecnology.

criterios concretos para determinar hasta dónde llega ese deber de información sobre la lógica aplicada en el sistema de la IA. Por este motivo, la Autoridad de Protección de Datos Británica (ICO, por sus siglas en inglés) y el Instituto Alan Turing han determinado cuál ha de ser el contenido de la explicación fundamentada que garantice la transparencia e interpretabilidad, no solo del procedimiento seguido por el modelo algorítmico, sino también de los datos utilizados por el modelo (ICO y Alan Turing Institute, 2020).

La información sobre la lógica aplicada debería consistir en explicar: i) cómo se ha ejecutado la IA y cómo se ha comportado para lograr la decisión; ii) cómo se ha diseñado el sistema y cómo se ha implementado el diagrama de flujo, incluyendo la recogida de datos, su preparación y su selección; iii) cómo los diferentes componentes de la IA son capaces de transformar los datos de entrada en datos de salida de forma específica, de manera que se puedan identificar las variables más significativas, las interacciones y parámetros del modelo implementado, y el peso e influencia de esos componentes en el logro de un resultado particular; iv) cómo los componentes técnicos de la lógica subyacente de los resultados pueden aportar evidencias para la decisión tomada; v) hasta qué punto la lógica subyacente puede comunicarse de forma inteligible y fácil de entender a los afectados por la decisión basada en IA; vi) hasta qué punto el modelo algorítmico goza de un grado de interpretabilidad consistente con el impacto producido en el afectado por la toma de decisión; y vii) qué tipo de herramientas de explicación suplementaria pueden ayudar a explicar la complejidad del sistema de forma suficiente para proveer una información comprensible y completa de la lógica aplicada por parte de la IA.

1.1.3. Avances en la regulación de la IA

En la UE está en fase de discusión una regulación sobre IA[7] que ayudará a despejar muchas de las incógnitas que se plantean en el uso de estos sistemas. La propuesta de Reglamento de la Inteligencia Artificial es el primer marco legal sobre esta tecnología, que además llega acompañada de otra normativa sobre maquinaria y robots. Se trata de una nueva normativa sobre IA que quiere garantizar la seguridad y fortalecer su inversión en la UE, creando varios niveles de riesgo y prohibiendo el reconocimiento facial en determinadas situaciones.

[7] Propuesta de regulación de la inteligencia artificial de abril de 2021. Disponible en: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

La propuesta de la Comisión Europea para regular la IA utiliza un enfoque basado en riesgos. Los riesgos se clasifican en cuatro niveles:

1. El mayor es el riesgo inaceptable, el que constituye una amenaza para la seguridad, los medios de vida y los derechos de las personas. Estos sistemas de IA estarán prohibidos, como el caso de la IA diseñada para manipular comportamientos y los sistemas de puntuación social, que dan una valoración social en función del comportamiento digital de los ciudadanos.

2. En un segundo lugar está el riesgo alto, en el que se incluyen usos de la IA en infraestructuras críticas que puedan afectar a la salud de la ciudadanía, usos de IA aplicada en la educación, componentes en cirugía, sistemas de reclutamiento de personal, servicios públicos, legislación, inmigración o IA para la Administración pública o la justicia. En todos estos ámbitos, la IA deberá estar sujeta a obligaciones estrictas, entre las que se incluye un análisis de riesgos, trazabilidad de resultados, documentación detallada, supervisión humana y un alto nivel de robustez.

3. En un nivel más bajo, de riesgo limitado, se incluyen los sistemas como *chatbots*, que deberán tener un mínimo nivel de transparencia y donde los usuarios deberán ser advertidos de que están hablando con una máquina.

4. En el riesgo mínimo se engloban el resto de los usos, como videojuegos, aplicaciones de imagen u otros sistemas de IA, que no impliquen riesgos. En estos casos, la nueva normativa no especifica ninguna medida.

La UE quiere impulsar el desarrollo de estándares para la IA y propone a las distintas organizaciones nacionales que supervisen esta normativa. Adicionalmente, desde la Comisión Europea invitan a la creación de códigos voluntarios de conducta para los sistemas de IA sin riesgos.

Además, de forma tímida, empieza a haber alguna jurisprudencia que reconoce la transparencia de los algoritmos en la toma de decisión por parte del sector público, como las sentencias del Tribunal Administrativo regional Lazio-Roma de 2017 y de 2019, y las decisiones de la Comisión francesa de acceso a documentos administrativos (2015, 2018) (Cotino Hueso; Soriano Arnanz, 2021). En Italia (Carloni, 2020), una última sentencia dictada en diciembre de 2019 por el Consejo de Estado define un primer decálogo de legalidad algorítmica

que se inspira significativamente en los principios del Reglamento europeo sobre protección de datos personales.

Por su parte, tal y como se explicará más adelante, en Holanda se utilizó un algoritmo por parte de los servicios sociales: *SyRI*, un sistema de indicación de riesgos que clasificaba a los receptores de ayudas sociales. Cuando el asunto llegó a los tribunales, se dio la razón al demandante, que alegaba vulneración de sus derechos. Pero, igual que en el caso del bono social energético en España, no se entendió que había que dar publicidad al código fuente del algoritmo.

Otro ejemplo de avance en la regulación es la recientemente aprobada Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación[8], en España, en la que se establecen requisitos de los algoritmos utilizados en el ámbito de las Administraciones públicas.

A su vez, la transparencia de los algoritmos en el ámbito laboral está siendo reconocida, poco a poco, en diferentes regulaciones: en el caso español, la Ley Riders (Real Decreto-ley 9/2021, de 11 de mayo, por el que se modifica el texto refundido de la Ley del Estatuto de los Trabajadores) incluye el derecho a estar suficientemente informado sobre el uso de los sistemas algorítmicos que le afectan.

En América Latina, hay que destacar la propuesta de modificación constitucional para la transparencia algorítmica en Brasil. También en Chile, el 11 de marzo de 2022, se publicó la Ley nº 21.431 que "Modifica el Código del Trabajo regulando el Contrato de Trabajadores de Empresas Digitales de Servicios". En dicha ley hay un avance relevante del marco regulatorio de la IA en el país, al prohibir la discriminación por parte de los algoritmos. El artículo 152 quinquies E del Código del Trabajo recoge desde esa fecha la obligación de ga-

[8] Artículo 23. *Inteligencia Artificial y mecanismos de toma de decisión automatizados*. 1. En el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la inteligencia artificial, las Administraciones públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las Administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio. 2. Las Administraciones públicas, en el marco de sus competencias en el ámbito de los algoritmos involucrados en procesos de toma de decisiones, priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos. 3. Las Administraciones públicas y las empresas promoverán el uso de una inteligencia artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido. 4. Se promoverá un sello de calidad de los algoritmos.

rantizar el derecho a la no discriminación algorítmica, especialmente en la asignación de trabajo, oferta de bonos e incentivos, por ejemplo.

En EE.UU. también ha habido avances con la aprobación de la Ley de Transparencia algorítmica de 2022[9]. Previamente, en el asunto del algoritmo de apoyo a los jueces para calcular el riesgo de reincidencia de una persona condenada (COMPAS) la Corte Suprema de Justicia no dio la razón al demandante. Por último, Canadá, a través de la Directiva sobre toma de decisiones automatizadas, ha sido uno de los primeros países en desarrollar una aplicación para medir y mitigar los impactos negativos en los derechos humanos de los sistemas de IA que se usan en servicios públicos.

1.2. Contexto ético, social y tecnológico de las neurotecnologías

Otro ámbito tecnológico que genera impactos éticos y sociales importantes es el de las neurotecnologías. Partiendo del estudio del cerebro, las neurotecnologías tienen muy diversas aplicaciones, entre ellas, la contribución a la curación de enfermedades neurológicas. Estas tecnologías utilizan tanto la neurociencia —el estudio del cerebro—, como la ingeniería —la aplicación de la ciencia y la tecnología para resolver problemas— y la IA —la ciencia que estudia y crea sistemas artificiales inteligentes—. Estas tecnologías reciben el nombre NBIC (nano-bio-info-cogno): nanotecnologías, biotecnologías, tecnologías de la información y ciencias cognitivas[10].

Hoy día se puede registrar la actividad neuronal y actuar sobre regiones del cerebro. Tal y como explican Ienca y Andorno (2017), Neurofocus —una multinacional estadounidense de neuromarketing recientemente adquirida por Nielsen— probó técnicas subliminales con el fin de obtener respuestas (por ejemplo, preferir el artículo A en lugar del B) que las personas no podían registrar conscientemente (Penenberg, 2011). Estas técnicas incluían la incrustación de estímulos de menos de 30 milisegundos, es decir, por debajo del umbral de percepción consciente. Todo esto deja clara la necesidad de analizar las implicaciones éticas y legales derivadas del uso de los datos neuronales, para evitar finalidades distintas a las consentidas en el inicio de un tratamiento. Aunque parece claro que por el camino se pueden abrir innume-

[9] Véase: H.R.6580 - Algorithmic Accountability Act of 2022. Disponible en: https://www.congress.gov/bill/117th-congress/house-bill/6580/text. Y Berkeley University: Center for Equity, Gender, and Leadership (2022) Mitigating bias in AI.

[10] Véase: https://theconversation.com/la-urgencia-de-los-neuroderechos-humanos-176071.

rables ventajas en educación, medicina y neurología, también se generan riesgos que deben controlarse.

Este tema constituye una preocupación en algunas cartas de derechos digitales, como la española, que incluye un apartado con los principios que deben orientar su regulación, y la de cualquier otra novedad tecnológica, que pueda incidir sobre: i) el control de cada persona sobre su identidad; ii) la autodeterminación individual, soberanía y libertad en la toma de decisiones; iii) la confidencialidad y seguridad de los datos obtenidos o relativos a sus procesos cerebrales; iv) el uso de interfaces persona-máquina susceptibles de afectar a la integridad física o psíquica de la persona, y v) la garantía de que las decisiones basadas en neurotecnologías no sean condicionadas por el suministro de datos.

Algunos autores como Suárez Xavier (2022) entienden que habría que vincular los neuroderechos al derecho a la identidad digital (derecho que se desprende del libre desarrollo de la personalidad del art. 10 de la Constitución Española), que, por otro lado, también aparece reconocido en la carta de derechos digitales española.

Según el Tribunal Europeo de Derechos Humanos, el derecho a la identidad está reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos (por ejemplo, Sentencia de 28 de enero de 2003, Peck c/ Reino Unido). En su Sentencia 26 de junio de 2014, en los asuntos 65192/11 (Mennesson c/ Francia) y 65941/11 (Labassee c/Francia), el Tribunal recuerda que el derecho a la propia identidad forma parte integral de la noción de vida privada (Mañas, 2020).

Desde el Parlamento Europeo (2022)[11], por su parte, se ha pedido a la Comisión:

> que estudie la posibilidad de presentar una iniciativa relativa a los neuroderechos, con el objetivo de proteger el cerebro humano contra la injerencia, la manipulación y el control por parte de la neurotecnología impulsada por la inteligencia artificial (IA) y anima a la Comisión a que defienda una agenda de neuroderechos a nivel de las Naciones Unidas con el fin de incluir estos derechos en la Declaración Universal de Derechos Humanos, concretamente en lo que respecta a los derechos a la identidad, al libre albedrío, a la privacidad mental, a la igualdad de acceso a los avances en materia de aumento del cerebro y a la protección frente al sesgo algorítmico (Resolución sobre la inteligencia artificial en la era digital, párrafo 247).

[11] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_ES.html.

Por lo demás, no existen ejemplos de países que hayan regulado esta cuestión, salvo el intento de constitucionalización de los neuroderechos en Chile. Una experiencia muy relevante es el caso del proyecto de ley que se está discutiendo en Brasil, en el que se define el dato neuronal como "cualquier información obtenida directa o indirectamente de la actividad del sistema nervioso central y cuyo acceso se realiza por medio de interfaces cerebro-ordenador, o cualquier otra tecnología, invasiva o no" (Proyecto de Ley que modifica la Ley n° 13.709, de 14 de agosto de 2018, o Ley General de Protección de Datos Personales).

2. ¿Cómo preservar los derechos digitales afectados por la IA y las neurotecnologías?

2.1. ¿Nuevos derechos digitales?

Los derechos digitales son derechos destinados a preservar la dignidad humana en la sociedad digital, lo que supone un reto social, filosófico, político, económico, técnico y jurídico de enorme relevancia. Hasta hace poco había un consenso acerca de la idéntica importancia de los derechos *offline* y *online* (Consejo de Derechos Humanos de las Naciones Unidas, 2018). Sin embargo, en la actualidad se está planteando la posibilidad del reconocimiento de nuevos derechos digitales (Agenda Digital 2025 del Gobierno de España), y en la doctrina se encuentran cada vez más opiniones a favor de ello (Barrio Andrés, Artemi Rallo, Ienca, Custers). Los retos que presenta la sociedad digital son grandes, no solo en cuanto a actores que intervienen, sino a cómo se gestionan los contenidos y a cuáles son los nuevos patrones de regulación. La ciudadanía se encuentra inserta en esta nueva sociedad y está cambiando su propia identidad.

La propuesta de nuevos derechos digitales ha sido importante en el marco de la IA (Laukyte, 2021: 183 y ss.) y en el de las neurotecnologías (Ienca, Andorno, 2017; Yuste, Genser y Herrmann, 2021: 154 y ss.). Sin embargo, hay parte de la doctrina que se plantea la necesidad de una reflexión más sosegada:

> De los cinco grandes grupos de neuroderechos a los que se refiere por ejemplo Ienca (Ienca, 2021), que coinciden en gran medida con los propuestos por Yuste y otros (Yuste/Genser/Herrmann, 2021), tres son fácilmente reconducibles a derechos y garantías ya existentes (libertad de pensamiento, privacidad e integridad). Sin embargo, el derecho a la identidad, que tiene una proyección sui

> generis en el campo de los derechos digitales a través de la identidad digital, no ha encontrado una plasmación jurídica en las Constituciones (salvo en la portuguesa). Y el derecho al igual acceso a la mejora sigue planteando la discusión previa sobre qué mejoras son éticamente aceptables (De Asís Roig, 2022: 36).

En todo caso, será importante contar con un sistema de garantías que haga eficaces los nuevos derechos digitales. El derecho de internet tiene algunas especificidades, puesto que debe poner de acuerdo a actores muy diversos con intereses diferentes: el Estado, las organizaciones —empresariales o de otro tipo—, las instituciones regionales e internacionales, la ciudadanía, etc. Este proceso regulatorio suele denominarse gobernanza, más que regulación —que supondría algo gestionado por cada Estado—; sin embargo, la mayor parte de las normas vinculantes en internet suelen aprobarse mayoritariamente por los Estados (Barrio, 2021).

Una cuestión que merece la pena resaltar es el hecho de que en la génesis de la mayoría de los derechos humanos no solo está el Estado, sino también las empresas y las diferentes organizaciones de la sociedad civil —aunque generalmente en menor medida—, que presionan a favor de una determinada regulación. Así sucedió en Brasil con el Marco Civil de Internet de 2014, sobre el que se trata en otros capítulos de este libro.

Un ejemplo muy claro de esto en España fue la declaración de inconstitucionalidad por el Tribunal Constitucional (TC) español de una previsión sobre el uso de IA por parte de los partidos políticos en España[12]. El asunto fue impulsado por la Asociación Pro Derechos Humanos de España y la Fundación Alternativas. Se entendió que el uso de IA para elaborar perfiles de los ciudadanos por parte de los partidos políticos no tenía cobertura legal, y podría traer consigo situaciones como la vivida con Cambridge Analytica.

2.2. Las cartas de derechos digitales

Existen distintas clasificaciones de derechos digitales, en función de las diversas declaraciones existentes.

La Carta Portuguesa de los Derechos Humanos en la Era Digital[13] fue la primera en Europa y reconoce algunos derechos clásicos, como las libertades de

[12] Art. 58.bis de la LOPDGDD (Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales).

[13] Aprobada por la Ley nº 27/2021, del 17 de mayo. Disponible en: https://www.parlamento.pt/Legislacao/Paginas/Educacao_Carta-Portuguesa-de-Direitos-Humanos-na-Era-Digital.aspx.

expresión, manifestación, asociación o participación en el mundo digital. Además reconoce otros derechos recientes, como el derecho al olvido y la protección contra la geolocalización abusiva, el uso de la IA y los robots.

En España, la Carta de Derechos Digitales, aprobada pocos meses después (julio de 2021) estableció con más profundidad seis categorías principales de derechos: i) derechos de libertad; ii) de igualdad; iii) de participación y de conformación del espacio público; iv) del entorno laboral y empresarial; v) derechos digitales en entornos específicos, y vi) de garantías y eficacia. La Tabla 1 desglosa el contenido de las cinco primeras categorías.

Tabla 1. Derechos incluidos en la Carta Española de Derechos Digitales

Derechos de libertad	**Derechos de igualdad**
- Derechos y libertades en el entorno digital. - Derecho a la identidad en el entorno digital. - Derecho a la protección de datos. - Derecho al pseudonimato. - Derecho de la persona a no ser localizada y perfilada. - Derecho a la ciberseguridad. - Derecho a la herencia digital.	- Derecho a la igualdad y a la no discriminación en el entorno digital. - Derecho de acceso a internet. - Protección de las personas menores de edad en el entorno digital. - Accesibilidad universal en el entorno digital. - Brechas de acceso al entorno digital.
Derechos de participación y de conformación del espacio público	**Derechos del entorno laboral y empresarial**
- Derecho a la neutralidad de internet. - Libertad de expresión y libertad de información. - Derecho a recibir libremente información veraz. - Derecho a la participación ciudadana por medios digitales. - Derecho a la educación digital. - Derechos digitales de la ciudadanía en sus relaciones con las Administraciones públicas.	- Derechos en el ámbito laboral. - La empresa en el entorno digital.
Derechos digitales en entornos específicos	
- Derecho de acceso a datos con fines de archivo en interés público, fines de investigación científica o histórica, fines estadísticos, y fines de innovación y desarrollo. - Derecho a un desarrollo tecnológico y un entorno digital sostenible. - Derecho a la protección de la salud en el entorno digital. - Libertad de creación y derecho de acceso a la cultura en el entorno digital. - Derechos ante la IA. - Derechos digitales en el empleo de las neurotecnologías.	

Fuente: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf.

En la UE se ha aprobado también una Declaración de Derechos Digitales suscrita por el Consejo, el Parlamento Europeo y la Comisión el 15 de diciembre de 2022. En ella se recogen principios y derechos clave en materia de transformación digital, tales como el carácter central de las personas y sus derechos, el apoyo a la solidaridad y la inclusión, la garantía de la libertad de elección en línea, el fomento de la participación en el espacio público digital, el aumento de la seguridad, la protección y el empoderamiento de las personas, y la promoción de la sostenibilidad del futuro digital.

Además, resulta esencial destacar el papel que desempeñará el Reglamento de Mercados Digitales aprobado en la UE, que se aplicará desde el año 2024, el cual establecerá la obligación a los prestadores de supervisar contenidos ilícitos que tengan conexión esencial con la UE, obligando por ejemplo a plataformas a borrar contenido dañino e ilegal, las cuales se enfrentarán a sanciones si no actúan acorde a la ley. Dentro de los tópicos más relevantes que serán revisados, se considera la incitación al odio, la desinformación y productos falsificados de venta en línea. Asimismo, la regulación permitirá a los usuarios opinar sobre lo que ven en línea, abriendo un canal de comunicación con la ciudadanía respaldado por un marco regulatorio. La nueva ley afectará a plataformas e intermediarios en línea como Twitter y Facebook, tiendas de aplicaciones, plataformas para compartir vídeos y música, como YouTube y Spotify, sitios de viajes en línea como Airbnb y otros mercados digitales, con especial atención a las grandes plataformas en línea, aquellas con más de 45 millones de usuarios activos al mes.

Por su parte, en Perú, desde la Presidencia del Consejo de Ministros y la Secretaría de Gobierno y Transformación Digital, se elaboró una Carta Peruana de Derechos Digitales en 2022[14], buscando "presentar a la ciudadanía una visión desde el Estado Peruano sobre el ejercicio y protección de los derechos a través del uso de las tecnologías digitales, así como orientar el desarrollo de las políticas públicas, con el objetivo de extender y profundizar la transformación digital en todos los ámbitos de la sociedad peruana".

La carta se abrió a un proceso de revisión por parte de la ciudadanía y considera preliminarmente 24 derechos digitales distribuidos en seis categorías: i) derechos relacionados con la protección de la persona en entornos digitales, ii) derechos que se ejercen en entornos o por medios digitales, iii) habilitadores, iv) derechos específicos para niñas, niños y adolescentes, v) derechos relacio-

[14] https://cdn.www.gob.pe/uploads/document/file/3454811/Derechos%20Digitales.pdf?v=1658950464.

nados con la Administración pública y vi) derechos específicos para el entorno laboral.

Entre los derechos relativos al uso de la IA y las neurotecnologías, se destaca el derecho a la identidad digital en el artículo 2, como "aquel conjunto de atributos que individualizan y permiten identificar a una persona en entornos digitales. El Estado promueve el acceso a los medios para que las personas puedan identificarse en el entorno digital, sin discriminación y priorizando a los grupos especialmente vulnerables". Por otro lado, en el capítulo de habilitadores, se menciona el uso de tecnologías emergentes, como la IA, explicitando que el Estado promueve su adopción, priorizando aquellas que permitan la realización de los derechos digitales mencionados en la carta. Finalmente, dentro de la categoría de los derechos relacionados con la Administración pública, el Estado se compromete de igual forma a promover la creación de canales digitales de atención, de forma que no habiliten nuevos tipos de discriminación, especialmente la que se realiza en función de la condición económica, social, por idioma o edad, o de cualquier otra índole. Por último, otro ejemplo en Latinoamérica es el caso del Marco Civil de internet en Brasil[15]. Representó la primera legislación vinculante sobre derechos digitales en la región y en ella se establecen "los principios, garantías, derechos y deberes para el uso de internet en Brasil".

3. Buenas prácticas desde la política pública. El Consejo para la Transparencia de Chile

3.1. Agendas nacionales e internacionales de IA

Desde el Observatorio de Políticas Públicas de Inteligencia Artificial de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), se ha realizado un análisis de las agendas y programas de IA por país a nivel global. En este sentido, gran parte de los países de América Latina, así como de la UE, cuentan con un programa que busca trazar objetivos a corto, mediano y largo plazo considerando las oportunidades, retos y necesidades de cara a 2030.

En este contexto, la OCDE supervisa que estas agendas reflejen un interés común por parte de los gobiernos y otros actores, orientado a la generación de una IA para el desarrollo de confianza, es decir, aquella que respeta principios

[15] Ley 12.965 del 23 de abril de 2014. Disponible en: https://bd.camara.leg.br/bd/handle/bdcamara/25560.

basados en el crecimiento inclusivo, el desarrollo sostenible y el bienestar, un enfoque centrado en las personas y la equidad, la transparencia y explicabilidad, la robustez y seguridad, o la rendición de cuentas.

Otra fuente que recoge buenas prácticas es el Observatorio alemán de IA en el trabajo y la sociedad, asociado al OECD.AI. Además, la evaluación canadiense ofrece un algoritmo en línea que obtiene puntuaciones de impacto bruto y de mitigación. Desde 2016 el gobierno francés, el Estado de California y el gobierno del Reino Unido llevan a cabo un trabajo relevante en este ámbito (Aguirre, 2022).

Por lo que se refiere a América Latina, a partir de los datos de la OCDE, en la Tabla 2 se mencionan nueve países iberoamericanos, indicando los principios que han incorporado en sus agendas de IA[16] (entre ellos, los programas nacionales que mencionan como beneficiarios directos a la sociedad civil son Argentina, Chile, Colombia y Costa Rica).

[16] Inclusive growth, sustainable development and well-being.
Disponible en: https://oecd.ai/en/dashboards/ai-principles/P5; Human-centred values and fairness.
Disponible en: https://oecd.ai/en/dashboards/ai-principles/P6; Transparency and explainability.
Disponible en: https://oecd.ai/en/dashboards/ai-principles/P7; Robustness, security and safety.
Disponible en: https://oecd.ai/en/dashboards/ai-principles/P8; Accountability.
Disponible en: https://oecd.ai/en/dashboards/ai-principles/P9.

Tabla 2. Programas nacionales y principios de IA de la OCDE incluidos

	Inclusive growth, sustainable development and well-being	Human-centered values and fairness	Transparency and explainability	Robustness, security and safety	Accountability
Argentina[17]	✔	✔			
Brasil[18]		✔	✔		
Chile[19]					
Colombia[20]	✔				
Costa Rica[21, 22]	✔				
México[23]	✔				
Perú[24]	✔	✔	✔		✔
España[25]	✔	✔	✔	✔	
Uruguay[26, 27]	✔				
UE[28, 29]	✔	✔	✔	✔	✔

Fuente: Elaboración propia.

[17] https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-26935.
[18] https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-27104.
[19] https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-24840.
[20] https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-26728.
[21] Digital Transformation Strategy: The Bicentennial Of Costa Rica.
[22] https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-25382.
[23] https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-26703.
[24] https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiat
[25] https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-27013.
[26] AI Strategy for The Digital Government.
[27] https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-26477.
[28] Coordinated Plan on Artificial Intelligence.
[29] https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-24126 / https://oecd.ai/en/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-23955.

3.2. El Consejo para la Transparencia y el Gob_Lab UAI

Un ejemplo de colaboración público-privada para enfrentar estos desafíos lo representa el estudio realizado por el Consejo para la Transparencia en Chile, junto con el Gob_Lab de la Universidad Adolfo Ibáñez, en octubre de 2021, sobre la transparencia algorítmica en el sector público a nivel nacional. Se llevó a cabo con el objetivo de conocer un estado del arte del uso de los sistemas de decisión automatizados, partiendo de la información básica respecto de su existencia, identificación, propósito y la información pública disponible.

En este sentido, tras un proceso de selección, se tomaron doce sistemas de decisión automatizada (SDA, en adelante) usados en organizaciones públicas de diversa índole y sectores —como los de la salud, educación, economía, agricultura, y vivienda y urbanismo—, tanto en ministerios como municipalidades (Tabla 1). La transparencia y disponibilidad de información de los SDA se analizó considerando trece criterios, teniendo como marco de referencia la propuesta "Transparency mechanisms for UK public-sector algorithmic decision-making systems" del Instituto Ada Lovelace del Reino Unido (por sus similitudes, dicho marco de referencia se ajusta al escenario normativo chileno).

Los criterios para determinar la transparencia de cada SDA fueron: i) relación con la habilitación legal; ii) relación con las políticas de gobierno que implementa; iii) fuente de los datos; iv) quién opera el SDA; v) quién lo construyó; vi) propósito del sistema; vii) indicación del sistema desarrollado y alternativas que fueron evaluadas para la selección; viii) funcionamiento del sistema (lógica asociada al sistema); ix) costo o valor; x) actores privados involucrados; xi) impactos en grupos específicos: indicar grupos e impactos; xii) acciones de mitigación en impactos o riesgos; y xiii) monitoreo de funcionamiento del sistema. Los principales hallazgos en la búsqueda de información de los sistemas para evaluar su transparencia algorítmica se muestran en la Tabla 3. De manera sintética, el estudio señaló los siguientes resultados:

1. Para el subconjunto de los sistemas seleccionados, ha existido un avance fortuito en materia de transparencia algorítmica impulsado por leyes de transparencia y participación de la ciudadanía en la gestión pública.

2. La información, si bien está disponible, se encuentra dispersa y fragmentada, existiendo distintas fuentes de información de los SDA.

3. La información presentada no cuenta con un destinatario definido, es casuística y responde a diversos objetivos de publicación.

4. Fue necesario un esfuerzo relevante para sistematizar la información disponible, para presentarla de manera coherente y adecuada al estándar de transparencia algorítmica, dado que estaba dispersa, en diferentes plataformas y fuentes, para diversos destinatarios y en formatos disímiles.

5. En la mayoría de los casos la información pública de los SDA era elaborada por el propio organismo. Esto demuestra que, en muchos casos, sería posible aprovechar las capacidades de los propios organismos para dar cumplimiento a los requerimientos que se le realicen en materia de transparencia algorítmica. En otros casos, la fuente de la información se encontró en proveedores privados de los sistemas de manera bastante completa.

6. En el ejercicio realizado fue posible encontrar explicaciones de alto nivel, que no infringen los derechos de propiedad intelectual asociados a los SDA desarrollados.

7. Al constituir un universo dispar de resultados encontrados en la Administración del Estado de los SDA implementados, resulta necesario, al menos en una primera etapa, enfocar los esfuerzos de transparencia en sistemas que desarrollen operaciones críticas o de mayor relevancia para el ciudadano que se relaciona con estos.

Tabla 3. SDA seleccionados para evaluación de transparencia

Organización	Sistema
FONASA	Red neuronal análisis de licencias médicas
MINSAL	DART
Municipalidad de Pedro Aguirre Cerda	RAYEN
Municipalidad de Renca	Centinela
Gobernación Provincial de San Antonio	Algoritmo de reserva de hora de extranjería
MINEDUC	SAE
Universidad de Aysén	Sistema de alerta temprana
INIA	Plan Predial
SAG	RPF
MINVU	Subsidio de clase media
MINVU	Selección beneficio de arriendo
FOSIS	Asistente virtual

Fuente: SDA seleccionados para evaluación de transparencia. "Transparencia algorítmica en el sector público", Consejo para la Transparencia y Gob_Lab UAI (2021).

Tabla 4. Resultados de la evaluación de la transparencia algorítmica

Criterio	FONASA Redes neuranles	MINSAL DART	M. PAC IRIS	M. Renca Centinela	GPSA Hora	MINEDUC SAE	U. Aysén SAT	INIA Plan Predial	SAG RPF	MINVU SCM	MINVU SAH	FOSIS A. Virtual
1												
2	X	X		X		X	X	X	X	X	X	X
3	X	X	X	X	X	X	X	X	X	X	X	X
4	X	X	X	X	X	X	X	X	X	X	X	X
5	X	X	X	X		X		X	X			X
6	X	X	X	X	X	X	X	X	X	X	X	X
7	X	X		X			X					X
8	X	X	X	X		X		X	X			X
9		X		X				X	X			
10		X	X	X		X		X	X			
11	X	X	X	X	X	X	X	X	X	X	X	X
12	X	X						X	X			X
13	X	X				X		X	X			X
Total	**11**	**12**	**7**	**10**	**4**	**9**	**6**	**11**	**11**	**5**	**5**	**11**
%	**85%**	**92%**	**54%**	**77%**	**31%**	**69%**	**46%**	**85%**	**85%**	**38%**	**38%**	**85%**

Fuente: SDA seleccionados para evaluación de transparencia. "Transparencia algorítmica en el sector público". Consejo para la Transparencia y Gob_Lab UAI (2021).

4. Otros ejemplos de buenas prácticas

Junto con la necesidad de desarrollar buenas políticas públicas y marcos regulatorios que permitan capturar las oportunidades que ofrece la IA, así como mitigar sus riesgos, es relevante también que se generen buenas prácticas desde otros sectores y ecosistemas, que frecuentemente son aquellos que están desarrollando tecnologías e incidiendo en esta temática.

Un ejemplo de ello es la guía de aplicación "Autoevaluación ética de la IA para actores del ecosistema emprendedor" lanzada por BID Lab en 2021, a través de fAIr LAC (https://fairlac.iadb.org/); se trata de una iniciativa que promueve el uso ético y responsable de la IA, que constituye una herramienta práctica de autoevaluación ética para el ecosistema emprendedor, y que permite analizar el desarrollo tecnológico basado en IA, así como el manejo de datos. Con sus diagnósticos, busca facilitar la identificación de potenciales riesgos para prevenir errores, sesgos, discriminaciones, exclusiones u otros impactos negativos resultantes del desarrollo tecnológico. La guía permite una evaluación en las áreas de conceptualización y diseño; gobernanza y seguridad; involucramiento humano en los sistemas de IA; ciclo de vida de la IA (datos y algoritmos); actores relevantes y comunicaciones.

En el ámbito sanitario, un ejemplo que merece la pena destacar es Portal Telemedicina, diseñado por una alianza entre Google California, Google Brasil, la Secretaría de Salud del Estado de São Paulo (SESSP) y la Fundación de Apoyo a la Investigación del Estado de São Paulo (FAPESP). Portal Telemedicina es una plataforma de telediagnóstico que se integra directamente con los dispositivos médicos, así como con los sistemas de salud electrónicos (EHR, por sus siglas en inglés), radiología y laboratorio, capturando y transfiriendo datos automáticamente a través de la nube, donde los médicos pueden diagnosticar en una aplicación web segura. Se trata de una aplicación de algoritmos de aprendizaje automático para predecir los hallazgos médicos, que se utiliza para detectar emergencias y clasificar los exámenes. Además, el sistema comprueba los diagnósticos contrarios a la predicción de la IA y, en caso de discrepancia, envía automáticamente el examen a otros tres médicos para minimizar el error humano (Roveri, 2022).

Otro ámbito de buenas prácticas a explorar es el litigio estratégico. Existen pocos pronunciamientos de los jueces acerca de la legalidad de los tratamientos de IA. Un asunto que ha sido ampliamente estudiado por la doctrina es la sentencia del Tribunal de Distrito de La Haya, de 5 de febrero de 2020[30], mencio-

[30] https://www.openglobalrights.org/landmark-judgment-from-netherlands-on-digital-welfare-states/?lang=Spanish

nado más arriba. El caso surge de la utilización de un algoritmo por parte de los servicios sociales en Holanda: *SyRI* era un sistema de indicación de riesgos que se utilizaba para clasificar a los receptores de ayudas sociales. El sistema incluía datos personales de los interesados, y se alimentaba de informes sucesivos elaborados a partir de esa información personal. Las personas no eran conscientes de esos nuevos datos personales que se iban generando por parte de los algoritmos ni autorizaban en ningún momento su uso.

Este caso pone de manifiesto que los servicios sociales pueden conseguir mejores resultados a través de la optimización de procesos que trae consigo la IA. Sin embargo, será necesario encontrar un equilibrio entre la injerencia en la vida privada de la ciudadanía que esta optimización requiere y el objetivo legítimo que se persigue, es decir, la racionalización del uso de los recursos disponibles por parte del Estado.

En general, la sociedad civil está reflexionando y aportando acerca de los asuntos planteados en este texto: piénsese en organizaciones como Open Knowledge Foundation, Quadrature du NeT, Algorithm Watch, Ranking Digital Rights, Asociación para el Progreso de las Comunicaciones (APC), Derechos Digitales, Algo.rights, Algo.race, Amnistía Internacional, ONGAWA, IRIGHTS, IT for Change, Just Net Coalition, entre otras.

Otros ejemplos de buenas prácticas —sin ánimo de exhaustividad— son los que señalamos a continuación, que suponen esfuerzos desde distintas instancias, dirigidos a poner a la persona en el centro de los avances tecnológicos:

· Naciones Unidas: el Grupo de Amigos sobre Tecnologías Digitales 9, alineado con los ODS, busca maximizar el impacto positivo de las nuevas tecnologías y mitigar posibles riesgos negativos. Está presidido por México, Finlandia y Singapur (Gómez Mont *et al.*, 2020).

· UNESCO: Recomendación sobre la Ética de la IA (https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa).

· Digital 9: foro internacional que agrupa a nueve países pioneros en el avance de prácticas digitales en beneficio de sus ciudadanos. México y Uruguay son los únicos países latinoamericanos que forman parte de este grupo; en 2019 Uruguay asumió la presidencia del foro. Cuenta con un grupo temático de IA (Gómez Mont *et al.*, 2020).

· Alianza del Pacífico: en 2017 se lanzó la Agenda Digital, así como la Hoja de Ruta que traza el camino para mejorar la competitividad de sus cuatro países (México, Perú, Colombia y Chile) a través de las tecnologías de la información y de las comunicaciones (TIC). La alianza busca marcar la pauta en IA, entre otros temas, para dar una señal de compromiso social (Gómez Mont *et al.*, 2020).

· La Corporación Andina de Fomento (CAF) ha llevado a cabo un esfuerzo muy interesante, en alianza con empresas como Microsoft o Telefónica, para aportar en la reflexión que nos ocupa[31].

· Red GEALC: la Red para el Desarrollo del Gobierno Electrónico para América Latina y el Caribe creó en 2018 el Grupo de Trabajo de Tecnologías Emergentes liderado por México. Este grupo realizó un primer mapeo de las diferentes iniciativas regionales (Gómez Mont *et al.*, 2020).

· G20: los ministros de Economía Digital del G20 debatieron cómo se pueden diseñar y aplicar políticas digitales para maximizar los beneficios y minimizar los retos del desarrollo de la economía digital, y para superar los desafíos con especial atención a los países en desarrollo y poblaciones subrepresentadas (https://www.mofa.go.jp/mofaj/files/000486596.pdf).

· Open Government Partnership.

· Institute of Electrical and Electronics Engineers (IEEE): su trabajo en el ámbito de la generación de conocimiento, estandarización e inclusión de la ética en la IA (Ethically Aligned Design) es muy relevante (https://ieeexplore.ieee.org/document/6733947).

· Ada Lovelace Institute.

· AI Now Institute.

· Iniciativas desde la academia: la red europea COST sobre derechos digitales (https://gdhrnet.eu/); el Centro de Internet y Sociedad de la Universidad de Oxford (https://www.oii.ox.ac.uk/); la Universidad de Harvard (https://cyber.har-

[31] CAF (2021) EXPERIENCIA. Datos e inteligencia artificial en el sector público.

vard.edu/); el Berkeley Haas Center for Equity, Gender & Leadership (https://haas.berkeley.edu/equity/industry/playbooks/mitigating-bias-in-ai/); la línea de Ética y Revolución digital del Centro de Innovación en Tecnología para el Desarrollo Humano de la Universidad Politécnica de Madrid (https://itd.upm.es/catedraods/etica-y-revolucion-digital/).

Destaca de manera muy especial el consenso al que se llegó en el ámbito de la UNESCO con la "Recomendación sobre la ética de la Inteligencia artificial". En ella se recuerda que los Estados miembros deberían alentar a las entidades públicas, las empresas del sector privado y las organizaciones de la sociedad civil a incorporar a diferentes partes interesadas a su gobernanza en materia de IA. Y también a considerar la posibilidad de añadir una función de responsable independiente de la ética de la IA o algún otro mecanismo para supervisar las actividades relacionadas con la evaluación del impacto ético, las auditorías y el seguimiento continuo, así como para garantizar la orientación ética de los sistemas de IA.

Asimismo, aporta elementos importantes para la región el documento de la Corporación Andina de Fomento citado. Se destaca la necesidad de abordar la IA desde un enfoque estratégico garantizando un marco ético para todo el ciclo vital de esta tecnología. Para ello se requiere la implicación de todos los actores y la necesidad de una cooperación multisectorial y transversal en la sociedad. Las recomendaciones propuestas tienen el objetivo de llevar adelante estrategias de uso efectivo, ético y responsable de la IA gracias a la mejora tanto en la formulación, la ejecución y la evaluación de las políticas públicas, y los servicios a la ciudadanía, cuanto en la gestión interna de los gobiernos. Con el fin de poder fomentar la sostenibilidad socioeconómica y ambiental en Iberoamérica, los Estados tienen que definir e implementar una política pública y una estrategia a largo plazo basadas en principios éticos *y derechos humanos* [añadido nuestro]. La gobernanza de los datos y los algoritmos debe ser soportada por un marco regulatorio adecuado. La fuerza laboral debe contar con preparación técnica y cultural que asegure la adaptación y la apropiación de la inteligencia artificial y que —eliminando la concepción de la inteligencia artificial genérica todopoderosa— nunca reemplace ni supere a las personas *y su dignidad* [añadido nuestro].

Las recomendaciones son las siguientes:

· Construir e implementar una política pública de IA basada en principios éticos, compromisos y una acción coordinada alrededor de metas comunes involu-

crando a los diferentes actores de la sociedad con liderazgo político y capacidad de coordinación.

· Diseñar estrategias y hojas de ruta flexibles, porque es una tecnología en constante evolución, y las realidades en diferentes niveles de gobierno y comunidades son variadas.

· Crear estructuras de gobernanza que permitan a las entidades públicas orientar, coordinar, supervisar y controlar lo que ocurre a lo largo del ciclo de vida de los sistemas de IA.

· Promover una cultura propicia a la explotación de la IA en entornos que puedan asumir riesgos controlados.

· Asegurar la sostenibilidad de la estrategia independizándola de los ciclos políticos.

· Poner en marcha estrategias de comunicación internas y externas que promuevan confianza y aceptación.

· Establecer los requisitos que deben cumplir los datos en términos de calidad, completitud, confiabilidad, consistencia y accesibilidad.

· Asegurar la cadena de valor de los datos.

· Abrir los algoritmos al escrutinio público.

· Adoptar enfoques integrales de transformación organizacional apoyándose en las potencialidades que ofrece el uso estratégico de los datos y la IA.

· Ofrecer programas permanentes y personalizados de formación para los servidores públicos.

5. Principales retos y desafíos: propuestas desde el enfoque de derechos humanos

Este capítulo ha intentado aportar luz en torno a los retos éticos, sociales y jurídicos de algunas tecnologías clave en la cuarta revolución industrial, la IA y

las neurotecnologías. Como en cualquier texto, no se han podido agotar todos los matices, aunque sí se pueden recordar aquí algunas de las ideas relevantes:

1. Un reto clave de nuestras sociedades es la *transición digital respetuosa con los derechos humanos*, que ponga a la persona y su dignidad en el centro de cualquier propuesta. Incorporar el *enfoque de derechos humanos* en el diseño, desarrollo e implementación de la IA y de las neurotecnologías puede ayudar a conseguirlo. Para ello, habrá que transversalizar los principios de los derechos humanos en todas y cada una de las iniciativas que se lleven a cabo, en cualquiera de sus fases. De esta forma, no deberían implementarse proyectos tecnológicos o iniciarse políticas públicas que no incorporasen la participación de todos los grupos de interés; no cabrán despliegues tecnológicos que no hayan pensado en cómo incorporar a los más vulnerables (personas con diversidad funcional, mujeres, menores, colectivos LGTBI, migrantes...). Existen algunas instituciones que están trabajando en esta línea, como la Comisión Australiana de Derechos Humanos, muchas organizaciones de la sociedad civil y de la academia, así como algunas empresas[32].

2. Teniendo en cuenta este objetivo, es esencial conseguir *consensos globales en relación a los derechos digitales* y clarificar qué políticas son las adecuadas, integrando todas las visiones de los diversos actores, y no solo y de manera prioritaria a las empresas tecnológicas que invierten en IA y neurotecnologías. En este sentido, la propuesta de un ecosistema de innovación para la salud basado en un enfoque sostenible y responsable es una propuesta reciente (Roveri, 2022) que merece la pena reflexionar, puesto que pone a la persona en el centro de la innovación y considera la importancia de la alianza de actores, según los ODS de la Agenda 2030.

3. Para que la IA y las neurotecnologías avancen con la mirada puesta en los derechos de las personas existen varias iniciativas desde la ética, las regulaciones y las políticas. Sin embargo, son muy diversas, están poco alineadas y escasamente evaluadas. Será necesario acometer un proceso riguroso de *construcción colectiva, libre de la aceleración del cambio tecnológico*, pero de su mano; nunca dando la espalda a la tecnología.

4. En la tarea quedan *muchos retos pendientes*: cómo hacer que los derechos que hemos consensuado *offline* también se apliquen, adaptados (o nuevos), al

[32] Véase: https://www.thoughtworks.com/es-es/perspectives/edition11-ethical-technology.

mundo *online* (sea el entorno que sea: internet, metaversos, etc.); cómo conseguir que las preocupaciones éticas y de derechos humanos no frenen la innovación tecnológica, sino que fomenten una innovación más segura y participativa; cómo conseguir que los robots sean agentes morales; cómo concienciar y educar para una participación responsable en la cuarta revolución industrial. Ojalá la inmensidad de los retos no desanime ni paralice nuestros esfuerzos.

5. No puede dejar de ponerse de manifiesto el potencial de las colaboraciones público-privadas y el rol del sector privado en su contribución a los derechos digitales en América Latina. Debido a la rapidez exponencial del desarrollo de la innovación, de las nuevas tecnologías y su implementación en los distintos mercados, es cada vez más importante contar con el sector privado por su papel en la innovación tecnológica. Su visión prospectiva sobre el impacto de estas nuevas tecnologías debiera tenerse en cuenta en la mejora de la protección y en el diseño de los derechos digitales. Sin duda este reto requiere tomar en cuenta las reflexiones y aprendizajes que, en el trabajo de redes y alianzas de actores (el ODS 17), se han avanzado hasta el momento (Scott, 2022). El sector privado ha innovado y propuesto soluciones tempranas de autorregulación y de adopción de principios éticos antes que cualquier Administración pública[33]. Es necesario tener en cuenta estos procesos y asegurar un buen diálogo entre el sector privado y el sector público, la academia y la sociedad civil, para no dejar a nadie atrás y elaborar unas normativas adecuadas y vinculadas a la realidad de un mundo en constante cambio.

6. Tenemos la convicción de que, así como las intuiciones procedentes de América Latina permitieron en su momento que los derechos económicos y sociales tuviesen su espacio en los textos internacionales de derechos humanos, la unión de fuerzas entre Estados latinoamericanos y europeos hoy puede ofrecer al mundo un modelo de revolución digital basado en los derechos y centrado en las personas, estando la tecnología al servicio de las personas y no al contrario.

[33] En el caso de la ética en la IA, Telefónica fue pionera y adoptó sus principios en 2018. Dos años antes, en 2016, ya había establecido principios de actuación relativos al uso de datos, la privacidad y la seguridad, poniendo al usuario en el centro de estos principios. Sin embargo, muchos expertos coinciden en la necesidad de contar con marcos de gobernanza digital exigibles, y ponen de manifiesto la debilidad de confiar exclusivamente en marcos de autorregulación (Ramos y Mazzucato, 2022). En el mismo sentido: Morley *et al.*, 2020.

Referencias bibliográficas

Aguirre Sala, J. F. (2022): "Especificando la responsabilidad algorítmica", *Teknokultura. Revista de Cultura Digital y Movimientos Sociales*, 19(2), pp. 265-275. https://doi.org/10.5209/tekn.79692.

Allen, C.; Wallach, W. y Smit, I. (2017): *Why Machine Ethics? The Ethics of Information Technologies*, Routledge.

Banks J. (2018): "The Human Touch: Practical and Ethical Implications of Putting AI and Robotics to Work for Patients", *IEEE Pulse* 9(3) (mayo-junio), pp. 15-18. DOI: 10.1109/mpul.2018.2814238.pmid: 29757747.

Barrio, M. (2021): *Formación y evolución de los derechos digitales*, Ediciones Jurídicas Olejnik.

— (2022): *Manual de Derecho Digital,* Valencia, Tirant lo Blanch.

Béliz, G. (2018): *Algoritmolandia*, Buenos Aires, BID/INTEL/Planeta.

Benkler, Y. (2019): "Don't let industry write the rules for AI", *Nature* 569 (7755).

Broussard, M. (2018): *Artificial Unintelligence: How Computers Misunderstand the World*, Cambridge, The MIT Press.

Carloni, E. (2020): "IA, algoritmos y Administración pública en Italia", *IDP. Revista de Internet, Derecho y Política*, nº 30. DOI: https://doi.org/10.7238/ idp.v0i30.3228.

Centro de Documentación e Información (2015): Marco Civil Brasileño de Internet en español.

Consejo de Derechos Humanos de las Naciones Unidas (2018): Promoción, protección y disfrute de los derechos humanos en Internet, A/HRC/38/L.10, Naciones Unidas.

Consejo de Europa (2022): *Human Rights, Democracy, and the Rule of Law Assurance Framework for AI Systems: A proposal prepared for the Council of Europe's Ad hoc Committee on Artificial Intelligence*, The Alan Turing Institute.

Consejo para la Transparencia y Gob_Lab UAI (2021): "Transparencia algorítmica en el sector público". Disponible en: https://www.consejotransparencia.cl/wp-content/uploads/estudios/2021/10/estudio-transparencia-algoritmica-en-el-sector-publico-goblab-cambio-tablas-1.pdf.

Cotino Hueso, L. (2022): "Nuevo paradigma en la garantía de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial", *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi.

Crawford, K. y Calo, R. (2016): "There is a blind spot in AI research", *Nature*, nº 20, 538 (7625) (oct.), pp. 311-313. DOI: 10.1038/538311a.

Custers, B. (2022): "New digital rights: Imagining additional fundamental rights for the digital era", *Computer Law & Security Review*, vol. 44.

De Asís, R. (2022): "Ética, Tecnología y Derechos", en *Inteligencia Artificial y Filosofía del Derecho*, Laborum.

De Asís, R. y Laukyte, M. (2020): "Transhumanismo y envejecimiento", *Soluciones tecnológicas para los problemas ligados al envejecimiento. Cuestiones éticas y jurídicas*, Madrid, Dykinson, pp. 93-114.

European Parliament (2020): The ethics of artificial intelligence: Issues and initiatives.

— (2022): Resolution of 3 May 2022 on artificial intelligence in a digital age (2020/2266(INI). Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0140_EN.html.

European Union Agency for Fundamental Rights (2020): Getting the future right – Artificial intelligence and fundamental rights, Publications Office of the European Union, Luxemburgo.

Fernández-Aller, C. *et al.* (2021): "An Inclusive and Sustainable Artificial Intelligence Strategy for Europe Based on Human Rights", *IEEE Technology and Society Magazine*, vol. 40, nº 1, pp. 46-54. Doi: 10.1109/MTS.2021.3056283.

Fjeld, J.; Achten, N.; Hilligoss, H.; Nagy, A. y Srikumar, M. (2020): "Principled Artificial Intelligence: Mappinig Consensus in Ethical and Rights-Based Approaches to Principles for AI", *SSRN Electronic Journal*. Disponible en: https://doi.org/10.2139/ssrn.3518482.

Gebru, T. (2020): "Race and Gender", en D. Dubber y F. Pasquale (eds.): *The Oxford Handbook of Ethics of AI*, Oxford University Press, pp. 251-269. Doi: 10.1093/oxfordhb/9780190067397.013.16.

Gilligan, C. (1982): *In a Different Voice: Psychological Theory and Women's Development,* Cambridge, Harvard University Pre*ss,* 1982.

Gómez Mont, C.; Del Pozo, C. M.; Martínez Pinto, C. y Del Campo Alcocer, M. (2020): *La Inteligencia Artificial al servicio del bien social en América Latina y el Caribe: panorámica regional e instantáneas de doce países*, BID.

Gutiérrez, E. (2020): "Trazabilidad y explicabilidad de los algoritmos públicos", ICO y Alan Turing Institute.

Ienca, M. (2021): "On neurorights", *Frontiers in Human Neurosciencie*, 15:701258. Doi: 10.3389/fnhum.2021.701258.

Ienca, M. y Andorno, R. (2017): "Towards new human rights in the age of neuroscience and neurotechnology", *Life Sci Soc Policy*, 13, 5. DOI: https://doi.org/10.1186/s40504-017-0050-1.

Jobin, A.; Ienca, M. y Vayena, E. (2019): "The global landscape of AI ethics guidelines", *Nature Machine Intelligence*, vol. 1, September 2, pp. 389-399. DOI: 10.1038/s42256-019-0088-2.

Kissinger, H.; Schmidt, E. y Huttenlocher, D. (2021): *The Age of AI: And Our Human Future*, Nueva York, Little, Brown and Company.

Köbis, N.; Bonnefon, J. F. y Rahwan, I. (2021): "Bad machines corrupt good morals", *Nature Human Behaviour* 5(6) (jun.), pp. 679-685. DOI: 10.1038/s41562-021-01128-2.

Lassalle, J. M. (2019): *Ciberleviatán*, Barcelona, Arpa.

Laukyte, M. (2021): " Dignidad humana y nuevos derechos: el derecho a la inteligencia artificial", *Inteligencia Artificial y Derecho. El jurista ante los retos de la era digital*, Aranzadi.

Morley *et al*. (2020): "From What to How: An Initial Review of Publicly Available AI Ethics Tools, Methods and Research to Translate Principles Into Practices", *Science and Engineering Ethics*.

Morley, J., Kinsey, L., Elhalal, A. *et al.* (2023): "Operationalising AI ethics: barriers, enablers and next steps", *AI & Soc* 38, pp. 411–423. DOI: https://doi.org/10.1007/s00146-021-01308-8.

Oliver, N. (2020): *Inteligencia artificial, naturalmente*, Ministerio de Asuntos Económicos y Transformación Digital, Secretaría General Técnica, Centro de Publicaciones, Madrid.

Ortega Klein, A. (2021): "El impacto del COVID-19: la digitalización como bien común", *Documento de trabajo*, 1/2021, Real Instituto Elcano.

Ortiz de Zárate-Alcarazo, L. y Guevara-Gómez, A. (2021): *Inteligencia artificial e igualdad de género. Un análisis comparado entre la UE, Suecia y España*, Madrid, Fundación Alternativas.

Penenberg, A. (2011): "NeuroFocus uses neuromarketing to hack your brain. Fast Company". Disponible en: https://www.fastcompany.com/1769238/neurofocus-uses-neuromarketing-hack-your-brain.

Piñar Mañas, J. L. (2020): "Derecho e innovación. Privacidad y otros derechos en la sociedad digital", *El Derecho a la protección de datos personales en la sociedad digital*, Centro de Estudios Ramón Areces.

Presidencia del Consejo de Ministros y la Secretaría de Gobierno y Transformación Digital (2022): Carta Peruana de Derechos Digitales.

Price Waterhouse Cooper (2018): "Sizing the prize. What's the real value of AI for your business and how can you capitalise?".

Rallo, A. (2017): "De la 'Libertad Informática' a la constitucionalización de nuevos derechos digitales (1978-2018)", *Revista de Derecho Político de la UNED*, nº 100, Madrid.

Ramos, G. y Mazzucato, M. (2022): "La IA al servicio del bien común", *Project Syndicate*, 26 de diciembre. Disponible en: https://www.project-syndicate.org/commentary/ethical-ai-requires-state-regulatory-frameworks-capacity-building-by-gabriela-ramos-and-mariana-mazzucato-2022-12/spanish

Roveri, C. (2022): "Inteligencia Artificial para el bienestar y una vida sana en Latinoamérica: Hacia un ecosistema de innovación responsable para la salud digital", *Análisis Carolina*, nº 21, Madrid, Fundación Carolina.

Sachs, J.D., Schmidt-Traub, G., Mazzucato, M., Messner, D., Nakicenovic, N. y Rockström, J., (2019): "Six transformations to achieve the sustainable development goals", *Nature sustainability* 2, pp. 805–814.

Salgado Criado, J. y Fernández-Aller, C. (2021): "A Wide Human-Rights Approach to Artificial Intelligence Regulation in Europe", *IEEE Technology and Society Magazine*, vol. 40, nº. 2, pp. 55-65. Doi: 10.1109/MTS.2021.3056284.

Salgado Criado, J.; Fernández-Aller, C.; Monge, C. y Mataix, C. (2021): *La digitalización sostenible*, Tiempo de Paz, MPDL.

Schiff, D. (2022): "Education for AI, not AI for Education: The Role of Education and Ethics in National AI Policy Strategies", *Int. J. Artif. Intell. Educ.*, 32, pp. 527-563. DOI: https://doi.org/10.1007/s40593-021-00270-2.

Scott, L. (2022): *Partnership and transformation. The promise of multi-stakeholder collaboration in context*, Routledge. DOI: https://doi.org/10.4324/9781003199434.

Stahl, B. C.; Schroeder, D. y Rodrigues, R. (2023): "The Ethics of Artificial Intelligence: An Introduction", *Ethics of Artificial Intelligence*, SpringerBriefs in Research and Innovation Governance, Springer, Cham. Disponible en: https://doi.org/10.1007/978-3-031-17040-9_1.

Stanford University (2022): Artificial Intelligence Index Report. Disponible en: https://aiindex.stanford.edu/report/.

Tegmark, M. (2017): *Life 3.0. Being human in the age of Artificial Intelligence,* Vintage.

The Alan Turing Institute (2022): Human Rights, Democracy, and the Rule of Law Assurance Framework for AI Systems: A proposal prepared for the Council of Europe's Ad hoc Committee on Artificial Intelligence.

Thoughtworks (2021): "Social Impact Report. Tech at the core of society". Disponible en: https://www.thoughtworks.com/about-us/social-change/reports/tech-at-the-core-of-society.

Turing, A. M. (1950): "Computing Machinery and Intelligence", *Mind*, nº 49, pp. 433-460.

Véliz, C. (2021): *Privacidad es poder. Datos, vigilancia y libertad en la era digital*, Debate.

Villas, M. y Camacho, J. (2022): *Manual de ética aplicada en Inteligencia Artificial*, Anaya Multimedia.

Vinuesa, R.; Azizpour, H.; Leite, I. *et al.* (2020): "The role of artificial intelligence in achieving the Sustainable Development Goals", *Nat Commun*, 11, 233. DOI: https://doi.org/10.1038/s41467-019-14108-y.

World Inequality Lab (2022): World Inequality Report 2022. Disponible en: https://wir2022.wid.world/www-site/uploads/2021/12/WorldInequalityReport2022_Full_Report.pdf.

Yuste, R.; Genser, J., y Herrmann, S. (2021): "It's Time for Neuro-Rights", *Horizons*, Center for International Relations and Sustainable Development.

3. La defensa de la libertad de expresión, la ciberseguridad, y el derecho a una información veraz frente a las *fake news* y la neutralidad de internet

J. Carlos Lara Gálvez[*]

1. Introducción

La expansión de las posibilidades de expresión y comunicación es probablemente una de las más evidentes consecuencias del explosivo crecimiento en el acceso a internet en el mundo entero. Ciertamente, no se trata de una expansión unívoca o unidireccional, y menos de una que no esté fuertemente marcada por las condiciones materiales de cada persona, grupo o territorio[1]. El porqué de su crecimiento puede estar dado por su carácter abierto, como tecnología (o conjunto de tecnologías) de carácter generativo y flexible para multiplicidad de aplicaciones y modelos de negocio, fortalecida por continuos avances tecnológicos (Zittrain, 2008), o bien debido a que esa flexibilidad y avance crearon y transformaron modelos de negocio, influenciando la inversión en su crecimiento. Los efectos, no obstante, son globales: la mayor parte de la humanidad se ha visto afectada, de formas notorias y ocultas, por el crecimiento de internet.

Esas posibilidades están estrechamente vinculadas a intereses humanos defendidos como derechos fundamentales. En mayo de 2011, el entonces Rela-

[*] Miembro de la organización Derechos Digitales de Chile desde 2008, actualmente es su codirector ejecutivo. Anteriormente se desempeñó como director del área de investigación y políticas públicas, liderando trabajos en temas vinculados a la propiedad intelectual, la libertad de expresión, el acceso al conocimiento y la labor académica en el entorno digital. Es abogado de la Universidad de Chile y magíster en Derecho y Tecnología por la Universidad de California, Berkeley.

[1] Condiciones que, tratándose de las tecnologías de la información y la comunicación, no se extienden tan solo a la disponibilidad de bienes materiales, sino también de otras condiciones.

tor Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión, en su informe anual, consolidó buena parte de la discusión sobre internet y libertad de expresión. Reconocía allí el carácter singular de internet como potenciador de derechos, en comparación con las demás tecnologías existentes para la comunicación y la expresión.

> A diferencia de los demás medios, Internet permite a las personas buscar, recibir y difundir información e ideas de todo tipo al instante y a bajo costo a través de las fronteras nacionales. Al ampliar enormemente la capacidad personal de disfrutar el derecho a la libertad de opinión y de expresión, que es un factor coadyuvante de otros derechos humanos, Internet potencia el desarrollo económico, social y político y contribuye al progreso de la sociedad en su conjunto (ONU, 2011).

El informe del Relator Especial hacía énfasis en la necesidad de asegurar acceso universal a internet por parte de los Estados[2]. A pesar del entusiasmo inicial de la prensa de la época por lo que se había entendido como una consagración del acceso a internet como derecho humano[3], el informe era más cuidadoso: reconocía a internet como medio facilitador no solamente para el ejercicio de la libertad de expresión, sino para el rango completo de derechos humanos, tanto civiles y políticos como económicos, sociales y culturales. En otras palabras, si ya existía consenso sobre el vínculo entre la libertad de expresión y el resto de los derechos humanos, la facilitación por parte de internet de la libertad de expresión ubicaba la conectividad como un factor clave para el ejercicio de todos los demás derechos humanos.

Centrándonos en lo más directamente vinculado a la expresión en línea, es inevitable tratar la expansión de internet como un factor que incide directamente en aquellos ámbitos que se refieren a la vida en sociedad (ONU, 2011). A la preclara noción de internet como instrumento para la universalización del ejercicio de la expresión con alcance global, se suma el mayor acceso a la emisión y recepción de expresiones legalmente ilícitas o socialmente dañinas. A la facilidad para la publicación sin límites y aceleradas de expresiones políticas o culturales se suma la facilidad para compartir material delictivo de forma anónima o sin capacidad suficiente de persecución de consecuencias. La escala a

[2] *Ídem*, p. 85.

[3] Como ejemplo, CNN entregaba la noticia global del nuevo derecho humano reconocido por la ONU (CNN, 2011).

que han crecido ciertas plataformas hace crecer el desafío de lidiar con tales contenidos (Kaye, 2019), solamente aumentando en el tiempo: cada minuto se ven más de tres millones de vídeos en YouTube, se comparten 66.000 fotos o vídeos en Instagram o se envían 575.000 trinos en Twitter (Localiq, 2022).

Aunque la experiencia en América Latina no es ajena a los vaivenes globales, el contexto latinoamericano está caracterizado por múltiples manifestaciones diversas, tanto materiales como jurídicas, que representan distintos niveles tanto de oportunidades como de riesgos para el ejercicio de las libertades de pensamiento y de expresión, así como para otros derechos fundamentales (Carbonell Sánchez, 2011). En parte, ese cúmulo de diversas historias viene marcado por caracteres comunes, como la histórica explotación de los recursos naturales y del trabajo humano por grandes fortunas privadas, y como las distintas historias nacionales con periodos de violencia política, gobiernos autoritarios y dictatoriales, y presión económica exterior (Sixirei, 2014).

En esos contextos —ya apremiantes para la defensa y el ejercicio de las libertades fundamentales—, las mismas características que han marcado la delimitación y el ejercicio de la libertad de expresión en América Latina se han visto replicadas y a menudo exacerbadas por la extendida presencia de las tecnologías de la información y la comunicación, incluida internet. No obstante, dada la diferente posición geopolítica y económica de los Estados latinoamericanos, la reacción normativa a los desafíos del entorno digital varía entre países. Como veremos en los próximos apartados, tanto la forma de comprender los desafíos para los derechos fundamentales del entorno digital como las reacciones institucionales se encuentran en un periodo extendido de experimentación en busca de soluciones, más en respuesta a ansiedades contingentes que a la fijación de estándares de convivencia de largo aliento. Si bien los estándares compartidos de derechos humanos son parte integrante de los bloques constitucionales de los países, las regulaciones sobre la libertad de expresión en general, y sobre su ejercicio o afectación en internet en particular, están —en general— todavía lejos de un desarrollo o un refinamiento que permitan calificarlas como ejemplares para otros países dentro o fuera de la región.

Dentro de ese escenario, y regresando al estrecho entrelazamiento entre internet, la libertad de pensamiento y expresión, la democracia, y el resto de los derechos fundamentales, mantendremos dos ideas como hilos conductores. La primera, que en la medida en que existen ataques de distinto tipo sobre internet (su uso, sus usuarias, sus redes, sus servicios, sus dispositivos), esos mismos pueden ser interpretados como ataques a la libertad de expresión. La

segunda, que la complejidad de tales ataques es mayúscula, extendiéndose a un rango que va desde las vías para la censura directa o indirecta, previa o posterior, hasta mecanismos privados y públicos que sin remover expresiones del ámbito público sí desincentivan o hacen indeseable la intervención en el espacio público, restando valor a la libertad de expresión como presupuesto para el ejercicio del conjunto de derechos humanos y la participación en una sociedad democrática. No es posible hacer en estas páginas un ejercicio exhaustivo de todas estas amenazas y afectaciones; no obstante, la experiencia latinoamericana es, al menos, rica en ejemplos que plantean los desafíos del impacto sobre los derechos humanos que conllevan acciones públicas y privadas sobre internet.

2. Conceptos: contenido esencial y naturaleza jurídica del derecho

2.1. La libertad de pensamiento y expresión

El derecho a la libertad de expresión es una parte fundamental del desarrollo de los derechos humanos. En términos extremadamente generales, se entiende como el derecho de todas las personas a buscar, recibir y difundir información y opiniones libremente, sin mediar censura. Para varios de los órganos del sistema internacional de los derechos humanos, como también dentro del sistema interamericano de derechos humanos, la libertad de expresión constituye la piedra angular de una sociedad democrática, y su aseguramiento es una condición esencial para que dicho tipo de sociedad esté suficientemente informada[4].

En un sentido positivo, la libertad de expresión está presente en numerosos instrumentos fundacionales del sistema de derechos humanos, como el Artículo 19 de la Declaración Universal de los Derechos Humanos (DUDH) y Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP), mientras que en el contexto americano es parte del Artículo IV de la Declaración Americana de los Derechos y Deberes del Hombre (DADDH) y está fuertemente consagrada en el Artículo 13 de la Convención Americana sobre Derechos Humanos (CADH).

Como se ha adelantado, la libertad de expresión ha sido reconocida a su vez como coadyuvante de otros derechos fundamentales. Se encuentra en la

[4] Corte Interamericana de Derechos Humanos, Caso La Última Tentación de Cristo (Olmedo Bustos y otros) vs. Chile, Sentencia de 5 de febrero de 2001 (Fondo, Reparaciones y Costas), párrafo 68.

base del derecho a la libertad de pensamiento y de opinión (DUDH, Artículo 18), de la libertad de asociación (DUDH, Artículo 20) y del derecho a la participación en el gobierno (DUDH, Artículo 21). También es un derecho crucial en relación con el ejercicio de los derechos económicos, sociales y culturales, tales como el derecho a la educación y el derecho a participar en la vida cultural y gozar de los beneficios del progreso científico y de sus aplicaciones (DUDH, Artículo 15; PIDESC, Artículo 15).

De este modo, si asumimos las tecnologías de la información y la comunicación como herramientas útiles para la libertad de expresión, estas tendrían un impacto positivo en todos los demás derechos. Es decir, en la medida en que internet facilita el ejercicio de la libertad de expresión, facilita a la vez a los derechos favorecidos por la libertad de expresión (ONU, 2011), creando así un potencial círculo virtuoso de ejercicio de derechos fundamentales.

Por otra parte, tanto por el ejercicio del derecho mismo como por su conexión con otros derechos —como el de reunión pacífica o los derechos económicos, sociales y culturales—, el derecho a la libertad de pensamiento y expresión tiene una dimensión que no es exclusivamente individual, sino también colectiva y social. Existen aspectos de estos derechos desarrollados en la doctrina y la jurisprudencia, como el derecho colectivo a recibir cualquier información y a conocer la expresión del pensamiento ajeno, que dan cuenta del carácter colectivo de los derechos bajo estudio (Fuentes Torrijo, 2002; OEA, 2009).

Se entiende en general que la libertad de pensamiento y expresión conlleva la obligación estatal negativa de respetar, esto es, que las autoridades no lleven a cabo acciones que lesionen derechos humanos, tales como prohibir ciertos tipos y formas de discurso (sin perjuicio de las restricciones permisibles). A la vez, existen obligaciones positivas para el Estado, como la de proteger, que incluye asegurar que las personas no vean violados sus derechos ni por las autoridades ni por sujetos particulares, y la de garantizar que obliga a la adopción de todas las medidas necesarias para crear las condiciones que permitan gozar efectivamente de los derechos, incluida la de asegurar mecanismos de remedio en casos de afectación del derecho por el Estado o por otros particulares.

Respecto de la aplicación a internet del derecho, sin perjuicio de la vasta literatura doctrinaria y jurisprudencial reforzando el mismo punto, el informe anual del Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión de 2011 recuerda que

> el artículo 19 de la Declaración Universal de Derechos Humanos y el Pacto se redactó con espíritu previsor para dar cabida a futuros adelantos técnicos gracias a los cuales las personas pudieran ejercer su derecho a la libertad de expresión. A ello se debe que el marco del derecho internacional de los derechos humanos siga siendo hoy pertinente y aplicable igualmente a las nuevas tecnologías de la comunicación como Internet (ONU, 2011).

A la vez, la Declaración conjunta sobre libertad de expresión e internet de distintas relatorías especiales regionales y globales destacaba el

> carácter transformador de Internet, como medio que permite que miles de millones de personas en todo el mundo expresen sus opiniones, a la vez que incrementa significativamente su capacidad de acceder a información y fomenta el pluralismo y la divulgación de información (ONU *et al*., 2011).

Finalmente, el informe "Libertad de Expresión en Internet" (OEA, 2013) describía principios orientadores para la libertad de expresión en internet, en consideración a las posibilidades regulatorias. Esto engloba: 1) el principio de acceso universal, que incluye la obligación positiva de los Estados de tomar medidas para superar las brechas tecnológicas, la obligación de asegurar infraestructura y servicios que permitan el acceso universal, y la obligación de abstenerse de bloquear o limitar el acceso a internet; 2) el principio de no discriminación, en virtud del cual ni las leyes ni las condiciones sociales, económicas o culturales deben establecer barreras que limiten el uso de internet, por razones ideológicas, de género, raza, idioma, ubicación geográfica u otras, además de la necesidad de la adopción de medidas positivas para asegurar la igualdad; 3) el principio de pluralismo, que implica el deber de promoción de pluralidad y diversidad en el debate público, y asegurar que cualquier medida que pueda afectar a internet esté destinada a que más y no menos personas, ideas, opiniones e información sean parte de la discusión pública, y 4) el principio de privacidad, que como garante de la libertad de expresión requiere garantías para la protección de información personal contra intromisiones arbitrarias, como también el derecho a la expresión sin obligación de identificación, salvo que participen en actos que vulneren derechos de terceros.

Lo anterior es reflejo de la necesidad de considerar de forma especial a internet en lugar de extender sin más las condiciones regulatorias propias de otros

medios o tecnologías. Pero esta visión potenciada de derechos contrasta con los efectos negativos de actos de expresión, que en ocasiones implica la habilitación de restricciones bajo ciertos requisitos. Antes de referirnos a ellos, debemos tener cuenta que los actos de expresión pueden impactar negativamente a derechos como la privacidad, la honra, la seguridad nacional, la propiedad intelectual, la fe pública y más; también que esos efectos pueden producirse con intención o no, o aun en aparente ejercicio de libertades informativas. Por estas razones, tanto la reglamentación como las posibles restricciones a la libertad de expresión, dentro del sistema interamericano, deben cumplir simultáneamente con tres características (el "test tripartito") desarrolladas a lo largo de la jurisprudencia (OEA, 2008), a saber: 1) la limitación debe haber sido definida en forma precisa y clara a través de una ley formal y material; 2) la limitación debe estar orientada al logro de objetivos imperiosos autorizados por la Convención Americana, y 3) la limitación debe ser necesaria en una sociedad democrática para el logro de los fines imperiosos que se buscan, idónea para lograr el objetivo imperioso que pretende lograr y estrictamente proporcional a la finalidad perseguida.

Si las formas de restringir legítimamente la expresión están sujetas a estas exigencias, pero a la vez las maneras —directas o indirectas— de restringir la expresión varían tan significativamente en relación con el uso de internet, ¿cuál es la manera sensible de regular internet sin infringir estas exigencias? Como veremos, las formas en que la libertad de expresión en línea puede verse afectada, directa o indirectamente, dan lugar a serios cuestionamientos sobre la legitimidad de esas acciones frente al derecho internacional de los derechos humanos y el sistema interamericano de derechos humanos.

3. Concreción de las experiencias

Hemos reiterado que existen múltiples formas de afectar directa o indirectamente a la expresión en línea. En las próximas subsecciones, agruparemos esas posibles experiencias de afectación en torno al acceso mismo a internet, a las variadas formas de regulación de discurso con el efecto probable de afectación desmedida de la libre expresión, y a las formas indirectas de limitar el discurso en línea, como ocurre con la regulación de las plataformas y los ataques dirigidos contra las personas que ejercen la libre expresión en línea.

3.1. Acceso a internet como factor garante de la libertad de expresión en línea

El ya citado informe del Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión en 2011 enfatizaba que "los Estados tienen la obligación positiva de promover o facilitar el disfrute del derecho a la libertad de expresión y los medios necesarios para ejercer este derecho, lo que incluye a internet" (ONU, 2011). La referencia expresa a la conectividad a la red fue también parte de la Declaración conjunta de los relatores (ONU *et al.*, 2011), según la cual "[l]os Estados tienen la obligación de promover el acceso universal a internet para garantizar el disfrute efectivo del derecho a la libertad de expresión".

Ciertamente esas aspiraciones contrastan con la realidad: las brechas digitales de América Latina están entre las más altas del mundo, limitando la capacidad de muchas personas de aprovechar el acceso a internet para la libertad de expresión.

Si en general el acceso a internet es o debe ser un derecho humano ha sido ya objeto de largo estudio en la literatura (Lara, 2015). No obstante, tanto las recomendaciones de los órganos internacionales como las progresivas iniciativas normativas y de política pública parecen apuntar en la dirección de la conectividad universal, en especial después de la pandemia de la COVID-19 declarada en 2020. Así, convertir el potencial de internet en el fundamento para defender una obligación de los Estados ha sido parte de la agenda entre órganos y especialistas de derechos humanos durante la última década, en documentos y declaraciones que se omiten en estas páginas.

No obstante, cabe destacar dos aristas significativas para el objeto de este texto. La primera, en relación con las características del acceso a internet —cuya garantía estatal se espera— para favorecer tanto la libertad de expresión como el rango completo de derechos humanos. La segunda, respecto del efecto que la denegatoria de la provisión de internet, o su interrupción, supone para los mismos derechos.

Respecto del aspecto garante de la libertad de expresión, cabe destacar al menos un par de documentos con cierto grado de autoridad. Uno es el informe sobre libertad de expresión e internet del sistema interamericano (OEA, 2013), que aboga por un acceso universal en condiciones de igualdad, asequibilidad, no discriminación, en distintos idiomas y lenguas, y mediado por medidas positivas adoptadas por los Estados para favorecer ese acceso, incluyendo la educación. Todo ello desarrollado a partir de recomendaciones de ámbito global e

interamericano, y tanto en relación con el derecho a la libertad de expresión, en general —y con distintas tecnologías comunicativas— como respecto de declaraciones sobre internet en particular. El otro documento, con un sentido más operativo, lo representa el marco ROAM-X de la UNESCO, con indicadores sobre la universalidad de internet (UNESCO, 2019), basados en los principios de derechos humanos, apertura, accesibilidad y participación de múltiples partes interesadas, para identificar puntos donde se hace necesario adoptar medidas para favorecer la universalidad de internet entre distintas partes interesadas. De lo anterior podemos dar cuenta de la suficiente existencia de guías sobre el modo en que el acceso a internet es deseable, superando la noción de la conectividad física o tecnológica como única arista prioritaria para facilitar el ejercicio de la expresión en línea.

A lo anterior hay que sumar la recomendación sobre el respeto al principio de neutralidad de la red: no debería haber discriminación, bloqueo, filtración ni interferencia del tráfico en internet en función de factores que no estén vinculados con la ingeniería de la red. Además, la neutralidad debería aplicarse a los modos de acceder a internet, sin restricciones con respecto a dispositivos compatibles. Así lo estima también el informe interamericano (OEA, 2013), sin perjuicio de los desafíos que eso presenta no solo ante la filtración y bloqueo de contenidos, sino de la promoción de ciertos servicios en perjuicio de otros a través de los sistemas de *zero-rating* (Pereira da Silva *et al*., 2017).

La segunda arista relevante es la referida a los actos contrarios a la conectividad, a saber, los bloqueos o apagones de internet, conocidos en inglés como *shutdowns*. Se conoce de esta forma —en un sentido más comprehensivo que las interrupciones de servicios de internet— a las interferencias en sistemas electrónicos usados primordialmente para comunicaciones entre personas, con la intención de hacerlos inaccesibles o inutilizables, para ejercer control sobre el flujo de información (Björksten, 2022). Bajo este concepto, detener el flujo de internet, y también reducirlo o imponer medidas técnicas que limiten su funcionamiento, es objeto de cuestionamiento, teniendo en cuenta que de por sí una definición estricta no implica los mismos efectos deletéreos sobre la expresión en línea.

Aunque en un sentido estrictamente jurídico no es pacífico que los apagones de internet sean *per se* ilícitos (De Gregorio y Stremlau, 2020), desde la perspectiva de los órganos expertos en derechos humanos (ONU *et al*., 2011), la interrupción no puede estar justificada en ningún caso, ni siquiera por razones de orden público o seguridad nacional, y lo mismo se aplica a las medidas de

reducción de la velocidad de navegación de internet o de partes de este. Es decir, ni los bloqueos totales o parciales, ni las restricciones a parte de la red, ni las medidas para reducir la funcionalidad de la red son admisibles desde la protección de la libertad de expresión.

Las declaraciones y expectativas contrastan con la práctica de bloqueos en la región. A partir de reportes recogidos tanto del monitoreo de la sociedad civil como de las empresas de internet, bases de datos como Pulse, de Internet Society (ISOC, 2022), mantienen registros sobre las disrupciones confirmadas en el mundo entero, incluida América Latina. Si bien en la región latinoamericana las instancias de bloqueo o filtrado de la red son menos prevalentes que en África o Asia, igualmente aparecen como ejemplos los siguientes:

· En Cuba, a mediados de 2021, en medio de protestas por las medidas para controlar la COVID-19, se cortó el acceso a internet (Gilbert, 2021). Cuando regresó, dos días después, algunos servicios de comunicación entre personas seguían bloqueados (AFP, 2021). La isla ya había reportado limitaciones o bloqueos para ciertos servicios de mensajería en 2020 (14 y Medio, 2020).

· También en Cuba, en 2022, después del paso del huracán Ian, se vivió un corte generalizado de internet móvil, al mismo tiempo que falló el sistema eléctrico en la isla (BBC, 2022).

· En Venezuela es quizás donde se han producido más casos. Coincidiendo con distintos eventos políticos de interés público, internet ha fallado total o parcialmente, sobre todo entre 2017 y 2019 (Alcalde y Solano, 2020). No obstante, cabe destacar que la infraestructura misma de internet en Venezuela ha caído en falta de mantención, lo que afecta al derecho mismo a la conectividad, independientemente de la existencia o no de apagones (Urribarrí y Díaz, 2018).

· Ha habido reportes de pérdida de conectividad en contextos de protestas. En Nicaragua en 2018, se reportaron fallas por un día que coincidían con una fuerte represión estatal (Access Now, 2019). En Ecuador, en 2019, hubo reportes de fallas en la conectividad y en el acceso a redes sociales durante un contexto de protestas sociales tras anuncios públicos de medidas de austeridad (Díaz, 2019; Global Voices, 2019). En Colombia, en 2021, hubo fallas que, si bien se dijo que no eran deliberadas, coincidieron con situaciones de protesta social en el país (Guerra, 2021).

Lo anterior no obsta a los casos en que, en razón de resoluciones administrativas o judiciales, sitios web o aplicaciones específicas han sido objeto de bloqueo en distintos niveles de funcionamiento de internet. Como veremos a continuación, a partir del contenido que difunden ciertos servicios en línea también hay restricciones más dirigidas, pero que a su vez afectan a las libertades de expresión e información en línea.

3.2. Filtrado, bloqueo y restricciones sobre contenido en línea

Un caso más acotado de limitación de la libertad de expresión a través de controles específicos sobre internet es el de las medidas de filtrado o bloqueo, dirigidas contra sitios web o sus identificadores, o aplicaciones móviles o sus protocolos[5]. Teniendo en cuenta que se trata de medidas de alcance más reducido que los apagones de internet, no reciben el mismo rechazo desde el sistema de derechos humanos. Así, por ejemplo, en los estándares interamericanos, la licitud proviene del cumplimiento de los requisitos de legalidad, necesidad, proporcionalidad y propósito legítimo descritos más arriba. Más específicamente,

> el bloqueo o suspensión obligatoria de sitios web enteros o generalizados, plataformas, conductos, direcciones IP, extensiones de nombre de dominios, puertos, protocolos de red o cualquier tipo de aplicación, así como medidas encaminadas a eliminar enlaces (links), datos y sitios web del servidor en el que están alojados, constituyen una restricción que solo será excepcionalmente admisible en los estrictos términos establecidos en el artículo 13 de la Convención Americana.

De acuerdo con la Declaración conjunta (ONU *et al*., 2011), el bloqueo obligatorio constituye una medida extrema, solo justificable bajo estándares internacionales, como en el caso del material de abuso sexual de niños, niñas y adolescentes. Según la misma declaración, el filtrado de contenidos que no sea controlado por el usuario final constituye una forma de censura previa y, por tanto, una infracción a la libertad de expresión. Finalmente, si se ofrecen productos destinados a facilitar el filtrado por los usuarios finales (por ejemplo, controles parentales para limitar el acceso a ciertos sitios o servicios por personas menores de edad), tales productos deben tener información clara acerca del modo en que funcionan y sus posibles desventajas (ONU *et al*., 2011).

[5] Para una explicación técnica sobre las formas de bloqueo, véase ISOC, 2017.

Sin perjuicio de las aristas jurídicas, la imposición de medidas de bloqueo presenta desafíos técnicos que las convierten en herramientas indeseables, pues como indica internet Society, el bloqueo como medida "suele ser ineficiente, a menudo no es eficaz y, en general, perjudica involuntariamente a los usuarios de Internet" (ISOC, 2017). El riesgo de bloquear o filtrar en demasía o en insuficiencia es un riesgo que constituye una amenaza a la libertad de expresión, que por tanto debe adoptarse con altos niveles de transparencia (art. 19, 2016).

En la subsección siguiente daremos cuenta de situaciones de bloqueo en razón de la ilicitud de contenidos, determinada legal o judicialmente. Pero cabe en este apartado listar situaciones de bloqueo y filtrado que han sido particularmente llamativas desde la perspectiva de derechos humanos en la región.

· En Brasil, durante más de 15 años, diversas órdenes judiciales han dispuesto el bloqueo de sitios y aplicaciones completas, por no eliminar contenido ilegal o por no hacer entrega de información requerida en procesos judiciales (De Souza Abreu, 2018). Los más llamativos son cuatro casos de bloqueo de WhatsApp entre 2015 y 2016 por no cumplir con órdenes de entregar información en investigaciones penales, casos que han llegado hasta el Supremo Tribunal Federal (Lara, 2020). Más recientemente se suma el breve bloqueo de Telegram, por no adoptar ciertas medidas contra la desinformación (*El Mundo*, 2022).

· En Perú, al menos 30 sitios fueron bloqueados en el país entre 2018 y 2019, sin orden judicial, pero autorizadas administrativamente, tanto para bloquear páginas por infracción de derechos de autor como para bloquear servicios de transporte (Villena, 2020).

· En Colombia, sitios de apuestas se reportaban bloqueados (Ververis, Khrustaleva y Quiroz, 2017), con escasa o nula información relevante sobre el bloqueo.

Como expresan Ferraz *et al.* (2012), los mecanismos de filtrado, por la afectación a la vez jurídica y técnica en el uso de la red, representan un riesgo no solamente para la libertad de expresión, sino para la innovación y la creación de nuevos modelos de negocios en la red. Veremos a continuación fundamentaciones jurídicas para órdenes de esa clase.

3.3. Contenidos ilícitos y dañinos

La regulación de la expresión, en general, contempla situaciones en que ciertos actos comunicativos, en forma de imágenes, palabras habladas o escritas, materiales audiovisuales u otros, sean objeto de sanción o de responsabilidades en la legislación, por ser contrarias a derechos fundamentales o intereses sociales relevantes. En el contexto de internet es habitual que la discusión sobre la regulación y la restricción de tales expresiones se haga dentro de la idea de "contenidos ilícitos".

Siguiendo con la línea del apartado anterior, ciertas medidas técnicas restrictivas de la expresión en línea podrían ser consistentes con la protección de la libertad de expresión, siempre que cumplan con las condiciones sustantivas de las restricciones legítimas, extendidas al entorno digital. En palabras de la Relatoría Especial para la Libertad de Expresión del sistema interamericano:

> En casos excepcionales, cuando se está frente a contenidos abiertamente ilícitos o a discursos no resguardados por el derecho a la libertad de expresión, resulta admisible la adopción de medidas obligatorias de bloqueo y filtrado de contenidos específicos. En estos casos, la medida debe someterse a un estricto juicio de proporcionalidad y estar cuidadosamente diseñada y claramente limitada de forma tal que no alcance a discursos legítimos que merecen protección. En otras palabras, las medidas de filtrado o bloqueo deben diseñarse y aplicarse de modo tal que impacten, exclusivamente, el contenido reputado ilegítimo, sin afectar otros contenidos (OEA, 2017a).

Para Bertoni (2017) existe una tensión entre la admisión de sistemas de filtrado en casos excepcionales y la prohibición de censura previa, y es evidente el contraste entre la declaración de la Relatoría del sistema interamericano, aparentemente más vinculada al sistema internacional de derechos humanos que al texto de la CADH. Por lo mismo, la adecuación a la CADH de cualquiera de esos sistemas es todavía una cuestión abierta.

Tal como ocurre en el mundo analógico, la regulación de los casos en que ciertas expresiones pueden ser legítimamente restringidas o sujetas a responsabilidades ulteriores es una materia compleja. Por una parte, debe establecerse bajo los parámetros del sistema de derechos humanos qué conductas o expresiones pueden ser objeto de esa responsabilidad; si bien hay casos donde se verifica un "acuerdo social tácito" —como en el del rechazo al abuso sexual infantil (Botero,

2021) y el contenido que lo representa— la delimitación de qué constituye el material prohibido puede ser problemática. Lo mismo ocurre con otras materias como el así llamado "discurso de odio", con los materiales infractores de propiedad intelectual cuando su existencia debe contrastarse con los permisos legales válidos, con discursos constitutivos de injuria, calumnia o difamación (u otros atentados contra la honra) y, finalmente, con la multiplicidad de expresiones asociadas a la idea de desinformación. Tanto la exposición a sanciones ulteriores como la posibilidad de forzar al bloqueo o retiro de tales contenidos son materias ampliamente disputadas en el contexto latinoamericano.

3.3.1. El contenido de abuso sexual infantil

En el sistema interamericano de derechos humanos se reconoce que hay tres excepciones a la protección por defecto de las expresiones humanas dentro del derecho a la libertad de expresión: la propaganda de la guerra y la apología del odio que constituya incitación a la violencia, la incitación directa y pública al genocidio, y la mal llamada "pornografía infantil" (OEA, 2009). A esto último nos referimos ahora.

Generalizando, la penalización del material de abuso sexual infantil se refiere, como mínimo, a la representación visual de una persona menor de edad que mantiene una conducta sexualmente explícita, una persona real que parezca ser menor de edad que participa en actos sexualmente explícitos o imágenes realistas de una persona menor de edad no existente que mantiene una conducta sexualmente explícita. La penalización incluye usualmente sanciones por captar, preparar, entregar o controlar a un menor con el fin de crear este material o con fines de posesión, divulgación, transmisión, exhibición o venta del mismo material.

La prohibición de esa clase de contenido es objeto de consenso internacional, por tratarse de una forma de explotación y abuso sexual, y por ser contenido que lesiona el interés superior y a los derechos de niñas, niños y adolescentes. En el contexto de las comunicaciones digitales, donde la celeridad y el potencial alcance de las comunicaciones conllevan un riesgo mayor para la indemnidad sexual de las personas menores de edad, la restricción de ese material es usualmente admitida aun sin obligaciones legales específicas dirigidas hacia las empresas de internet. Es más, se trata del caso por antonomasia de restricción admitida de contenidos en internet, aun sin mediar intervención o control judicial previo, mediante bloqueos o filtros, sea mediante control humano o automatizado.

Sobre este punto, varias legislaciones latinoamericanas mencionan la exigencia para empresas proveedoras de internet de poner a disposición de sus clientes sistemas de filtrado de contenido (Ferraz *et al*., 2012). A la vez, existen sistemas que han permitido automatizar el filtrado de esta clase de material: es el caso de la identificación automatizada de imágenes de abuso infantil con códigos alfanuméricos o *hashes*, para luego compartir bases de datos de los mismos *hashes* entre empresas y con fundaciones de protección de la niñez (Douek, 2020). El éxito del esquema respecto de esta clase de contenidos arriesga su expansión a otros ámbitos distintos del abuso sexual infantil, llevando a mayor restricción de contenidos o de "censura" (Citron, 2018), en una coordinación contraria a la libertad de expresión (Llansó, 2019) o, más ampliamente, a un mayor control entre algunas empresas de lo que efectivamente son expresiones válidas en línea (Douek, 2020).

3.3.2. Discurso de odio y la incitación a la violencia en línea

Uno de los ámbitos más complejos de la sanción del odio en línea es la falta de delimitación de lo que constituye expresión de odio. En años recientes parece haberse hecho más popular la expresión "discurso de odio", aun cuando puede ser equívoca. Se trata de una expresión que parece replicar un término anglo-parlante ("*hate speech*"), comprehensivo de distintas incitaciones a la violencia y la discriminación, pero sin una consagración legal o jurisprudencial como la que ya tienen ciertas formas de incitación a la violencia discriminatoria.

Ciertamente, definir normativamente el "odio" parece un esfuerzo estéril frente a la necesidad de delimitar conductas concretas sin afectar a la libertad de expresión y opinión. Lo mismo ocurre si ciertas expresiones pueden legítimamente interpretarse como formas de discriminación en función de razones contextuales, sin que se trate más que de expresiones molestas, pero no menos protegidas.

No obstante, dentro de una narrativa global contraria a la discriminación y las expresiones violentas, resulta un concepto suficientemente extendido como para ser de utilidad. Así, la Organización de las Naciones Unidas (ONU) ha hecho propio el término para la difusión del Plan de Acción de Rabat sobre la prohibición de la apología del odio nacional, racial o religioso que constituye incitación a la discriminación, la hostilidad o la violencia (ONU, 2012): un documento resultante de la reunión convocada por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) con

conclusiones y recomendaciones para prevenir y combatir el odio y la discriminación. A partir de reuniones de expertos también se llegó a una estrategia y plan de acción, con consensos tales como la caracterización del discurso de odio como "cualquier forma de comunicación de palabra, por escrito o a través del comportamiento, que sea un ataque o utilice lenguaje peyorativo o discriminatorio en relación con una persona o un grupo sobre la base de quiénes son o, en otras palabras, en razón de su religión, origen étnico, nacionalidad, raza, color, ascendencia, género u otro factor de identidad" (ONU, 2019a).

En el contexto latinoamericano esto presenta dos aristas de interés. La primera es la relativa al discurso de odio como categoría problemática desde la perspectiva de los derechos humanos, esto es, como fuente de afectación de los derechos de personas, especialmente de grupos vulnerables, y en particular con el efecto de silenciar o excluir del debate en línea a las personas que integran tales grupos. La segunda arista es la del discurso de odio como límite a la libertad de expresión materializado tanto en restricciones y consecuencias de carácter legal como respecto de las medidas que pueden adoptarse para su limitación en el entorno digital bajo reglas más estrictas que las legales.

Respecto de lo legal, la prueba del umbral de Rabat (ONU, 2012) exige considerar, para la calificación de un acto expresivo como discurso de incitación al odio: 1) el contexto social y político, 2) la categoría del hablante, 3) la intención de incitar a la audiencia contra un grupo determinado, 4) el contenido y la forma del discurso, 5) la extensión de su difusión, y 6) la probabilidad de causar daño, incluso de manera inminente. Es solo entonces que resulta convencionalmente admisible la restricción.

En el sistema interamericano, el estándar regional exige una prueba "actual, cierta, objetiva y contundente" de que la alegada conducta de incitación no era la simple manifestación de una opinión (por dura, injusta y perturbadora que fuera) y que tenía no solo una intención clara de cometer un crimen sino también la posibilidad actual, real y efectiva de lograr sus objetivos (OEA, 2009). Ello no ha obstado a soluciones legislativas muy diversas, que Bertoni (2011) ha sistematizado entre modelos sancionatorios y no sancionatorios, con los primeros alternando entre la sanción mediante códigos penales, penalización en leyes separadas, y prohibiciones relativas a medios de comunicación. A la vez, los contenidos regulatorios son profundamente diversos en cuanto a los requisitos del tipo penal.

Estas diferencias se ven exacerbadas con tendencias recientes a abordar los discursos de incitación al odio sin una perspectiva propia del sistema internacional

ni del sistema interamericano de derechos humanos, aparentemente con la motivación de abordar el problema del odio en línea. Díaz (2020) da cuenta de la existencia de distintas iniciativas regulatorias, que incluyen las siguientes:

· En Honduras, una iniciativa de 2018 pretendía regular "los actos de odio y discriminación en redes sociales e Internet", con responsabilidad para las empresas de proveedores de servicios de internet y plataformas, y vaga definición del objeto de reproche.

· En Perú, la iniciativa de un congresista para regular "la utilización indebida de redes sociales", incluyendo una versión agravada del delito de difamación, en 2019.

· En Colombia, un proyecto del Código Electoral de 2020 incluía sanción a conductas de violencia política contra las mujeres mediante difusión de imágenes o mensajes de mujeres en ejercicio de sus derechos políticos de forma física o virtual, con el objetivo de afectar negativamente a su imagen pública o limitar sus derechos políticos.

No obstante, la más evidente restricción bajo la excusa del combate a la incitación al odio es una iniciativa de ley exitosa en Venezuela. La Ley contra el Odio, la Intolerancia y por la Convivencia Pacífica —sancionada en noviembre de 2017 por la Asamblea Nacional Constituyente— incluye penas de cárcel, órdenes de remoción de contenidos, sanciones de revocación de concesiones a medios de comunicación y empresas de internet, prohibiciones de funcionamiento de organizaciones, entre otros. Según el Instituto Prensa y Sociedad de Venezuela, entre 2018 y 2021, 18 casos de medios de comunicación y trabajadores de prensa fueron objeto de persecución por esta ley (IPYS, 2022), que ha recibido fuertes críticas desde dentro y fuera de Venezuela, incluso desde la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) (OEA, 2017b). A cierre de este capítulo (diciembre de 2022), la ley seguía siendo usada contra expresiones proferidas en redes sociales.

3.3.3. Desinformación y el acceso a información verídica

Mencionamos antes que la idea de una sociedad bien informada es uno de los objetivos de la protección del derecho a la libertad de expresión y el acceso a la

información. Es una condición necesaria dentro de una sociedad democrática, un factor crucial para que las personas o para que grupos incidan en la vida pública; y más que eso, "una sociedad que no está bien informada no es plenamente libre" (Corte IDH, 1985). Subsecuentemente, es una duda razonable si la expectativa de una sociedad bien informada constituye la base para exigencias de veracidad, es decir, si el derecho a estar informado incluye, correlativamente, el derecho a no recibir información falsa.

Dentro del sistema interamericano, la respuesta es negativa. La Corte IDH, en su Opinión Consultiva OC 5-85, ha declarado que no es aceptable exigir que el ejercicio de la libertad de expresión esté atado a una condición de veracidad: si fuera así se abriría una puerta de abusos sobre los controles de la información que afectaría al derecho de acceso a la información de todas las personas.

A la vez, no solamente no puede exigirse veracidad para la protección, sino que tampoco puede usarse como base para restringir expresiones no veraces, pues es contradictorio "invocar una restricción a la libertad de expresión como un medio para garantizarla, porque es desconocer el carácter radical y primario de ese derecho como inherente a cada ser humano individualmente considerado, aunque atributo, igualmente, de la sociedad en su conjunto" (Corte IDH, 1985).

En otras palabras, también las falsedades constituyen por regla general un discurso protegido, sin perjuicio de otras responsabilidades ulteriores. Esto refleja suficientemente las dificultades por abordar cabalmente el fenómeno de la desinformación. En nuestra opinión, se trata de un fenómeno muy complejo que supera la dicotomía verdad/falsedad, de por sí difícil de resolver. Se trata de un fenómeno que también se extiende a la difícil definición sobre cuánta información es necesaria para poder decir que está disponible la información completa, pertinente y actual relacionada con un hecho específico. También es complicado abordar la intención de los agentes de un acto comunicativo. Por todo lo anterior, sin perjuicio de los numerosos intentos de listar tipos de desinformación (Spitzberg, 2022), resulta preferible hablar en términos genéricos sobre desórdenes informativos, y abordar manifestaciones concretas a nivel normativo.

Al igual que con otros fenómenos aparentemente exacerbados por internet, la respuesta desde los países de América Latina ha estado marcada por la contingencia, incluida la proveniente de momentos políticos álgidos y de la pandemia de la COVID-19. Según Pita (2021), esto se ha mostrado principalmente como una respuesta generalmente punitiva, tanto a través de la apli-

cación de reglas vigentes como en la búsqueda de la aprobación de nuevas reglas contra la difusión de falsedades, especialmente a través de medios de comunicación y a través de internet. Entre los ejemplos más significativos debemos considerar estos:

· La Ley Especial de Ciberdelito en Nicaragua, que establece en su artículo 30 sanciones de cárcel y multa por la propagación de "información falsa y/o tergiversada, que produzca alarma, temor, zozobra en la población, o a un grupo o sector de ella, a una persona o a su familia". Desde antes de su promulgación, la ley era objeto de crítica como fuente de restricción del trabajo de periodistas y comunicadores (BBC, 2020).

· En Bolivia, durante un muy disputado periodo político en marzo de 2020, dos decretos supremos anunciaban que se extendería la persecución por delitos penales a quienes difundieran "información [...] que ponga en riesgo o afecte a la salud pública, generando incertidumbre en la población", a pesar de que la desinformación no es un delito penal en ese país (InternetBolivia, 2021).

· Un proyecto de ley en Brasil —la llamada Ley de Fake News (PL 2630/2020)— fue presentado en 2020 para ordenar tanto el retiro de informaciones falsas como el rastreo de mensajes, entre otras medidas. La versión de 2020 fue objeto de amplia controversia y rechazo (Derechos Digitales, 2020a). Una nueva versión de marzo de 2022, con varios aspectos corregidos, no recibió respaldo para votación urgente antes de la elección presidencial de fines de año.

· También en Brasil, frente a la elección presidencial de 2022, cabe mencionar las acciones del Tribunal Superior Electoral (TSE). Conforme a lo dispuesto por el Código Electoral de ese país, que prohíbe en su artículo 323 la divulgación en periodo de campaña de datos conocidamente falsos en relación con partidos o candidatos, que puedan influenciar al electorado. El presidente del TSE anunció públicamente la preocupación por la difusión de falsedades específicamente en internet, y fue bajo esa lógica que en marzo de 2022 ordenó el bloqueo de Telegram en Brasil (*El Mundo*, 2022).

· A todo lo anterior se suma lo reportado por Pita (2021) en torno a la advertencia de la intención de uso, de reglas penales vigentes, aplicadas contra la diseminación de información supuestamente falsa, en Colombia, Ecuador, Guate-

mala, Panamá y Perú, y el uso de normas de esa clase en Argentina[6], Bolivia[7] y Brasil. A la vez, nuevos proyectos de ley durante el periodo de pandemia en Argentina, Brasil, Chile, El Salvador, Panamá y Paraguay planteaban nuevas sanciones contra la diseminación de información falsa.

Las iniciativas anteriores dan cuenta de una actitud más activa por parte de distintos órganos en torno a la desinformación en contextos electorales y de crisis sanitaria, pero con serias fallas de desproporcionalidad entre el resultado buscado y las medidas adoptadas. Sea por falta de ponderación o como efecto intencionalmente buscado, esas medidas terminan apareciendo como una sobrerreacción al problema, contraria a la libertad de expresión. No corresponde desconocer que el problema es real; no obstante, sus complejidades no deberían ser resueltas en desmedro de la expresión ni con base en una dicotomía entre restricción y no restricción. En palabras de la actual Relatora Especial para la libertad de expresión de la ONU, tanto las prácticas de las empresas como la regulación estatal deben apuntar hacia la transparencia, los derechos de las personas usuarias, y los deberes de precaución de las empresas respecto de los derechos humanos, incluso en relación con los modelos de negocio que dependen del tratamiento de información personal (ONU, 2021).

3.3.4. La violencia de género en línea

Los actos de violencia perpetrados con auxilio o por medio de tecnologías de la información y la comunicación contra mujeres, niñas y personas LGBTIQ+ son un fenómeno estudiado en todo el mundo, incluida América Latina. Se trata de una categoría de actos de violencia de género cometidos, facilitados o agravados por el uso de tecnologías de la información y la comunicación (Association for Progressive Communications, 2015). La violencia de género en línea cubre una serie de actos ya mencionados, incluidos la creación o difusión de contenido íntimo sin consentimiento, ataques contra la reputación, ciberacoso, amenazas, *cyberbullying*, hackeo de dispositivos y acceso no autorizado a servicios, vigilancia de comunicaciones, entre muchos otros. La propia OEA ha facilitado la creación de conocimiento práctico en la materia, recogiendo tanto las distintas experiencias de violencia en las Américas

[6] Ferreyra (2021) menciona la persecución en Argentina, no solo por las publicaciones en sitios web, sino también por mensajes de WhatsApp.
[7] Véase InternetBolivia (2021) para un extenso listado de casos en Bolivia.

como los esfuerzos y recomendaciones para combatirlas (Vera Morales, 2021).

Es importante reconocer la violencia de género como fenómeno singular de vulneración de los derechos humanos de las personas afectadas. No solamente en términos de los intereses directamente afectados, sino también por lo que implica: la limitación en la capacidad de mujeres, niñas y personas LGBTIQ+ de utilizar de manera libre y sin miedos ni amenazas las tecnologías de información y comunicación, inclusive para su libre expresión. Los despliegues de esfuerzos de control y silenciamiento, mediante actos de violencia de género constituyen, por tanto, vulneraciones de la libertad de expresión que deben considerarse como amenazas de derechos humanos (Art. 19, 2020). Las iniciativas de ley en América Latina (Vera Morales, 2021), si bien variadas, todavía apuntan a manifestaciones externas de problemas sociales más amplios.

No obstante, los propios órganos internacionales que promueven acciones contra la violencia de género en línea han resaltado la dificultad de la regulación frente a los desafíos por preservar la libertad de expresión. En el Día Internacional de la Mujer Trabajadora (8 de marzo) de 2017, tanto el entonces Relator especial de Naciones Unidas para la libertad de expresión como la Relatora especial de Naciones Unidas sobre la violencia contra la mujer, sus causas y consecuencias, hicieron un llamado a los gobiernos, las empresas y la sociedad civil a abordar el abuso y la violencia de género en línea. Señalaron que un internet libre de abuso es vital para la libertad de expresión de las mujeres; no obstante, advirtieron la necesidad de cumplir con estándares de derechos humanos para evitar la censura, que también puede afectar especialmente a las mujeres (ONU, 2017).

3.4. Regulación de plataformas y responsabilidad por contenido de terceros

Uno de los elementos clave en la gestión de las libertades informativas en la era digital es la importancia de las empresas intermediarias, a saber, los actores mayoritariamente privados que mantienen la capacidad de controlar la difusión de contenidos en internet, con alcance global. Ello se extiende a la difusión de contenidos como los descritos más arriba: ilegales, prohibidos, o incluso legales pero con gran potencial de causar daño. Como expresa Kaye (2019), las plataformas se han convertido en espacios abiertos para el debate público y privado, con el odio difundiéndose a través de los sistemas de amplificación facilitados por las plataformas, y como zonas exitosas y rentables para la desinformación, la interferencia electoral y la propaganda. A la vez, las mismas plataformas se

han convertido en instituciones de gobernanza con reglas y esquemas burocráticos de observancia.

De lo anterior ha surgido un nutrido debate con expresiones en la doctrina, la legislación, la jurisprudencia, los órganos de derechos humanos y el público general, sobre la necesidad de hacer que las plataformas, en cuanto puntos de control, rindan cuentas de sus actividades y a la vez mantengan un rol potenciador de la expresión. El volumen y la profundidad de esos debates exceden a estas páginas; no obstante, es necesario destacar sucesos en la región que son importantes para el arduo proceso de alineación de expectativas sobre los esquemas de regulación y de gobernanza de la expresión en línea.

Desde una perspectiva más amplia, sobre la regulación de las plataformas en sus distintas aristas, la experiencia latinoamericana no ha sido especialmente rica. Donde sí ha existido un mayor desarrollo es en relación con la responsabilidad de los intermediarios de internet por los contenidos de terceros, es decir, en la determinación de las consecuencias sobre las empresas intermediarias allí donde su función facilite la disponibilidad o la difusión de contenidos ilícitos, y bajo qué condiciones operaría esa responsabilidad.

La responsabilidad de los intermediarios por los contenidos de terceros puede tener varias formas, como la inmunidad absoluta, la responsabilidad objetiva, la responsabilidad subjetiva y la responsabilidad condicionada (Meléndez, 2012). De estas opciones, ya desde la Declaración conjunta (ONU *et al.*, 2011) se excluía la opción de la responsabilidad objetiva, que desincentivaría radicalmente la existencia de intermediarios (OEA, 2013) y sirve como base para una censura privada contraria a la libertad de expresión (ONU, 2011).

De ese catálogo de opciones, sin embargo, la mayor parte de América Latina no ha logrado incluir reglas legales explícitas. La jurisprudencia, sin embargo, se ha preocupado de delimitar o excluir ciertas formas de responsabilidad, avanzando en general hacia sistemas de responsabilidad condicionada por la acción del intermediario frente al conocimiento de que está facilitando la difusión de un contenido ilícito, calificado entonces como beneficiario de un puerto seguro (*safe harbor*). Así, a modo de ejemplo, cabe citar:

· En Argentina, el caso Rodríguez con Google (2014) excluye la responsabilidad objetiva porque afectaría a la libertad de expresión, pero admite que podría asignarse responsabilidad a un "buscador" cuando este "haya tomado efectivo conocimiento de la ilicitud" de un contenido y tras ello no adoptó un "actuar diligente", de conformidad con las reglas de responsabilidad objetiva

del Código Civil. El criterio fue ratificado en 2017 en Gimbutas con Google, con posterioridad a la entrada en vigor del nuevo Código Civil y Comercial de Argentina.

· En Brasil era habitual que se atribuyera responsabilidad objetiva a proveedores de servicios de internet hasta antes de la entrada en vigor del Marco Civil de Internet de 2014 (Del Campo *et al*., 2021). A la vez, hasta agosto de 2018, alrededor del 60% de las solicitudes judiciales de remoción de contenidos en Brasil eran ilegítimas, infundadas o abusivas (Oliva, 2019). No obstante, la jurisprudencia reciente parece avanzar en un sentido más restringido.

· En Colombia, la Corte Constitucional ha reafirmado que los intermediarios de internet no son responsables por el contenido que publican sus usuarios como sí lo son quienes publican ese contenido, pero una autoridad judicial puede ordenar su remoción, como expresó la Sentencia de Unificación de Tutela SU-420/19.

Legalmente, son desarrollos relevantes los siguientes:

· En 2014, Brasil introdujo un mecanismo de responsabilidad que opera como regla general sobre su sistema, en el artículo 19 del Marco Civil de Internet. En virtud del mismo, un intermediario solo puede ser civilmente responsable de los daños producidos por contenidos de terceros si no hace indisponible el contenido después de una orden judicial específica. Las excepciones son los casos de contenido sexual íntimo, sometido a una notificación privada, y los contenidos infractores de derechos de autor, exceptuados en el propio Marco Civil, pero sin reglamentación especial hasta la fecha (Vargas, 2020).

· En 2010, Chile ya había introducido un sistema de responsabilidad de prestadores de servicios en internet con la exigencia de orden judicial como gatillante, restringido sin embargo a las infracciones en materia de derechos de autor. El sistema es profundamente detallado y es consecuencia del tratado de libre comercio (TLC) entre Chile y EE.UU., aun cuando no sigue de manera estricta el modelo estadounidense (la Digital Millennium Copyright Act de 1998, o DMCA) que motivaba la propuesta (Lara y Sears, 2020), y que requiere tan solo una notificación privada como forma de conocimiento que hace operativo el esquema de responsabilidad.

· En Costa Rica, el régimen de exenciones de responsabilidad de intermediarios por infracciones de derechos de autor cometidas por terceros fue establecido a través del Reglamento nº 36880-COMEX-JP de 2011, que establece un procedimiento de notificación privada y un procedimiento judicial.

· En Paraguay, la ley nº 4.868 de 2013 establece un procedimiento de notificación y bajada administrativo, y permite un mecanismo privado de notificación y bajada establecido por los intermediarios en el caso de infracciones de propiedad intelectual. El esquema, en general, es tan indeterminado que su operación concreta y su adecuación al marco internacional de libertad de expresión están en entredicho (Vargas, 2016).

· Cabe mencionar algunos de los muchos proyectos que no han llegado a convertirse en ley:

1) En Colombia un primer intento por implementar la responsabilidad por infracciones de derechos de autor ordenadas por el TLC entre ese país y EE.UU., proyecto conocido como Ley Lleras y que establecía un sistema de notificación privada afín a la DMCA, pero que fue rápidamente presentado y archivado, con gran rechazo público (Cortés, 2013).

2) En Argentina, un proyecto de ley sobre responsabilidad de intermediarios de alcance general fue discutido entre 2016 y 2018, incluyendo una disposición general de responsabilidad que requería una orden judicial de remoción para operar, y admitía esquemas de autorregulación (Ferreyra, 2017). El proyecto no fue aprobado y tampoco había consenso entre los miembros de distintas partes interesadas sobre la conveniencia de la iniciativa.

3) En México, el 1 de julio de 2020 se reformó la Ley Federal de Derechos para establecer un sistema de exención de responsabilidad de intermediarios, también para infracciones de derechos de autor, como un sistema mixto que funcionaba por aviso privado de los titulares de derechos como por resolución de la autoridad competente, o en caso de haber medidas tecnológicas para identificar material protegido automáticamente. El proyecto está siendo revisado judicialmente tras la acción de inconstitucionalidad presentada por la Comisión Nacional de Derechos Humanos, frente a lo

que se interpreta como una amenaza a la libertad de expresión, acción celebrada por los detractores de la polémica reforma (*El Universal*, 2020).

Íntimamente relacionada con la responsabilidad legal surge la cuestión sobre la legalidad de reglas de moderación de contenidos allí donde no solamente se crean mecanismos para restringir expresiones declaradas como ilegales, sino también para la remoción de contenidos que en rigor no son ilegales, pero son igualmente dañinos o indeseados para las propias plataformas o para sus usuarios. Es decir, las reglas de remoción allí donde no hay una sanción legal a —por ejemplo— discursos discriminatorios o la difusión de información personal. No se trata de un problema sencillo: que las plataformas mantienen un poder sobre la expresión individual es incuestionable, pero las reglas a que se ciñe la conservación de esas expresiones son en general las propias de las plataformas, con categorías de contenido a remover más extensas y amplias que las que se aceptarían como discurso restringido por la autoridad pública. Y esas decisiones sobre contenidos —en circunstancias tales como la pandemia de la COVID-19 o los periodos electorales— vienen también condicionadas por las expectativas gubernamentales sobre el comportamiento de plataformas privadas (Keller, 2019).

La misma circunstancia es verificable en aquellos casos en que la sanción legal, o al menos el mecanismo operativo para ordenar la restricción de contenidos, no se ha convertido en parte de la legislación nacional. Esto ha significado que se usen ya no los mecanismos legales, sino los mecanismos propios de las plataformas de internet, a su vez basados en esquemas legales como la DMCA estadounidense, para así quitar de circulación contenidos o expresiones perfectamente legítimas, a menudo con fines de acatamiento o censura, sin la necesidad de una orden judicial. Los ejemplos más elocuentes son:

· En Ecuador, la empresa española Ares Right, representando al gobierno ecuatoriano, usó la DMCA para exigir a los proveedores de servicios de la organización Fundamedios en EE.UU. el retiro de contenidos del gobierno, en circunstancias que la organización realizaba acciones de crítica política (Fundamedios, 2015). Casos similares han ocurrido con posterioridad.

· En Nicaragua, en 2020, se cerraron las cuentas de YouTube de dos canales de noticias (cuyas instalaciones físicas ya habían sido ocupadas), tras múltiples quejas por infracciones de derechos de autor presentadas por empresas de pro-

piedad de la familia gobernante (CPJ, 2020), en un caso flagrante de uso de la normativa de derechos de autor para la censura.

Quepan aquí algunas líneas también sobre otra forma indirecta del uso de mecanismos dirigidos a los intermediarios, para la defensa de intereses particulares y con el riesgo de impactar el derecho a la libertad de expresión y el acceso a la información. Nos referimos a las solicitudes de desindexación de datos personales de identificación desde motores de búsqueda de internet (derecho al olvido) en la clave popularizada por el Tribunal de Justicia de la Unión Europea desde 2014, con el bullado fallo en el caso Google Spain. Esto consiste fundamentalmente en la supresión o cancelación de ciertos resultados al buscar nombres en motores de búsqueda de internet, sin afectar al contenido de los sitios donde está contenida la información indizada.

La alegación presenta no solamente el problema de la falta de regulación directa en la materia, o la aparente insuficiencia de las leyes de protección de datos personales, sino también la ausencia de criterios legalmente fijados para resolver problemas de ponderación de derechos: la necesidad de sopesar el interés público frente a la protección de datos personales; la consideración de la ubicuidad y persistencia de información en línea; la ausencia de mecanismos que fijen directamente los órganos y procedimientos para la ponderación de derechos fundamentales, etc. Ciertamente, todo ello presenta no solo contrastes respecto de las diferencias normativas entre la Unión Europea y los países latinoamericanos, sino también respecto de las perspectivas políticas sobre el pasado y la verdad, hasta el punto de calificarse la alegación de este derecho como un "insulto" a la historia latinoamericana (Bertoni, 2014).

Para los estándares para internet del sistema interamericano, no existiendo una protección a este derecho, cualquier intento regulatorio de reconocimiento debe hacerse de manera extraordinariamente limitada: la regulación debe ser "absolutamente excepcional", en casos de daño sustantivo, mediando sentencia judicial que pondere distintos derechos y con caracteres de debido proceso, de manera participativa y transparente (OEA, 2017a). En palabras de Keller (2019), basar un derecho al olvido en reglas de protección de datos similares a las de la Unión Europea conlleva un "desequilibrio en las reglas, que dejan sin protección suficiente a los derechos de libertad de expresión de los usuarios de internet", por lo que deben considerarse resguardos de esos derechos.

3.5. Represión, vigilancia y ataques cibernéticos

Todo lo considerado en los apartados anteriores constituye formas específicas de afectación, tanto positiva como negativa, de la libertad de expresión en línea en América Latina. No obstante, volviendo a un punto inicial, existe una continuidad entre los derechos humanos fuera de línea y los que se ejercen en internet. Y esto alcanza también a formas de afectación de la libertad de expresión —en América Latina, con contextos e historias plagados de prácticas autoritarias y abusos gubernamentales y de empresas privadas, los impactos sobre las libertades informativas se ven también reproducidos en línea— y respecto de las personas, grupos y organizaciones que usan internet para el legítimo ejercicio de sus derechos.

En contextos de prácticas autoritarias, las restricciones sobre la libertad de expresión descritas anteriormente no son actividades aisladas, sino que suelen venir acompañadas de formas más tradicionales de incidir negativamente sobre la libre opinión y expresión, como ocurre con las acciones de violencia o intimidación mediante amenazas, acoso o agresiones físicas. También ocurre con las acciones de represión legal, como el cierre de medios o la persecución penal de las personas por sus opiniones en línea, como en los casos de Venezuela y Nicaragua ya indicados. Todo ello lleva o pretende llevar a la supresión de la expresión, es decir, al silencio. No ahondaremos en ejemplos, a riesgo de no dar espacio justo a situaciones extremas de vulneración de derechos humanos. No obstante, cabe destacar algunas categorías concretas de afectaciones indirectas a la libertad de opinión y expresión en América Latina, mediante acciones que pueden derivar en el silenciamiento, o peor, la autocensura de personas o grupos completos afectados por esas prácticas.

3.5.1. El ciberpatrullaje

No es de extrañar que gobiernos de todo el mundo incurran en la revisión de las expresiones en internet, en sitios web y redes sociales abiertas, en lo que se conoce como inteligencia de redes sociales o SOCMINT (Social Media Intelligence), a saber, las técnicas y tecnologías que permiten monitorear sitios de redes sociales digitales, incluyendo mensajes o imágenes, como también otros datos generados (Privacy International, 2017) como la ubicación o la hora. Se trata de formas de recolección de información útiles para detectar el contenido del debate público, y también para identificar y perfilar a personas específicas,

incluso con el propósito de persecución criminal. Resulta problemático que tales actividades no estén específicamente reguladas, a pesar del riesgo exacerbado sobre los derechos a la privacidad, al debido proceso y la presunción de inocencia, y finalmente a la libertad de expresión que estas prácticas suponen.

En años recientes, especialmente marcados por la pandemia de la COVID-19, hemos sido testigos de iniciativas más o menos abiertas para el ciberpatrullaje, entendiendo como tal un conjunto diverso de métodos para la recolección de información desde redes sociales digitales, con fines de inteligencia, de investigación criminal, o de detección de situaciones de riesgo. Los que siguen son casos que se han producido en la región:

· En Argentina, en abril de 2020, el gobierno reconoció que recurriría al ciberpatrullaje para "detectar el humor social" (Ferreyra, 2021), incluidas convocatorias a disturbios y saqueos. El gobierno preparó un protocolo de actuación para enfrentar las críticas, aunque la autoridad de control de datos personales solicitó su suspensión por ser insuficiente para la protección de la privacidad (Roko y Serra, 2021).

· En Bolivia, en marzo de 2020, sin protocolos de por medio y en un contexto de gobierno de transición al inicio de la pandemia, uno de los ministros anunció el ciberpatrullaje para identificar instancias de desinformación sobre la COVID-19 (InternetBolivia, 2021). La coincidencia temporal con otras medidas de carácter represivo (Derechos Digitales, 2020b) hacía sospechosa la declaración como una no necesariamente vinculada a la gestión sanitaria, sino de control del flujo de información en el país (InternetBolivia, 2021).

· Desde finales de abril de 2021, en Colombia estalló una serie de enormes protestas contra una reforma tributaria propuesta por el gobierno y otras medidas públicas (Guerra, 2021). La situación llevó a una fuerte represión policial, como también al reconocimiento del Ministerio de Defensa de que desde el Puesto de Mando Unificado Cibernético (PMU-Ciber) se monitorearían redes sociales para identificar información falsa que afectaba a la imagen de la Policía Nacional (FLiP, 2021). La CIDH recibió denuncias sobre la situación en su visita *in loco* a Colombia con motivo de las protestas (OEA, 2022).

· En El Salvador, el ministro de Seguridad y Justicia reveló en julio de 2021 que el monitoreo de redes sociales se había "intensificado" en razón de un alza en

las denuncias sobre delincuencia (Elsalvador.com, 2021), al mismo tiempo que anunciaba otra serie de medidas de seguridad interior.

Es importante destacar que la prevalencia de la persecución judicial del discurso en línea en distintos países de la región permite afirmar que prácticas de inteligencia de redes sociales o de ciberpatrullaje son más frecuentes que en los casos en que la autoridad lo admite públicamente. Esto, a la vez, puede llevar al silenciamiento o la autocensura, por lo que debe considerarse un riesgo continuo para la libertad de expresión mientras no existan marcos legales suficientes para fijar los límites de estas prácticas.

3.5.2. Ataques cibernéticos y vigilancia

La seguridad de los sistemas digitales, desde las redes hasta los equipos, pasando por las distintas plataformas y servicios, es una cuestión compleja que obliga a una actitud vigilante entre distintas personas. No obstante, ataques dirigidos contra activistas y defensores de derechos humanos, en particular quienes ejercen sus libertades de opinión y expresión para acciones contrarias o críticas del poder, se han visto frecuentemente en América Latina, inclusive a través de técnicas sofisticadas.

Deben considerarse dos aristas significativas. La primera tiene relación con el uso de técnicas destinadas a hacer fallar sitios de medios de comunicación, blogs, organizaciones activistas y más. Así, por ejemplo, esa clase de ataques se han vuelto habituales en Venezuela, donde solo en 2021 se verificaron 14 ataques de distinta naturaleza según la organización Redes Ayuda (2022).

Un segundo gran sentido de preocupación es el relativo a las tecnologías para la vigilancia. En 2019, el entonces Relator Especial de la ONU para la libertad de expresión emitió un informe vinculando directamente la afectación de la libertad de expresión con las actividades de vigilancia, especialmente aquellas que se sirven de tecnologías digitales (ONU, 2019b). Según el entonces Relator Especial, "la interferencia con la privacidad mediante la vigilancia selectiva está diseñada para reprimir el ejercicio del derecho a la libertad de expresión" (ONU, 2019b).

Una parte de esta preocupación apunta al desarrollo o la adquisición de tecnologías para la vigilancia, sea en forma de falsas antenas de telefonía celular (los IMSI catchers) o bien en forma de tecnología de vigilancia dirigida, usualmente operativa mediante la explotación de vulnerabilidades o fallas de

seguridad en equipos informáticos como computadores y teléfonos celulares. El informe de la ONU mencionaba empresas como Gamma International, Hacking Team o NSO Group, que junto a otras como M.L.M. Protection o Digitro Tecnologia Ltda., han vendido tecnología para la vigilancia a países de América Latina.

Por otra parte, han existido revelaciones concretas del uso de estas tecnologías de vigilancia para afectar directamente a personas —en particular activistas y periodistas— de una forma tan intrusiva que resulta difícil conciliar la vigilancia mediante *spyware* con cualquier forma legalmente permitida de recolección de información. Entre estos casos de escándalo pueden citarse los siguientes:

· En 2015, en Ecuador, el activista opositor Carlos Figueroa sufrió hackeo de sus cuentas de redes sociales, como consecuencia de la acción de la Secretaría Nacional de Inteligencia en uso de *software* de Hacking Team (Bajak y Satter, 2015).

· En México, en 2017, se reveló el uso del *software* Pegasus, de The NSO Group, para vigilar a abogados de derechos humanos, periodistas y activistas anticorrupción (Ahmed y Perlroth, 2017). Más revelaciones sobre el uso del mismo malware aparecerían con posterioridad.

· En El Salvador, en 2022, fue develada la inoculación de los teléfonos de la mayoría de los empleados de un sitio de noticias crítico del gobierno, entre julio de 2020 y noviembre de 2021 (Abi-Habib, 2022). El gobierno negó su responsabilidad.

En general, el conocimiento sobre estas adquisiciones y desarrollos aparece a través de filtraciones y reportes de prensa, y solo ocasionalmente por reconocimiento de los gobiernos de la región. Esto expone un problema significativo: el desconocimiento, por falta de transparencia, sobre la clase de tecnologías y capacidades con las que cuentan los Estados para llevar adelante acciones de vigilancia que afectan de manera crítica a periodistas, activistas o sus entornos personales, en franca vulneración de sus derechos. Es por esto que la vigilancia no debe ser vista solamente como un problema de seguridad digital o de privacidad, sino intrínsecamente como una afectación de la libertad de expresión.

4. Retos y líneas de trabajo pendientes

La Declaración conjunta sobre libertad de expresión e internet (ONU *et al.*, 2011) planteaba hace más de una década ciertas aproximaciones útiles para la posible regulación de la libertad de expresión en línea, haciendo notar que los enfoques regulatorios propios de otros medios de comunicación no pueden trasladarse sin más, sino que deben ser diseñados específicamente para las comunicaciones digitales. También advertía sobre la necesidad de que no se establezcan restricciones especiales al contenido de los materiales que se difunden a través de internet. Además, reconocía la posible efectividad de la autorregulación para abordar las expresiones injuriosas. Finalmente invitaba al fomento de medidas educativas y de concienciación destinadas a promover la capacidad de todas las personas de efectuar un uso autónomo, independiente y responsable de internet (alfabetización digital). En teoría, todo ello debía propender a un ambiente digital más favorable a la libre expresión, con base en los auténticos intereses de toda la ciudadanía.

Debemos reconocer también las situaciones de daño que se producen en línea. Situaciones cotidianas y muy reales de incitación a la violencia o actos de acoso en redes sociales digitales, con serias consecuencias para las víctimas, que afectan desde el debate público hasta la salud pública y la integridad de niños, niñas y adolescentes, a gran escala y fuera de expectativas realistas de control. En tales circunstancias, los esquemas regulatorios rígidos o que no contemplen un margen de acción a las propias empresas intermediarias pueden exacerbar los riesgos; a la vez, obligaciones desmedidas pueden resultar ineficaces o privilegiar acciones excesivas de retiro de contenidos, afectando a la expresión libre en línea. Atendida la dificultad de alcanzar el equilibrio, y la constante evolución de las plataformas y modos de comunicación, los llamados por una regulación (o corregulación) inteligente requieren un estudio más profundo.

En la realidad latinoamericana, los intentos de regulación parecen dirigirse más a formas de control del discurso público que de protección de los derechos de las personas, como se observa en algunos casos de prácticas autoritarias en la región. Toda misión por hacerse cargo de los riesgos y problemas en la expresión en el ciberespacio deben abordar también los excesos regulatorios. Coincidimos con Douek (2022) en que, aunque una moderación de contenidos sujeta a un formalismo —por acabado que este sea— no será suficiente para reflejar la complejidad, la amplitud, y el volumen de la expresión en línea, el ideal de los sistemas idóneos sigue siendo una aspiración válida, que debería guiar tanto

los esfuerzos dentro de cada plataforma como de la industria en general, y ciertamente a la vista de los intentos regulatorios estatales.

Por otra parte, la realidad del mundo mayoritario no puede ignorar el rol significativo de algunas empresas de tecnología ubicadas en el Norte global, con la capacidad no solamente de diseminar contenidos globalmente, sino también de fijar de manera concreta y eficaz las reglas de lo que es admisible o no en el debate público. Esto, a su vez, es parte de una economía basada en la explotación de información personal. Existe un desafío significativo de contrarrestar ese poder, de una forma que en los hechos no puede depender solamente de la voluntad estatal fragmentaria en regiones como América Latina, sino que requiere abordajes coordinados, tomando en cuenta simultáneamente las cuestiones de libertad de expresión y las de otras disciplinas como la protección de los derechos de los consumidores, la protección de la libre competencia contra los abusos de posición dominante de mercado y la protección de datos personales. Ello corresponde a un desafío normativo que por mucho supera las capacidades de Estados aislados, pero donde el sistema interamericano de derechos humanos puede servir como guía para la acción conjunta con los derechos humanos como centro de atención.

Referencias bibliográficas

14 y Medio (2020): "Los internautas cubanos denuncian el 'bloqueo intermitente' de las redes sociales" (30/11/2020). Disponible en: https://www.14ymedio.com/cuba/internautas-denuncian-bloqueo-intermitente-sociales_0_2994900490.html.

Abi-Habib, M. (2022): "Periodistas en El Salvador fueron blanco de un programa espía", *The New York Times* (12/01/2022). Disponible en: https://www.nytimes.com/es/2022/01/12/espanol/el-faro-pegasus.html.

Access Now (2019): "Targeted, Cut Off and Left in the Dark". Disponible en: https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf.

Agence France-Presse (2021): "Cuba restores internet access after protests, but not social media", *France24* (14/07/2021). Disponible en: https://www.france24.com/en/live-news/20210714-cuba-restores-internet-access-after-protests-but-not-social-media.

Ahmed, A. y Perlroth, N. (2017): "Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families", *The New York Times*

(19/06/2017). Disponible en: https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html.

Alcalde, C. y Solano, L. (2020): "En aumento y con sus propias características: la censura digital en Venezuela", *VOA News* (06/05/2020). Disponible en: https://dialogo-americas.com/es/articles/en-aumento-y-con-sus-propias-caracteristicas-la-censura-digital-en-venezuela/.

Antonialli, D. (2019): "Da 1ª instância ao STF: bloqueios e sanções do Marco Civil da Internet", *InternetLab* (22/4/2019). Disponible en: https://www.internetlab.org.br/pt/especial/da-1a-instancia-ao-stf-bloqueios-e-sancoes-do-marco-civil-da-internet/.

Article 19 (2016): *Freedom of Expression Unfiltered: How blocking and filtering affect free speech*. Disponible en: https://www.article19.org/data/files/media-library/38586/Blocking_and_filtering_final.pdf.

— (2020): *Freedom of expression and women's equality: Ensuring comprehensive rights protection.* Disponible en: https://www.article19.org/wp-content/uploads/2020/11/Gender-Paper-Brief-1.pdf.

Association for Progressive Communications (2015): "Technology-related violence against Women". Disponible en: https://apc.org/sites/default/files/HRC%2029%20VAW%202-pager_FINAL_June%202015_0.pdf.

Bajak, F. y Satter, R. (2015): "Exclusiva AP: Gobierno ecuatoriano hackea a opositores", *AP News* (07/08/2015). Disponible en: https://apnews.com/article/archive-60a199f39d064845b7683539eb199965.

BBC (2020): "Nicaragua: la dura ley que amenaza con cárcel a quien publique 'noticias falsas' en ese país", *BBC News Mundo* (28/10/2020). Disponible en: https://www.bbc.com/mundo/noticias-america-latina-54703913.

— (2022): "Cuba | "¡Queremos luz!": cientos salen a protestar por los apagones y el gobierno corta internet", *BBC News Mundo* (30/09/2022). Disponible en: https://www.bbc.com/mundo/noticias-america-latina-63097483.

Bertoni, E. (2011): "Estudio sobre la prohibición de la incitación al odio en las Américas", Oficina del Alto Comisionado de Derechos Humanos de Naciones Unidas. Disponible en: http://www.ohchr.org/Documents/Issues/Expression/ICCPR/Santiago/SantiagoStudy_sp.pdf.

— (2014): "The Right to Be Forgotten: An Insult to Latin American History", *HuffPost* (24/09/2014). Disponible en: https://www.huffpost.com/entry/the-right-to-be-forgotten_b_5870664.

— (2017): "OC-5/85: Su vigencia en la era digital", en OEA: *Libertad de Expresión: a 30 años de la Opinión Consultiva sobre la Colegiación Obligatoria de Periodistas*, Bogotá.

Björksten (2022): *A Taxonomy of Internet Shutdowns: The Technologies Behind Network Interference*, *Access Now.* Disponible en: https://www.accessnow.org/cms/assets/uploads/2022/06/A-taxonomy-of-internet-shutdowns-the-technologies-behind-network-interference.pdf.

Botero, C. (2021): "Una censura disfrazada de defensa de la infancia", *Razón Pública* (21/06/2021). Disponible en: https://razonpublica.com/una-censura-disfrazada-defensa-la-infancia/.

Carbonell Sánchez, M. (2011): "Los derechos fundamentales en América Latina: una perspectiva neoconstitucionalista", *Derecho y Humanidades*, 18, Universidad de Chile.

Citron, D. (2018): "Extremist Speech, Compelled Conformity, and Censorship Creep", *Notre Dame Law Review*, 93.

CNDH (2020): "CNDH presentó 46 acciones de inconstitucionalidad ante la Suprema Corte de Justicia de la Nación", CNDH (7/8/2020). Disponible en: https://www.cndh.org.mx/sites/default/files/documentos/2020-08/COM_2020_245.pdf.

CNN (2011): "El acceso a Internet, un derecho humano según la ONU" (9/6/2011). Disponible en: https://cnnespanol.cnn.com/2011/06/09/el-acceso-a-internet-un-derecho-humano-segun-la-onu/.

Committee to Protect Journalists (2020): "YouTube censors independent Nicaraguan news outlets after copyright complaints from Ortega-owned media" (06/05/2020). Disponible en: https://cpj.org/2020/05/youtube-censor-nicaragua-outlets-100-noticias-confidencial-ortega/.

Correa, M. (2018): "Zero-Rating y la neutralidad de la red en Chile", *Revista Chilena de Derecho y Tecnología*, 7(1), pp. 107-135. Doi: 10.5354/0719-2584.2018.48961.

Corte Interamericana de Derechos Humanos (1985): Opinión Consultiva OC-5/85 del 13 de noviembre de 1985, la colegiación obligatoria de periodistas (arts. 13 y 29, Convención Americana Sobre Derechos Humanos).

Cortés, C. (2013): "El debate pendiente en Colombia sobre la protección de derechos de autor en Internet. El caso de la 'Ley Lleras'", Fundación Karisma. Disponible en: https://redpatodos.co/wp-content/uploads/2013/04/Paper1ElCasoLeyLleras.pdf.

De Gregorio, G. y Stremlau, N. (2020): "Internet Shutdowns and the Limits of Law", *International Journal of Communication,* 14, 20. Disponible en: https://ijoc.org/index.php/ijoc/article/view/13752.

De Souza Abreu, J. (2018): "Disrupting the disruptive: making sense of app blocking in Brazil", *Internet Policy Review*, vol. 7, nº 3. Disponible en: https://doi.org/10.14763/2018.3.928.

Del Campo, A.; Schatzky, M.; Hernández, L. y Lara, J. C. (2021): "Mirando Al Sur. Hacia nuevos consensos regionales en materia de responsabilidad de intermediarios en Internet", *Al Sur*. Disponible en: https://www.alsur.lat/sites/default/files/2021-06/Responsabilidad%20de%20intermediarios%20ES.pdf.

Derechos Digitales (2020a): "Propuesta de regulación de desinformación puede aumentar brechas y exponer las comunicaciones de millones de personas en Brasil" (25/06/2020). Disponible en: https://www.derechosdigitales.org/ 14643/.

— (2020b): "Declaración pública: En respaldo a la libertad de expresión en espacios digitales y presenciales solicitamos la abrogación del DS. 423" (13/05/2020). Disponible en: https://www.derechosdigitales.org/14607/.

Díaz, M. (2019): "Apagones de Internet y censura en América Latina", Derechos Digitales (18/10/2019). Disponible en: https://www.derechosdigitales.org/13924/apagones-de-internet-y-censura-en-america-latina/.

— (2020): *Discurso de Odio en América Latina. Tendencias de regulación, rol de los intermediarios y riesgos para la libertad de expresión*, Derechos Digitales. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/discurso-de-odio-latam.pdf.

Douek, E. (2019): "Two Calls for Tech Regulation: The French Government Report and the Christchurch Call", *Lawfare* (18/5/2019). Disponible en: https://www.lawfareblog.com/two-calls-tech-regulation-french-government-report-and-christchurch-call.

— (2020): "The Rise of Content Cartels", Knight First Amendment Institute at Columbia, 2020. Disponible en: SSRN: https://ssrn.com/abstract=3572309.

— (2022): "The Siren Call of Content Moderation Formalism", en L. Bollinger y G. Stone (eds.): *Social Media, Freedom of Speech, and the Future of our Democracy*, Nueva York, Oxford Academic. Disponible en: https://doi.org/10.1093/oso/9780197621080.003.0009.

El Mundo (2022): "El bloqueo de 48 horas en Brasil que asustó a Telegram", *Pixel* (25/03/2022). Disponible en: https://www.elmundo.es/tecnologia/2022/03/25/623daec1e4d4d8453d8b4577.html.

El Universal (2020): "Celebran que CNDH haya presentado acción de inconstitucionalidad por reformas a ley de Derecho de Autor" (10/08/2020). Disponible en: https://www.eluniversal.com.mx/cultura/celebra-que-cndh-haya-presentado-accion-de-inconstitucionalidad-por-reformas-ley-de-derecho.

Elsalvador.com (2021): "Ministro de Seguridad confirma revisión de redes sociales de ciudadanos" (26/07/2021). Disponible en: https://historico.elsalvador.com/historico/862779/ministro-seguridad-revision-redes-sociales-ciudadanos.html.

Espacio Público (2020): "Internet amurallado: acceso restringido en Venezuela" (29/06/2020). Disponible en: http://espaciopublico.ong/internet-amurallado-acceso-restringido-en-venezuela/.

Ferraz, J. V.; De Souza, C. A.; Magrani, B. y Britto, W. (2012): "Filtrado de contenido en América Latina: razones e impacto en la libertad de expresión", en E. Bertoni (comp.): *Hacia una Internet libre de censura. Propuestas para América Latina*, Buenos Aires, Universidad de Palermo. Disponible en: http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf.

Ferreyra, E. (2017): "Responsabilidad de Intermediarios: comentarios acerca de un proyecto de ley clave para la libertad de expresión", Asociación por los Derechos Civiles (17/11/2017). Disponible en: https://adc.org.ar/2017/11/17/responsabilidad-intermediarios-comentarios-acerca-proyecto-ley-clave-la-libertad-expresion/.

— (2021): *La protección del espacio cívico en línea. Un repaso a las amenazas actuales a la libertad de expresión en internet*, Asociación por los Derechos Civiles. Disponible en: https://adc.org.ar/wp-content/uploads/2021/07/ADC-La-protecci%C3%B3n-del-espacio-c%C3%ADvico-en-l%C3%ADnea-07-2021.pdf.

Fuentes Torrijo, X. (2002): "La protección de la libertad de expresión en el sistema interamericano de derechos humanos y la promoción de la democracia", *Revista de Derecho*, 13 (diciembre). Disponible en: http://revistas.uach.cl/index.php/revider/article/view/2795.

Fundación para la Libertad de Prensa (2021): *En vivo: de la calle a la pantalla. Medios Digitales, redes sociales y protesta social*. Disponible en: https://www.flip.org.co/images/FLIP_C.E._Medios_paro_2021-V.2.pdf.

Fundamedios (2015): "SECOM intenta dar de baja página web de Fundamedios a través de reclamos de Ares Rights" (31/12/2015). Disponible en: https://www.fundamedios.org.ec/alertas/secom-intenta-dar-de-baja-pagina-web-de-fundamedios-traves-de-reclamos-de-ares-rights/.

Gilbert, A. (2021): "Cuba corta internet para evitar la diseminación de las protestas", *elPeriódico.com* (12/07/2021). Disponible en: https://www.elperiodico.com/ es/internacional/20210712/cubaba-corta-internet-evitar-diseminacion-11905584.

Global Voices (2019): "Netizen Report: Iraq and Ecuador Face Network Shutdowns Amid Public Protests" (11/10/2019). Disponible en: https://globalvoi-

ces.org/2019/10/11/netizen-report-iraq-and-ecuador-face-network-shutdowns-amid-public-protests.

Guerra, J. (2021): "¿Se han violado los derechos humanos en internet en Colombia? Necesitamos explorar esa posibilidad", Derechos Digitales (04/06/2021). Disponible en: https://www.derechosdigitales.org/16031/.

Internet Society (2017): *Perspectivas de Internet Society (ISOC) sobre el bloqueo de contenido en Internet: Visión general*. Disponible en: https://www.internetsociety.org/wp-content/uploads/2017/09/ContentBlockingOverview_ESLA.pdf.

— (2022): *Internet Society Pulse: Internet Shutdowns*. Disponible en: https://pulse.internetsociety.org/shutdowns.

InternetBolivia (2021): *Reporte sobre la situación de los derechos digitales en Bolivia durante el COVID-19*. Disponible en: https://internetbolivia.org/file/ 2020/11/fd_tecnopandemia_2021.pdf.

Kaye, D. (2019): *Speech Police: The Global Struggle to Govern the Internet*, Columbia Global Reports.

Keller, D. (2019): "Who Do You Sue? State and Platform Hybrid Power over Online Speech", *Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper*, nº 1902. Disponible en: https://www.lawfareblog.com/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech.

Lara, J. C. (2015): "Internet access and economic, social and cultural rights", Association for Progressive Communications. Disponible en: https://www.apc.org/sites/default/files/APC_ESCR_Access_Juan%20Carlos%20Lara_September2015%20%281%29_0.pdf.

— (2020): "El futuro del cifrado se define en Brasil", Derechos Digitales (07/08/2020). Disponible en: https://www.derechosdigitales.org/14800/.

Lara, J. C. y Sears, A. M. (2020): "The Impact of Free Trade Agreements on Internet Intermediary Liability in Latin America", en G. Frosio (ed.): *The Oxford Handbook of Online Intermediary Liablity*, Oxford University Press.

Llansó, E. (2019): "Platforms Want Centralized Censorship. That Should Scare You", *Wired* (18/4/2019). Disponible en: https://www.wired.com/story/platforms-centralized-censorship/.

LocaliQ (2022): "What happens in an internet minute?" (5/5/2022). Disponible en: https://localiq.com/resources/what-happens-in-an-internet-minute/.

Meléndez, H. (2012): "Intermediarios y Libertad de Expresión", en E. Bertoni (comp.): *Hacia una Internet libre de censura. Propuestas para América Latina*, Buenos Aires, Universidad de Palermo. Disponible en: http://www.palermo.edu/cele/pdf/internet_libre_de_censura_libro.pdf.

Oliva, T. (2019): "Responsabilidade de intermediários e a garantia da liberdade de expressão na rede", *InternetLab* (23/04/2019). Disponible en: https://www.internetlab.org.br/pt/especial/responsabilidade-de-intermediarios-e-a-garantia-da-liberdade-de-expressao-na-rede/.

ONU (2011): "Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión", Naciones Unidas, Asamblea General, A/HRC/17/27.

— (2012): "Annual report of the United Nations High Commissioner for Human Rights", Naciones Unidas, Asamblea General, A/HRC/22/17/Add.4.

— (2017): "UN experts urge States and companies to address online gender-based abuse but warn against censorship" (8/3/2017). Disponible en: https://www.ohchr.org/en/press-releases/2017/03/un-experts-urge-states-and-companies-address-online-gender-based-abuse-warn.

— (2019a): *La Estrategia y Plan de Acción de las Naciones Unidas para la lucha contra el Discurso de Odio*. Disponible en: https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_ES.pdf.

— (2019b): "La vigilancia y los derechos humanos Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión", Naciones Unidas, Consejo de Derechos Humanos, A/HRC/41/35.

— (2021): "La desinformación y la libertad de opinión y de expresión. Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan", Naciones Unidas, Consejo de Derechos Humanos, A/HRC/47/25.

OEA (2008): *Informe Anual 2008. Volumen II: Informe Anual de la Relatoría Especial para la Libertad de Expresión*, Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión.

— (2009): *Marco jurídico interamericano sobre el derecho a la libertad de expresión*, Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, OEA/Ser.L/V/II CIDH/RELE/INF.2/09.

— (2013): *Libertad de expresión e Internet*, Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, OEA/Ser.L/V/II, CIDH/RELE/INF. 11/13.

— (2017a): *Estándares para una internet libre, abierta e incluyente*, Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf.

— (2017b): "Relatoría especial para la libertad de expresión manifiesta su grave preocupación por la aprobación de 'la ley contra el odio' en Venezuela y sus efectos en la libertad de expresión y de prensa", Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión (10/11/2017). Disponible en: https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1082&lID=2.

— (2022): *Informe Anual de la Comisión Interamericana de Derechos Humanos 2021, Volumen II, Informe Anual de la Relatoría Especial para la Libertad de Expresión*, Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, OEA/Ser.L/V/II Doc. 64 rev. 1.

ONU, OEA, OSCE y CADHP (2011): "Declaración conjunta sobre libertad de expresión e internet". Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&lID=2.

Pereira da Silva, S.; Viollier, P.; Castro, O. y Brito, C. (2017): *Neutralidad de la red en América Latina: Reglamentación, aplicación de la ley y perspectivas*, Derechos Digitales.

Pita, M. (2021): "Desinformación durante la pandemia y la respuesta regulatoria Latinoamericana", UNESCO. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000377721.

Privacy International (2017): "Explainer: Social Media Intelligence" (23/10/2017). Disponible en: https://privacyinternational.org/explainer/55/social-media-intelligence.

Puddephatt, A. (2016): "Internet y la libertad de expresión", *Cuadernos de Discusión de Comunicación e Información*, 6, UNESCO.

Redes Ayuda (2022): *Informe 2.0 - Error 404: Democracia no encontrada*. Disponible en: https://redesayuda.org/wp-content/uploads/2022/06/INFORME-2.0-ESP-FINAL-1.pdf.

Roko, P. y Serra, F. (2021): "Los derechos de reunión y asociación en el espacio digital: perspectivas regionales a partir del caso argentino", *Revista Latinoamericana de Economía y Sociedad Digital*, 2. Disponible en: https://revistalatam.digital/issue/agosto-2021/?pdf=3078.

Sixirei, C. (2014): "Tres décadas de democracia en América Latina: una reflexión", *Revista Psicología Política*, 14(30), pp. 225-242.

Spitzberg, B. H. (2022): *Taxonomies and typologies of (dis/mis)information*, manuscrito no publicado, School of Communication, San Diego State University. Disponible en: http://dx.doi.org/10.13140/RG.2.2.28074.90565.

Triviño, R.; Franco, A. y Ochoa, R. E. (2019): "Regulación de la Neutralidad de Red en Latinoamérica: Una revisión del progreso", *Latin American Journal of Computing*, VI(1), pp. 17-26.

UNESCO (2019): *Indicadores de la UNESCO sobre la universalidad de Internet: marco para la evaluación del desarrollo de Internet*, París.

Urribarrí, R. y Díaz, M. (2018): "Políticas públicas para el acceso a internet en Venezuela. Inversión, infraestructura y el derecho al acceso entre los años 2000-2017", Derechos Digitales. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/CPI_venezuela.pdf.

Vargas, R. (2016): "Responsabilidad de intermediarios por infracciones a los derechos de autor en Chile, Paraguay y Costa Rica: Un análisis desde la libertad de expresión", *Revista Chilena de Derecho y Tecnología*, 5(1). Doi: https://doi.org/10.5354/0719-2584.2016.41782.

— (2020): "Sucesos regulatorios en materias de libertad de expresión e internet en Latinoamérica", *Derechos Digitales*. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/tendencias-regulacion-digitales.pdf.

Vera Morales, K. (2021): *La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta,* OEA/Ser.D/XXV.25.

Ververis, V.; Khrustaleva, O. y Quiroz, E. (2017): "Networks interference in Latin America: evaluating network measurements to detect information controls and internet censorship", *5º Simposio Internacional LAVITS | Vigilancia, Democracia y Privacidad en América Latina: Vulnerabilidades y resistencias*. Disponible en: https://lavits.org/wp-content/uploads/2018/04/32-Vasilis-Ververis -Olga-Khrustaleva-e-Eliana-Quiroz.pdf.

Villena, D. (2020): "Bloqueo de páginas webs y aplicaciones", *Hiperderecho* (12/03/2020). Disponible en: https://hiperderecho.org/2020/03/bloqueo-de-paginas-webs-y-aplicaciones/.

Zittrain, J. (2008): *The Future of the Internet— And How to Stop It*, New Haven, Yale University Press, 2008.

4. Participación cívica y relaciones con la Administración pública en el marco de su innovación tecnológica

Carlos Affonso Souza
Janaina Costa[*]

1. Introducción

La mitología de varias culturas precolombinas deposita la creación de la humanidad en la figura de un dios furtivo que, en particular, enseña las técnicas de siembra y las reglas de convivencia en sociedad. Los dioses Quetzalcóatl, Pachacamac y Sumé —cada uno a su manera y en los más diversos panteones— repiten un ciclo que incluye la transmisión de enseñanzas y una posterior desaparición. Sumé, dios de los pueblos tupi, dejó su huella antes de partir.

Las huellas sirven para indicar que alguien pasó por allí, pero también sirven para indicar caminos. En muchos países, la construcción de políticas públicas sobre derechos digitales se ha realizado en las últimas décadas a través de mecanismos de participación cívica. Al participar en un proceso colaborativo para construir una política pública, los ciudadanos terminan dejando su marca en la iniciativa, como una huella. Por otro lado, varias huellas encontradas por los que vienen a continuación permiten comprender el camino seguido para alcanzar el resultado.

---

[*] Carlos Affonso Souza es el director del Instituto de Tecnología y Sociedad de Río de Janeiro (ITS Rio). Profesor de Derecho de la Universidad del Estado de Río de Janeiro (UERJ). Miembro afiliado al Proyecto Sociedad de la Información de la Facultad de Derecho de Yale. Es miembro del Comité Ejecutivo de la Red Global de Centros de Investigación de Internet y Sociedad, que abarca más de 100 centros de investigación, y trabaja actualmente en proyectos sobre IA e Inclusión y Ética de la Digitalización. Janaina Costa es investigadora senior del Instituto de Tecnología y Sociedad de Río de Janeiro. Licenciada en Derecho, es Máster por el Institut d'Étude du Développement Économique et Social (IEDES) de la Sorbona.

Es en este sentido que es necesario comprender cómo los modelos de participación cívica producen más y mejores conocimientos sobre posibles soluciones a problemas complejos que enfrenta la comunidad. A la hora de regular los derechos digitales, o incluso enfatizar cómo se da la relación del ciudadano con la Administración pública, la opción de caminar desde un proceso abierto y colaborativo ha demostrado ser una opción rica, pero con peculiaridades y desafíos que es necesario conocer para que puedan ser superados.

En este capítulo, revisamos el surgimiento de declaraciones de derechos en varios países en las últimas décadas, con énfasis en la experiencia sudamericana encontrada en Brasil y Perú. Nos preguntamos por el motivo que justifica la creación de estas cartas, enfatizando el modelo colaborativo de su producción.

En este contexto, intentaremos subrayar cómo una carta de derechos digital no estaría completa si no aborda la forma en que los ciudadanos se relacionan con la Administración pública y cómo esta debe hacer uso de las modernas tecnologías para garantizar una mayor eficiencia y confianza en la ejecución de sus actos. Por último, analizando diferentes experiencias de creación de estas cartas, esbozaremos algunas lecciones de mejores prácticas que se pueden replicar para futuras iniciativas.

2. ¿Por qué y cómo regular sobre derechos digitales?

Una cuestión previa y fundamental que se podría plantear al abordar iniciativas de participación cívica en la regulación de derechos digitales es la necesidad de una ley (o de instrumento jurídico) que articule los principios relacionados con la protección de los derechos fundamentales en línea. En un panorama en constante cambio de desarrollo tecnológico cada vez más rápido, ¿es el enfoque legal la mejor manera de proteger los derechos y libertades que se disfrutan en internet?

Allá por 1996, la conocida "Declaración de Independencia del Ciberespacio", de John Perry Barlow, trazó una línea entre los Estados como "gigantes cansados de carne y acero" y el ciberespacio como "el nuevo hogar de la Mente". Al señalar las virtudes que se derivan de la existencia de un espacio virtual para el libre flujo de información, Barlow instó a los Estados a no interferir en el desarrollo de la red mediante regulaciones de ningún tipo.

La regulación se presenta en muchas formas diferentes y, ciertamente, una ley impuesta por el Estado no es la única forma en que los comportamientos pueden estimularse o restringirse. Lawrence Lessig, en 1999, sugirió que este

tira y afloja regulatorio podría ser más complejo cuando se trata de abordar cómo la tecnología afecta el comportamiento humano. Las normas jurídicas no serían la única fuente de regulación, sino que en realidad disputarían espacio con fuerzas en competencia como el mercado y su lógica económica, las constricciones sociales y, finalmente, la propia tecnología, que podría permitir o prohibir un comportamiento por medio de su arquitectura.

El escenario trazado por Lessig revela que un cambio en la arquitectura podría ser más efectivo que un cambio en la legislación a la hora de configurar las relaciones y el comportamiento humano. "El código es la ley" se convirtió así en un mantra repetido en los debates sobre el futuro de la regulación de internet. La codificación puede ser una forma más confiable de lograr los objetivos de una regulación determinada que pasar por el proceso formalista, y generalmente opaco, de la elaboración de leyes. Pero no es que los propios algoritmos puedan ser menos opacos.

Por tanto, ¿cómo asegurar que la libertad que se disfruta precisamente por el desarrollo de internet no se vea erosionada por los resultados del tira y afloja regulatorio? Aquí es donde entra el debate sobre la creación de un instrumento jurídico basado en los derechos humanos.

Un conjunto completamente nuevo de reglas legales no es la mejor respuesta cada vez que aparece una nueva tecnología. La mayoría de las veces, el deseo de aprobar una ley que aborde un tema muy específico (por muy popular que parezca) conducirá rápidamente a una ley obsoleta. Tan pronto como cambie la tecnología, la misma ley tendrá poca aplicación o incluso podría restringir el marco para la innovación. En consecuencia, la regulación que aborda los cambios tecnológicos debe seguir un enfoque basado en principios para evitar la obsolescencia inminente. Por eso mismo, muchas iniciativas de participación cívica para la construcción de normas sobre derechos digitales no se traducen en la aprobación de una ley formal, sino en una carta rectora de principios, que puede servir de guía para la actuación de jueces, legisladores y autoridades ante el tema.

En todo caso, cualquiera que sea la modalidad que se elija, ley o carta de principios, los procesos de participación cívica en derechos digitales están recibiendo cada vez más atención en cuanto a su metodología de participación pública, la forma en que se presentan los aportes, además de las métricas para evaluar los resultados obtenidos.

Antes de detallar algunas experiencias sobre participación cívica en la construcción de normas sobre derechos digitales, vale la pena señalar algunas de estas piezas fundamentales para comprender qué es un proceso de participación cívica en línea y cómo se desarrolla.

3. ¿Qué es un proceso de participación cívica en línea?

Los procesos de participación cívica pueden darse de diferentes formas y con diferentes propósitos. Al abordar el uso de internet para posibilitar la participación cívica, algunas experiencias de construcción colaborativa de cartas digitales aparecen como ejemplos relevantes. En cierto modo, estos casos representan una aplicación de técnicas de participación cívica a la elaboración de un documento legal, ya sea una ley formal o una recomendación aprobada por el gobierno o por el Parlamento para orientar la actuación de las autoridades públicas y la ciudadanía en general.

Esta práctica, también denominada *crowdlaw*, hace uso de la tecnología para ampliar los medios por los cuales el Estado puede tener acceso al conocimiento de la comunidad sobre un tema determinado, facilitando la discusión entre especialistas e interesados, lo que redundaría en una mejor toma de decisiones sobre el contenido de los instrumentos jurídicos[1].

Los estudios sobre cómo la tecnología ha transformado la participación ciudadana en los procesos legislativos y la construcción de instrumentos jurídicos por parte de los poderes públicos aún está en pañales (Capone y Noveck, 2017: 63). Sin embargo, ya se pueden extraer algunas consideraciones generales de experiencias que buscan aprovechar el potencial colaborativo de internet y de las tecnologías modernas para asegurar una mayor participación, diversidad y transparencia en la formulación de soluciones regulatorias.

Algunas características esenciales definen un proceso de participación cívica en línea para la construcción de instrumentos jurídicos; entre ellas, podemos enumerar: i) el uso de la tecnología como herramienta para ampliar el acceso, la eficiencia y el compromiso en las prácticas participativas; ii) la necesidad de integrar la participación en las distintas fases del ciclo de las políticas públicas; iii) la inteligencia colectiva (manifestada en ideas, opiniones, acciones, datos y conocimientos) como mecanismo para mejorar la calidad de las decisiones; iv) valorar el *design* como una forma de delinear procedimientos que sean accesibles al público, útiles para las instituciones y sostenibles para todos los involucrados; v) fomentar la experimentación como forma de descubrir prácticas que funcionan, y vi) la necesidad de institucionalizar los procesos (Monteiro, 2021).

[1] Como explica Julia Iunes Monteiro, el *crowdlaw* "parte del análisis de experiencias concretas de participación digital realizadas en diferentes partes del mundo con el fin de comprender las estrategias y métodos que aseguran la sostenibilidad de las prácticas participativas digitales a lo largo del ciclo de las políticas públicas" (Monteiro, 2021: 138).

Un proceso de participación cívica en línea para la construcción de instrumentos jurídicos puede contener diferentes fases. El primero es la definición de la agenda, buscando identificar claramente los contornos del tema a abordar y el problema que se pretende tratar. Una vez definidos los alcances del proceso, las autoridades encargadas de su conducción pueden abrir una convocatoria pública de aportes o desarrollar una plataforma que permita a todos los interesados participar en la construcción de soluciones al problema.

La mayoría de las veces, esta es la fase que recibe más atención, ya que crea una oportunidad para que la comunidad interesada participe. No existe una fórmula única aplicable en esta etapa del proceso. Algunos procesos se realizan únicamente con la presentación de aportes formales por parte de los interesados a las autoridades respectivas. Estas contribuciones pueden o no hacerse públicas.

Después de analizar las contribuciones, la autoridad responsable producirá un borrador de un instrumento legal, que idealmente volvería a ser discutido por la comunidad. Es importante aquí entender cómo estas oportunidades para la participación ciudadana pueden ser más o menos complejas. El simple envío de aportes (por correo electrónico, por ejemplo) representa una forma de ampliar el universo de conocimientos que pueden ser relevantes para la toma de decisiones por parte de las autoridades. Sin embargo, no logra construir un verdadero ambiente para el intercambio de experiencias y conocimientos entre la comunidad interesada.

Por lo tanto, además de simplemente recibir (y eventualmente publicar) contribuciones estáticas de partes interesadas y expertos, los procesos de participación cívica en línea más ricos terminan desarrollándose a través de la construcción de una plataforma que permite la interacción entre los miembros de esa comunidad, ya sea comentando las presentaciones de otros o, más comúnmente, la propia redacción sugerida por la autoridad para el instrumento jurídico en cuestión. En estas modalidades, la redacción del instrumento legal —como un proyecto de ley o una declaración— está abierta para que la comunidad pueda sugerir cambios, como en una herramienta *wiki*. Como cada participante puede visualizar las sugerencias de otras personas, se crea un espacio para el intercambio de conocimientos, además de la identificación de convergencias y divergencias en la comunidad, lo que facilita una toma de decisiones más reflexiva por parte de la autoridad responsable.

Una vez finalizado el periodo de aportes, corresponde a la autoridad resumir el contenido recibido, realizar los cambios necesarios y regresar a la comunidad con el producto de la consulta, teniendo especial cuidado de enfatizar, siempre que sea posible, la razones por las cuales se aceptarán ciertas contri-

buciones y otras no. Esta retroalimentación a la comunidad es igualmente sensible y relevante, ya que asegura el estímulo para la participación continua.

Si se trata de una ley, es posible que el texto resultante de la consulta pública pase luego por el trámite legislativo del respectivo Parlamento. Si es un acto del poder ejecutivo, se procede a su aprobación y publicación.

En todo caso, vale la pena mencionar que la aprobación de un texto final no cierra el ciclo de un proceso de participación cívica en línea. El seguimiento de la evaluación de los efectos de la ley cobra cada vez más protagonismo, lo que hace que, con cierta periodicidad, las autoridades vuelvan a la comunidad para buscar medir con mayor precisión cómo se ha aplicado el instrumento legal, cuáles son sus repercusiones y qué modificaciones podrían ser realizadas para que logre sus objetivos.

4. Un mosaico de experiencias de participación cívica

La construcción de leyes o declaraciones sobre derechos digitales ha sido una oportunidad para experimentar formas innovadoras de participación ciudadana. En América Latina, Brasil fue pionero cuando en 2009 inició un proceso de consulta pública en línea para la creación de un proyecto de ley sobre derechos digitales. Más recientemente, Perú inició su proceso de consulta pública para la creación de una carta de derechos digitales.

Mientras tanto, fuera de la región, los países europeos también buscaron crear sus instrumentos legales sobre derechos digitales basados en diferentes modalidades de participación ciudadana. Comprender el contexto y las peculiaridades de estas experiencias será relevante para trazar un panorama de cómo diferentes gobiernos, en diferentes situaciones, buscaron aprovechar el potencial de la red para ampliar y diversificar el proceso de construcción de estos documentos.

4.1. La experiencia brasileña con el Marco Civil de Derechos para Internet

La Ley Federal n° 12.965/2014 es más conocida en Brasil como Marco Civil de Derechos para Internet (Marco Civil da Internet). Fue el resultado de la primera iniciativa a gran escala encabezada por el gobierno nacional para utilizar internet como una forma de ampliar y diversificar las voces en el proceso de elaboración de leyes. Al utilizar internet para radicalizar el componente democrático

del proceso legislativo, el Marco Civil brinda varias oportunidades para comprender mejor cómo se crea una ley, quiénes son las partes interesadas relevantes en su aprobación y cómo contribuyen a lo largo del proceso.

Al proporcionar una plataforma abierta para que todas las partes interesadas compartan sus puntos de vista y experiencias sobre los asuntos en discusión, el Marco Civil abrió un nuevo capítulo de transparencia en el proceso legislativo a nivel nacional. Es importante entender cómo surgió esta iniciativa y sus logros indiscutibles, pero también prestar atención a sus limitaciones.

4.1.1. El proceso de participación cívica en línea del Marco Civil

El Marco Civil es el resultado de una iniciativa que comenzó con una consulta pública en línea que se produjo entre 2009 y 2010. El proyecto de ley, resultado de la consulta, fue enviado al Congreso Nacional en 2011 y durante tres años más fue debatido ferozmente hasta su aprobación en 2014. El proyecto estuvo bajo el escrutinio de una amplia gama de actores, desde organizaciones de la sociedad civil hasta el sector privado, desde la comunidad técnica hasta otras entidades gubernamentales relevantes.

Debido a que era la primera vez que se realizaba un experimento de este tipo, reuniendo a una amplia gama de actores, muchas de las características de la iniciativa se desarrollaron a lo largo del camino. Desde el debate inicial en 2007 hasta la aprobación de la ley en 2014, el Marco Civil demostró ser un proceso muy educativo para todas las partes que participaron en la discusión y consolidó el camino para experiencias futuras —y mejoradas— en consultas en línea en Brasil.

La redacción del Marco Civil surgió como una fuerte reacción pública contra un proyecto de ley sobre ciberdelitos. El Proyecto de Ley nº 84/99 —originalmente presentado por el diputado Luiz Piauhylino— recibió una enmienda del senador Eduardo Azeredo que vinculó el nombre del senador al Proyecto de Ley de Delitos Cibernéticos. Así, a partir de 2007, el proyecto se denominó popularmente Ley Azeredo. El proyecto preveía crear sanciones de hasta cuatro años de prisión para quienes violaran los mecanismos de protección de los celulares (*jailbreaking*) o para quienes decidieran transferir canciones de un CD a otros dispositivos.

Con un espectro de sanciones tan amplio —estrechamente relacionado con las mismas discusiones que terminaron desembocando, más tarde, en el debate en Estados Unidos de los proyectos de la ley de Cese a la Piratería en Línea

(SOPA, por sus siglas en inglés) y a la de Protección a la Información Persona (PIPA)—, el Proyecto de Ley Azeredo convertía en delincuentes a millones de internautas en Brasil. Además, restringía las oportunidades de innovación, convirtiendo en delictivas las actividades de investigación y desarrollo que se necesitan regularmente.

En 2006 se generó una coalición muy amplia contra el Proyecto de Ley Azeredo. Uno de los primeros grupos en alzar la voz fue el sector académico, seguido de una fuerte movilización de la sociedad civil, que incluyó una petición en línea que en poco tiempo recibió 150.000 firmas. Los congresistas tomaron nota de la reacción y, gracias a esa movilización, iniciaron una discusión más amplia sobre la regulación de internet en el Poder Legislativo.

Las voces en contra del Proyecto Azeredo fueron muchas. Sin embargo, no hubo un consenso claro sobre qué alternativa debía presentarse. Si un proyecto de ley penal no era la mejor manera de regular internet, ¿cuál podría ser la alternativa? En mayo de 2007, un artículo de Ronaldo Lemos en el diario *Folha de São Paulo* presentó la propuesta de que, en lugar de acercarse al Derecho Penal, Brasil podría tener un marco regulatorio civil para internet, un Marco Civil. Esta fue la primera vez que se hizo público el concepto "Marco Civil da Internet".

El apoyo del Gobierno Federal a la noción de que un Marco Civil podría oponerse al Proyecto de Ley Azeredo se produjo en 2009. En el Foro Internacional de Software Libre de 2009 realizado en Porto Alegre, el presidente Luis Inácio Lula da Silva afirmó que Brasil no necesitaba una "ley penal para Internet" y que la mejor solución sería modificar el Código Civil para proteger los derechos digitales.

Aunque inicialmente se formuló como una "modificación del Código Civil", el mensaje presidencial fue claro: los derechos civiles deben priorizarse antes que un proyecto de ley sobre ciberdelincuencia. Tras ello, el Ministerio de Justicia invitó a un grupo de especialistas para crear un proceso abierto y de múltiples partes, con el fin de desarrollar un mecanismo para recopilar experiencias diversas sobre regulación de internet. Y estuvo claro desde el principio que esta regulación no se podía hacer sin usar internet en aras de mejorar el debate en torno a los temas relevantes.

Dado el potencial de internet para hacer converger diferentes puntos de vista, la plataforma en línea Cultura Digital —desarrollada en ese momento por el Ministerio de Cultura— se adaptó para recibir la primera consulta sobre un proyecto de ley que se implementaría en Brasil. Fue la primera experiencia del go-

bierno brasileño con el uso de plataformas en línea para mejorar el proceso de elaboración de leyes. Muchas de las lecciones aprendidas de esta iniciativa se implementaron luego en consultas posteriores. Se podría decir que esta primera consulta en línea fue casi artesanal. En 2009, había significativamente menos metodologías, *software*, conocimiento de buenas prácticas y experiencias previas orientadas el *crowdsourcing* de un proyecto de ley que en la actualidad.

El concepto inicial detrás de la consulta era que el futuro anteproyecto de ley contase con un grupo de especialistas lo más diverso posible. Para tal efecto, la consulta pública se dividió en dos fases. En la primera, que comenzó en octubre de 2009 y duró poco más de 45 días, todas y todos los interesados pudieron presentar sus aportes sobre temas predefinidos. Inicialmente, se proporcionó un pequeño conjunto de principios para que los participantes pudieran adherirse a ellos, sugerir otros diferentes o incluso proponer un nuevo enfoque a un principio ya sugerido.

También en 2009, el Comité Directivo de Internet de Brasil (CGI.br) aprobó sus Diez Principios para la Gobernanza y el Uso de Internet. Esta resolución contemplaba una serie de principios que acabaron sirviendo de inspiración al Marco Civil, como la protección de la "libertad, la privacidad y los derechos humanos", el fomento de una "gobernanza democrática y colaborativa" y la neutralidad de la red.

Durante esta primera fase, la consulta pública recibió más de 800 comentarios. El grupo de expertos y el personal de la Secretaría de Asuntos Legislativos del Ministerio de Justicia analizaron cada aporte e identificaron las principales tendencias que guiarían la redacción del proyecto de ley. Una vez el borrador estuvo listo, se inició una segunda fase de consulta con otros 45 días para que los participantes presentaran sus aportes. Dada la cantidad de solicitudes presentadas, además de las solicitudes de ampliación de plazo, esta segunda fase se extendió por una semana y finalizó el 30 de mayo de 2010.

La segunda fase de la consulta en línea proporcionó al público un borrador de texto que podía ser comentado artículo por artículo. Los participantes podían estar de acuerdo o no con la redacción propuesta o sugerir modificaciones. Todos los participantes podían ver los comentarios de los demás para que se estableciera una conversación real entre ellos.

En esta segunda fase hubo cerca de 1.200 comentarios al texto del anteproyecto de ley. Además de individuos, académicos/as y organizaciones de la sociedad civil, varias empresas de tecnología y medios también participaron en la consulta, aumentando la diversidad de partes involucradas en el proceso.

Dado que todos los comentarios se pusieron a disposición del público, ello arrojó una luz sin precedentes sobre las demandas de las partes interesadas con respecto a los cambios en el texto propuesto. De este modo, las opiniones, críticas y propuestas de modificación de la futura ley ya no se restringieron a piezas técnicas distribuidas directamente a las oficinas de los congresistas. Dichas contribuciones podían luego ser revisadas y comentadas por todas las partes, como en un foro de discusión en internet.

Dicho proceso, en todo caso, suscitaba algunos interrogantes. ¿Cómo asegurarse de que la comunidad interesada participase efectivamente en tal consulta? ¿Qué tipo de retroalimentación debía proporcionarse para que los participantes supieran que sus contribuciones iban a ser analizadas? ¿Cómo incentivar la participación continua en la plataforma y no solo en el momento en que se envía una contribución? ¿Cómo garantizar que se fuesen a escuchar diferentes voces durante la consulta? ¿Cómo presentar los resultados para incluir los aportes que fueran fundamentales para la elaboración del texto final?

Esos fueron los temas que motivaron una cuidadosa mirada por parte del equipo revisor reunido por el Ministerio de Justicia, no solo sobre el contenido de los aportes, sino también sobre la forma en que los diferentes actores terminan involucrándose en el proceso.

Una vez se llegó a un acuerdo sobre un texto final, se envió un proyecto de ley al Congreso Nacional en 2011. Luego vinieron tres años de proceso legislativo que desembocaron en la aprobación de la Ley nº 12965, en 2014. Simbólicamente, el presidente sancionó la ley en la ceremonia de apertura de la Conferencia NetMundial de 2014, que trajo a Brasil varias delegaciones internacionales para discutir el futuro de la gobernanza de internet. La ley entró en vigor el 23 de junio de 2014.

4.1.2. Administración pública e innovación en el Marco Civil

La actuación de la Administración pública recibió un capítulo dedicado en el Marco Civil. El artículo 24, I, de la ley establece que los lineamientos para la acción del Estado, en todos sus niveles, son el "establecimiento de mecanismos de gobernanza multiparticipativa, transparente, colaborativa y democrática, con la participación del gobierno, el sector empresarial, la sociedad civil y comunidad académica". Es importante señalar que este dispositivo incorpora el principio de multisectorialidad en la formulación de instrumentos de gobernanza en red.

El mismo artículo 24 determina que la acción del Estado debe guiarse por la interoperabilidad entre los servicios y sistemas gubernamentales "para permitir el intercambio de información y la celeridad de los trámites". Además, el Estado debe adoptar preferentemente tecnologías, estándares, y formatos abiertos y libres.

Reflejando un logro del movimiento por los datos abiertos de gobierno, el mismo artículo 24, VI, enumera como lineamiento para la acción del Estado la "publicidad y difusión de datos e información públicos, de manera abierta y estructurada". A este respecto, no solo llama la atención la mención de los datos abiertos, sino también la indicación de que deben estar disponibles de forma estructurada, facilitando así su comprensión (y probablemente reutilización, aunque no se expresó esta posibilidad).

El artículo 26 establece que el Estado debe promover iniciativas de formación "para el uso seguro, consciente y responsable de internet como herramienta para el ejercicio de la ciudadanía, la promoción de la cultura y el desarrollo tecnológico". Este dispositivo está directamente relacionado con los esfuerzos para reducir la brecha digital en el país, advirtiendo que acceder a internet no significa necesariamente saber utilizar sus recursos de manera segura y responsable. Esta misión por parte del poder público se vuelve aún más relevante cuando se advierte que Brasil aparece frecuentemente en la lista de países más vulnerables a los ataques de los ciberdelincuentes.

Otro objetivo de acción del Estado se encuentra en el artículo 27, II, cuando establece que las iniciativas públicas de promoción de la cultura digital y de internet como herramienta social deben "buscar la reducción de las desigualdades, especialmente entre las distintas regiones del país, en condiciones de acceso a las tecnologías de la información y la comunicación y su uso".

En resumen, el Marco Civil incluyó lineamientos para que la Administración pública fomentase diversos mecanismos que permitiesen una mayor participación ciudadana, tales como la interoperabilidad tecnológica (art. 24, III y IV; art. 25, I); la adopción de tecnologías, estándares y formatos abiertos y libres (art. 24, V y VI), además del deber de promover la inclusión digital de sus ciudadanos (art. 27, I), a través de la capacitación (art. 24, VIII y art. 26) y la accesibilidad a las aplicaciones de internet por parte de las entidades públicas (art. 24, X; art. 25, II, III y IV).

Estos son los principales aspectos que en Brasil orientan las relaciones de la Administración pública con la ciudadanía en lo referido a la gobernanza de internet y las nuevas tecnologías a partir del Marco Civil. Veremos a continuación

cómo el grado de participación ciudadana (e incluso su significado) en la construcción de los derechos digitales varía en otros marcos normativos.

4.2. Carta Peruana de Derechos Digitales

La Carta Peruana de Derechos Digitales es una iniciativa del gobierno para la elaboración de un documento oficial, no vinculante, que busca delinear la aplicación de los derechos humanos al entorno digital, así como orientar el desarrollo de políticas públicas relacionadas con la transformación digital desde Perú (SGTD, 2022). Según la presentación de la Presidencia del Consejo de Ministros (PCM, 2022):

> el contenido de la Carta consiste en un listado con los derechos nominados y propuestas para el desarrollo de los mismos, siempre desde la perspectiva de las obligaciones que tiene el Estado peruano en relación a su realización. En todos los casos, la redacción se basa en la Constitución y las leyes peruanas. Esto significa que la Carta no crea nuevos derechos u obligaciones para el sector público o privado. Por el contrario, reafirma la vigencia de la misma en los entornos digitales.

El proceso de elaboración de la Carta Peruana de Derechos Digitales se basa en un enfoque multisectorial, que significa que su contenido busca ser cocreado por personas y organizaciones de diferentes ámbitos del Estado, el sector privado, la academia y la sociedad civil. Para ello, de manera similar a lo observado en la elaboración del Marco Civil brasileño, el proceso se dividió en dos etapas. La primera se llevó a cabo a través de un proceso de consulta a especialistas en diversos temas relacionados con los derechos humanos y las tecnologías digitales, realizado entre mayo y julio de 2022 (PCM, 2022).

Durante esta primera etapa, la Secretaría de Gobierno y Transformación Digital convocó a más de 39 participantes y lideró 18 mesas temáticas en las que se discutieron diferentes propuestas para la Carta Peruana de Derechos Digitales. La consulta pública recibió aportes de 21 organizaciones de la sociedad civil, el sector privado, la comunidad técnica y otras entidades gubernamentales relevantes (PCM, 2022).

La segunda etapa de la consulta pública en línea, realizada entre julio y octubre de 2022 a través de la plataforma de participación electrónica Participa Perú, brindó a la ciudadanía la propuesta de Carta de Derechos Digital, así como

una presentación de su proceso de creación, contexto y objetivos. En esta etapa, la ciudadanía pudo enviar sus comentarios y sugerencias sobre el documento de trabajo de la Carta Peruana de Derechos Digitales, así como sobre su proceso de cocreación (PCM, 2022). Las contribuciones recibidas tendrían el poder de influir en la redacción de un documento final para diciembre de 2022.

La Carta pretende plasmar los derechos ya establecidos por el ordenamiento jurídico peruano de tal forma que los ampare frente a las tecnologías digitales. En este sentido, el contenido de la Carta consiste en un listado de derechos y propuestas para su desarrollo, siempre desde la perspectiva de las obligaciones del Estado hacia su realización. La Carta contiene 25 derechos, divididos en seis categorías. En el documento de trabajo algunos incluyen comentarios sobre la pertinencia de su inclusión y la redacción de su contenido. Algunos derechos, a fecha de cierre de este texto (diciembre de 2022), no tienen todavía propuestas de contenido. En estos casos, además de comentarios sobre su relevancia, también se buscan ideas para dotarlos de contenido.

En relación con la Administración pública, la Carta reserva una categoría dedicada a los derechos en este ámbito. Sin embargo, solo dos de los cuatro artículos incluidos en esta categoría presentan una propuesta de redacción, de modo que, además de comentarios sobre su pertinencia, aún se buscan ideas para desarrollar el contenido de estos derechos. En la categoría de derechos relacionados con la Administración pública se enumeran artículos en asuntos como "salud digital" (art. 20) y "educación digital" (art. 21). La cuestión de la justicia digital está tratada en el artículo 22. De acuerdo con dicho dispositivo, el Estado promoverá la adopción de tecnologías digitales en el desarrollo de las actividades del poder judicial, centrándose en mejorar el acceso y la calidad de estos servicios, manteniendo siempre a la persona en el centro de atención de cualquier reforma que se realice sobre la materia.

Es interesante que la Carta peruana traiga un artículo específico sobre el funcionamiento del poder judicial, ya que las transformaciones producidas por la digitalización tienden a modificar sustancialmente las prácticas notariales de este poder, al mismo tiempo que la petición y la realización de otras diligencias procesales. Los actos a través de internet también pueden facilitar el acceso a la justicia. La mención a la protección de la persona como "el centro de toda reforma" también parece tener en cuenta que la adopción de herramientas tecnológicas debe mejorar la protección de los derechos, y no restringirlos en nombre de la posible practicidad en la realización de actos procesales.

Por lo demás, de acuerdo con el artículo 23, el Estado promoverá la creación de canales digitales de atención, procurando que su funcionamiento mejore la calidad de las relaciones entre la ciudadanía y las entidades del sector público. Según este artículo, dicha medida se implementa para que los nuevos canales no representen nuevas formas de discriminación, "especialmente la que se produce por motivos económicos, sociales, de idioma y de datos de cualquier otra naturaleza". Sin abandonar el tema de la exclusión digital, el texto explicativo del artículo menciona que el Estado promoverá que "siempre existan formas en que las personas puedan relacionarse de manera no digital con las entidades del sector público, cuando el desarrollo social y tecnológico ha logrado un mayor grado de transformación digital" (PCM, 2022: 34).

La Carta Peruana alude en otras ocasiones al papel del Estado en el fomento de la participación cívica como elemento apremiante para el cumplimento de los derechos digitales a los que se dedica el documento. En este sentido, afirma que la participación política a través de medios digitales debe promoverse por el Estado bajo las mismas garantías y observando los mismos requisitos que en los canales tradicionales. En el mismo sentido, propugna que el Estado facilite el derecho de acceso a la información por medios digitales (art. 7 bajo el título Derechos que se ejercen en ambientes o por medios digitales) (PCM, 2022: 18).

Cabe señalar, además, que la Carta se preocupa en varios momentos de resaltar el deber del Estado de promover el acceso de las poblaciones particularmente vulnerables a los derechos enumerados (arts. 1, 8 y 12). Sin embargo, la Carta solo menciona la gobernanza de múltiples partes interesadas con respecto al derecho a la libertad de expresión e información (art. 6):

> La libertad de expresión y la libertad de información se ejercen en entornos digitales a través de la palabra hablada, la palabra escrita o la imagen, por cualquier medio de comunicación social, incluido Internet. El Estado promueve las condiciones para el ejercicio efectivo de la libertad de expresión e información en los entornos digitales, incluyendo algunas de estas: el acceso universal, el pluralismo, la igualdad y no discriminación, la neutralidad de las redes y la gobernanza digital con enfoque multiactor.

Por último, en la Carta peruana se señala el rol central del Estado en la promoción del acceso al disfrute de los beneficios del progreso científico y sus aplicaciones como afirmación de los derechos económicos, sociales y culturales. En este sentido, no profundiza en mecanismos de participación ciudadana, ni el

Estado se compromete a compartir la gobernanza del espacio digital y los derechos conexos.

4.3. Carta de Derechos Digitales de España

La Carta de Derechos Digitales lanzada en España propone un marco, sin carácter normativo, para que las autoridades públicas naveguen en el entorno digital existente "aprovechando y desarrollando todas sus potencialidades y oportunidades y conjurando sus riesgos" (MAETD, 2021). De acuerdo con las consideraciones previas que introducen la iniciativa, el objetivo de la Carta es descriptivo, prospectivo y prescriptivo. Descriptivo de los contextos y escenarios digitales determinantes de conflictos, inesperados a veces, entre los derechos, valores y bienes de siempre, pero que exigen nueva ponderación; esa descripción ayuda a visualizar y tomar conciencia del impacto y las consecuencias de los entornos y espacios digitales. Prospectivo al anticipar futuros escenarios que pueden ya predecirse. Prescriptivo en el sentido de revalidar y legitimar los principios, técnicas y políticas que, desde la cultura misma de los derechos fundamentales, deberían aplicarse en los entornos y espacios digitales presentes y futuros (SEDIA, 2021: 3).

Es importante señalar que, antes de la publicación de esta Carta, en España ya existían leyes que contemplaban diferentes derechos digitales. Así, el propósito del documento es asegurar los mismos derechos existentes en el mundo físico para el ámbito digital, además de establecer nuevos derechos debido a las especificidades del entorno relacionados con los derechos digitales. En otras palabras, la Carta refuerza los derechos de la ciudadanía, genera certidumbre en la nueva realidad digital y aumenta la confianza ante los cambios y disrupciones tecnológicas al reconocer los novísimos retos de aplicación e interpretación que la adaptación de los derechos al entorno digital plantea, así como al sugerir principios y políticas referidos a ellos en el citado contexto.

El Gobierno de España impulsó la elaboración de la Carta de Derechos Digitales dentro del plan España Digital 2025. La Agenda España Digital 2025 planteaba como una de sus 10 metas estratégicas la redacción de una Carta de Derechos Digitales como marco de referencia para garantizar los derechos de ciudadanos y empresas en la nueva realidad digital (eje estratégico 10, medida 45).

La elaboración de la Carta de Derechos Digitales siguió un proceso participativo en dos pasos, con contribuciones de especialistas en la materia y las asociaciones de defensa de derechos, así como de la ciudadanía, junto con la

contribución del sector privado, proveedores de servicios, y sector público competencialmente afectado. La Carta comenzó a elaborarse en junio de 2020, con la participación del Grupo de Expertos constituido por la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA) del Ministerio de Asuntos Económicos y Transformación Digital paralelamente a una consulta abierta en la que pudieran participar todos los ciudadanos, y cuyo resultado serviría también como contribución al trabajo de este grupo. La primera versión de la Carta quedó entonces abierta a consulta pública hasta el 20 de enero de 2021 y, tras definirse su redacción final, fue publicada y adoptada por el Gobierno de España el 14 de julio de 2021.

La etapa abierta a consulta entregó al público un documento introductorio y consideraciones previas que enmarcan y presentan la iniciativa, así como el documento Carta de Derechos objeto de consulta. En esta segunda etapa, se recibieron alrededor de 200 aportes al texto preliminar. Para participar en la consulta abierta, los interesados debían enviar sus aportaciones a la dirección de correo electrónico disponible en la página web del gobierno, donde también se podía encontrar una traducción no oficial de la carta, comentarios preliminares y un enlace a los aportes recibidos (MAETD, 2020). Una amplia gama de partes interesadas participó en la consulta: individuos, académicos/as y organizaciones de la sociedad civil, y varias empresas de tecnología y medios.

La Carta tiene un título dedicado a los derechos de participación y de conformación del espacio público en el que se observa la opción de establecer activamente ámbitos de participación ciudadana que se extiendan a sus relaciones con la Administración pública en el terreno de su innovación tecnológica (GE, 2021).

En el apartado dedicado al derecho a la participación ciudadana a través de los medios digitales (XVI), la Carta recomienda fomentar la participación de las personas en la vida pública a través de la promoción de entornos digitales que contribuyan al derecho al acceso efectivo a la información pública, la transparencia, la rendición de cuentas, así como a la proposición e implicación de las personas en la actuación de las Administraciones públicas en sus respectivos ámbitos de actuación (art. 1). Asimismo, asegura que los procedimientos de participación ciudadana garantizarán la igualdad de condiciones sin discriminación ni exclusión de las personas (art. 2). Por su parte, la parte dedicada a los derechos digitales de la ciudadanía en sus relaciones con las Administraciones públicas reconoce que el derecho a la igualdad de las personas se extiende al acceso a los servicios públicos y en las relaciones digitales con las Administra-

ciones públicas, las cuales deben promover políticas públicas activas para lograr este fin (art. 1). Igualmente, busca promover estándares tecnológicos que permitan la interoperabilidad, no discriminación y medios multicanal de acceso a los servicios de la Administración (arts. 2, 3 y 4).

Es interesante notar que, en el capítulo dedicado a los derechos en entornos digitales, la redacción de la Carta se modificó significativamente después de la consulta pública. El texto puesto a consulta establecía que solo el poder público era responsable de evaluar, y eventualmente revisar, las normas relativas a los derechos digitales en el país: "Los poderes públicos evaluarán las leyes administrativas y procesales vigentes a fin de examinar su adecuación al entorno digital y propondrán en su caso la realización de reformas oportunas en garantía de los derechos digitales" (SEDIA, 2021). La nueva redacción, en cambio, aunque no menciona expresamente la participación de la sociedad en este proceso, abre esta posibilidad al determinar que: "se promoverá la evaluación de las leyes administrativas y procesales vigentes a fin de examinar su adecuación al entorno digital y la propuesta en su caso de reformas oportunas en garantía de los derechos digitales" (GE, 2021).

4.4. La Carta Portuguesa de Derechos Humanos en la Era Digital

La Carta Portuguesa de Derechos Humanos en la Era Digital, lanzada oficialmente en mayo de 2021, regula en sus 23 artículos los derechos relacionados con el acceso, uso y seguridad en el entorno digital. El proyecto apareció por primera vez en el Parlamento en 2019, a través del Proyecto de Ley 1217/XIII/4 - Carta de los Derechos Fundamentales en la Era Digital, iniciativa que eventualmente vencería con el final de la legislatura (PORT1).

En la legislatura siguiente, en julio de 2020, volvió a la discusión en el Parlamento portugués un proyecto de ley de los mismos autores: el Proyecto de Ley 473/XIV - Carta de los Derechos Fundamentales en la Era Digital (PORT2), que fue acompañado, en una iniciativa similar, por el Proyecto de Ley 498/ XIV/1 - Carta de Derechos Digitales (PORT3). Estos dos proyectos de ley finalmente se unieron y se trabajaron juntos para dar lugar a la versión que fue aprobada.

La participación de entidades de la sociedad civil, la industria y el gobierno se limitó a aportes durante el proceso legislativo, en audiencias públicas como la promovida por la Comisión de Asuntos Constitucionales, Derechos, Libertades y Garantías, de la Asamblea de la República sobre la materia (ARTV, 2021). Veinte opiniones de partes interesadas relevantes —incluidos organismos re-

presentativos de organizaciones de medios, la industria editorial, consumidores, abogados, así como organismos públicos con funciones de supervisión sobre los tribunales, los medios y los datos personales— se presentaron al comité parlamentario correspondiente.

Después de su promulgación, la Carta recibió críticas, puesto que su proceso de redacción se consideró demasiado acelerado y no proporcionó espacio para una amplia participación y discusión pública. Según Eduardo Santos, presidente de Associação D3, de defensa de los derechos digitales:

> Para lograr un documento impactante y realmente bien hecho, se necesitaba más. Hubiera sido necesario invertir más en el documento incluso antes de su ingreso a la Asamblea de la República, por ejemplo entregando su elaboración a académicos/investigadores del área, sin perjuicio de las formas de recibir aportes de los interesados. Pero eso hubiese sido incompatible con el ritmo de la política nacional. Tendría que haber seguido el ritmo de la academia y la participación y discusión pública, necesariamente más lento. Los titulares y la buena cobertura de prensa hubiesen tenido que esperar, pero entonces Portugal ya no podía presentarse como "pionero", ya que los españoles tienen un proceso legislativo idéntico en curso y también querían ser pioneros. [...] Recordemos el Marco Civil da Internet, de 2014. Un documento ineludible e histórico del ordenamiento jurídico brasileño, una especie de Constitución Brasileña de Internet, que ciertamente inspiró nuestra Carta. Incluso antes de ser un proyecto de ley, el borrador fue ampliamente debatido y con participación pública. Desde la idea original hasta la aprobación pasaron siete años, cinco de los cuales estaban en trámite legislativo (Santos, 2021).

El contenido de la Carta también fue objeto de críticas a las pocas semanas de su publicación. Estas se vertieron sobre diversos asuntos: alegaciones hacia disposiciones normativas redundantes, críticas hacia el controvertido artículo 6 —que, al establecer el derecho a la protección contra la desinformación, ha sido leído como un salvoconducto para que el Estado institucionalice la censura—, o hacia su propia forma de aprobación, presentándose como un instrumento jurídico que, pese a su vocación de establecer derechos fundamentales, se adopta como acto legislativo ordinario y no como acto legislativo constitucional.

Pasando al análisis de su contenido, el artículo 19 tiene por objeto regular los derechos digitales frente a la Administración pública, reconociendo que toda persona tiene derecho a:

> i) beneficiarse de la transición a los procedimientos administrativos digitales; ii) obtener información digital sobre trámites y actos administrativos y comunicarse con los tomadores de decisiones; iii) asistencia personal en el caso de trámites exclusivamente digitales; iv) que los datos proporcionados a un servicio sean compartidos con otro, en los casos legalmente previstos; v) beneficiarse de regímenes de "datos abiertos" que permitan el acceso a los datos contenidos en las aplicaciones informáticas de servicio público y permitan su reutilización, en los términos legalmente previstos; y vi) uso gratuito de una plataforma digital única europea para el acceso a la información, de conformidad con el Reglamento (UE) 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018.

Sumado a esto, la Carta también aboga por el deber del Estado de promover la inclusión y accesibilidad digital (art. 3, 2, c). Pero no prevé derechos ni mecanismos de participación en la construcción de derechos digitales.

Por último, el Estado aparece como garante de los derechos digitales (art. 3; art. 11 y art. 12), promotor de prácticas de accesibilidad (art. 14, 2,) y única autoridad competente para definir políticas públicas que garanticen la protección de los ciudadanos, y redes y sistemas de información (art. 15).

5. Líneas generales sobre el papel de la Administración pública

Como se ha revisado, una parte significativa de las cartas sobre derechos digitales dedican algunos de sus artículos a la actuación de la Administración pública, enfatizando cómo esta debe hacer uso de los recursos tecnológicos para lograr que su relación con la sociedad se produzca de manera cada vez más incluyente, transparente y eficiente. En cierto modo, el mismo proceso de construcción de estas cartas ya es una iniciativa que busca alcanzar estos importantes objetivos.

Hay algunos puntos en común entre los diferentes documentos analizados que vale la pena destacar en lo que se refiere al desempeño de la Administración pública. El primero es el reconocimiento de la accesibilidad como piedra angular para entender la relación entre la ciudadanía y la Administración pública, asegurando que toda ella pueda acceder a los servicios públicos prestados a través de medios digitales. En este sentido, algunas cartas mencionan el deber del Estado de asistir a quienes no saben o no pueden utilizar estas herramientas.

La Carta peruana, en su artículo 23, menciona que el Estado debe brindar alternativas no digitales a quienes, por diversas razones, no puedan relacionarse

con la Administración por estos medios. Por su parte, la Carta española menciona que el Estado debe brindar alternativas "en el mundo físico".

Un segundo asunto muy presente en las declaraciones de derechos digitales es la necesidad de interoperabilidad entre los sistemas y servicios puestos a disposición digitalmente por la Administración pública. Este comando es especialmente importante en un momento en que se está popularizando internet móvil, que tiende a priorizar el acceso a los servicios a través de aplicaciones. Para el administrador, lanzar una aplicación por medio de la cual los ciudadanos accedan a un servicio público puede parecer una acción ágil y moderna, pero vale la pena señalar que una posible profusión de aplicaciones —que no siempre se comunican entre sí— puede terminar siendo, más que una solución, un problema para el ciudadano.

La divulgación de datos abiertos de gobierno también es, en tercer lugar, un elemento presente en varias cartas. Vale la pena destacar cómo los 10 años que separan la redacción del Marco Civil presentada al Congreso Nacional en Brasil y la aprobación de la Carta portuguesa revelan una maduración del tema. El documento brasileño afirma la necesidad de publicar datos gubernamentales en formato abierto y de forma estructurada. De alguna manera, al detallar que la divulgación debe ser "de forma estructurada", se puede entender que la finalidad de la norma brasileña es permitir que esos datos sean entendidos por terceros y potencialmente reutilizados.

Sin embargo, la mención expresa de la posibilidad de reutilizar estos datos solo aparece en el documento portugués, 10 años después. Mientras tanto, se ha avanzado mucho en el debate sobre el uso de datos públicos para la creación de una serie de aplicaciones innovadoras, que pueden surgir tanto dentro de la Administración como en *startups* u organizaciones del tercer sector que se dedican a analizar y generar inteligencia de los datos del gobierno. Estas aplicaciones pueden complementar los usos gubernamentales de los datos públicos, creando nuevas soluciones a problemas complejos.

En cuarto lugar, la adopción preferencial de tecnologías y estándares abiertos también aparece en algunos documentos. La cuestión es importante porque apunta no solo a garantizar un mayor acceso a los documentos, servicios y actividades, en general, que realiza la Administración, sino también a evitar que los gobiernos se conviertan en usuarios cautivos de una solución de *software* cerrada, cuyas opciones de soporte están restringidas o que pueden incluso comprometer cuestiones de seguridad (dependiendo de la fiabilidad de la solución contratada).

Por lo demás, cabe destacar cómo la apuesta por la regulación y gobernanza de redes de carácter multisectorial y participativo no siempre se expresa en las cartas sobre derechos digitales. Además de Brasil, un país europeo que encarnó este mandato en su declaración sobre los derechos de internet fue Italia. En cuanto a la gobernanza y regulación de la red en su conjunto, la Declaración italiana establece en su artículo 14 que "Internet requiere reglas coherentes con su dimensión universal y supranacional, destinadas a implementar plenamente los principios y derechos definidos anteriormente, a garantizar su naturaleza abierta y democrática, para prevenir cualquier forma de discriminación y evitar que las normas que la rigen dependan del poder que ejercen los actores de mayor poder económico".

En definitiva, se puede apreciar que el rol de la Administración ocupa un lugar importante en el diseño de las cartas de derechos digitales, buscando que la misma tecnología que se utilizó para la consulta que dio lugar a la construcción de las cartas de derechos también pueda ser utilizada por la Administración en sus relaciones con la ciudadanía, acercando el Estado a la sociedad y aprovechando las facilidades que aporta la comunicación digital.

6. Lecciones de participación ciudadana

Las cartas digitales que se han analizado en este texto no solo tienen contenidos diferentes, que reflejan las peculiaridades de cada ordenamiento jurídico, sino que sus procesos de construcción también guardan elementos singulares, vinculados a la forma, tiempo y contexto de cada país en el que se desarrollaron las iniciativas. Aun así, en la suma de las experiencias es posible esbozar algunas lecciones aprendidas en el camino.

El primero se refiere precisamente al papel fundamental que desempeñan los gobiernos en la realización de procesos de participación ciudadana para la elaboración de cartas sobre derechos digitales. Por regla general, corresponde a los gobiernos organizar la iniciativa, definir sus fases, cronograma y objetivos a alcanzar. En este sentido, la centralidad del papel que tiene el Estado puede ser un facilitador del proceso o una trampa, dependiendo de la actuación de las autoridades involucradas. Este aspecto negativo se presenta especialmente cuando condiciones propias del gobierno impactan en el curso del proceso de participación, tales como demoras o intentos de conducir los debates hacia resultados que parecen más favorables al Estado.

Una segunda lección que se deduce de los procesos de participación cívica es la importancia de contar con una plataforma que permita no solo el envío de aportes, sino también la interacción entre las partes interesadas, de modo que se expongan con mayor claridad las diferentes opiniones, lo que incluso facilita el trabajo de los líderes, de la iniciativa en el mapeo del debate, sus actores y los puntos de convergencia y divergencia.

Una tercera lección a extraer de las experiencias discutidas es la importancia de diseñar estas plataformas para informar mejor el debate, ofreciendo recursos (como materiales de referencia y otros contenidos), visualizaciones y otros instrumentos que no solo pueden armar a las partes interesadas, sino también estimular la discusión sobre los temas propuestos. Existen diferentes diseños de plataformas y modalidades de participación. Así, junto al diseño, cabe subrayar el papel que desempeñan los monitores o agentes encargados de comisariar los recursos y moderar los excesos que puedan producirse en los debates.

Una cuarta lección está directamente relacionada con el resultado de los debates sobre los temas propuestos. Una vez enviados los aportes y finalizado el periodo de discusiones en la plataforma, comienza la tarea de los responsables de la consulta de recopilar las manifestaciones, ordenar los argumentos y decidir cuáles generarán efectivamente una transformación, por ejemplo, en el texto del instrumento legal presentado. Es importante que los responsables puedan devolver a la comunidad algún tipo de respuesta sobre los aportes realizados. Por supuesto, no todas las contribuciones pueden ser respondidas de manera efectiva, aclarando las razones de su incorporación al texto final o no, pero en general es importante que se haga este retorno a la comunidad de interesados, incluso como una forma de alentar a estos actores para seguir participando de futuros procesos colaborativos.

Una quinta lección se refiere a la celebración, siempre que sea posible, de reuniones presenciales, como conferencias, reuniones o audiencias, que pueden tener lugar en paralelo con la discusión en línea. La participación ciudadana en línea es muy rica y crea posibilidades de acceso a debates que no habrían existido sin internet. Al mismo tiempo, las reuniones presenciales generan una forma diferente de participación y permiten a las autoridades sensibilizar a ciertas comunidades (a menudo directamente impactadas por el proceso) sobre la relevancia del tema en cuestión.

Finalmente, una sexta lección extraída de las experiencias analizadas es el papel que tiene un comité de especialistas en el proceso de participación ciudadana. Si, por un lado, la formación de estos grupos puede facilitar la comprensión del estado del arte de algunos debates, es importante abrir la conversación a una

comunidad técnica más amplia, que permita visualizar, por ejemplo, las divergencias que puedan existir dentro de la propia academia o en otros sectores interesados en la iniciativa.

7. Conclusión

Las cartas de derechos digitales analizadas en este capítulo cumplen una doble función. Por un lado, revelan cómo los mecanismos de participación cívica son fundamentales para garantizar la inclusión, la diversidad y la transparencia en la forma en que el Estado organiza procesos de construcción colaborativa sobre cuestiones de mayor relevancia. Por otro, al centrarse en las relaciones entre la ciudadanía y la Administración pública, estos mismos documentos revelan un plano, un verdadero camino que debe seguir la Administración para garantizar que las promesas de las tecnologías digitales se hagan realidad.

Estas cartas —tengan fuerza de ley o se limiten a orientar a los ciudadanos y a las autoridades públicas— son necesarias para preservar los derechos fundamentales y garantizar que la tecnología sirva como instrumento para potenciar el desarrollo de la personalidad, la mejora de las condiciones económicas y sociales, y no al contrario.

La adopción de tecnologías digitales avanza a un ritmo acelerado en América Latina. Es necesario que más países —inspirados en las experiencias destacadas aquí— desarrollen iniciativas para construir cartas sobre derechos digitales, tanto como una forma de mejorar la protección de los derechos de sus ciudadanos en un contexto cada vez más digital, como para detallar su integración en las Administraciones públicas de cara a su relación con la ciudadanía. El público buscará enfrentar los desafíos que traen estas tecnologías. Cada actor que participa en estas iniciativas realiza un aporte con lo que sabe. Esta huella, como se ha dicho, también tiene una doble función. Señala interés y contribución sobre un asunto determinado, pero también un camino a seguir para aquellos que llevan adelante la discusión.

Referencias bibliográficas

Arnaudo, D. y Radu, R. (2017): "Transatlantic Perspectives on the Internet Bill of Rights", *Brazil's Internet Bill of Rights: A Closer Look*, Rio de Janeiro, Instituto de

Tecnologia e Sociedade, pp. 119-132. Disponible en: https://itsrio.org/pt/publicacoes/marco-civil-da-internet-visoes-para-o-publico-internacional/.

Capone, G. y Noveck, B. S. (2017): *Crowdlaw. Online Public Participation in Lawmaking,* Nueva York, The Governance Lab at New York University.

Gobierno de España (2021): "Carta Derechos Digitales". Disponible en: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf.

Ministerio de Asuntos Económicos y Transformación Digital (2020): "Consulta pública para la elaboración de una Carta de Derechos Digitales". Disponible en: https://portal.mineco.gob.es/es-es/ministerio/participacionpublica/audienciapublica/Paginas/SEDIA_Carta_Derechos_Digitales.aspx.

— (2021): "El Gobierno adopta la Carta de Derechos Digitales para articular un marco de referencia que garantice los derechos de la ciudadanía en la nueva realidad digital" (13/07/2021). Disponible en: https://portal.mineco.gob.es/es-es/comunicacion/Paginas/210714_np_Carta-.aspx.

Monteiro, J. I. (2021): *CrowdLaw: abrindo as portas do governo para a participação digital*, Rio de Janeiro, Lumen Juris.

Plataforma de Web TV da Assembleia da República (2021): "Audição conjunta sobre direitos fundamentais na era digital" (04/03/2021). Disponible en: https://canal.parlamento.pt/?cid=5193&title=audicao-conjunta-sobre-direitos-fundamentais-na-era-digital.

PORT1 (2019): Projeto de Lei 1217/XIII/4. Disponible en: https://www. parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=43768.

PORT2 (2020): Projeto de Lei 473/XIV/1. Disponible en: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=45116.

PORT3 (2020): Projeto de Lei 498/XIV/1. Disponible en: https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=45218.

Presidencia del Consejo de Ministros (2022a): "Carta Peruana de Derechos Digitales" (27/07/2022). Disponible en: https://www.gob.pe/institucion/pcm/informes-publicaciones/3302991-carta-peruana-de-derechos-digitales.

— (2022b): "Proceso de cocreación de Carta de Derechos Digitales". Disponible en: https://facilita.gob.pe/t/2438.

Santos, E. (2021): A Carta Portuguesa de Direitos Humanos na Era Digital, Sapo, 16 de junio. Disponible en: https://tek.sapo.pt/opiniao/artigos/opiniao-a-carta-portuguesa-de-direitos-humanos-na-era-digital.

Secretaría de Estado de Digitalización e IA (2021): "Introducción Carta de Derechos Digitales". Disponible en: https://portal.mineco.gob.es/RecursosAr-

ticulo/mineco/ministerio/participacion_publica/audiencia/ficheros/SEDIAIntroduccionCartaDerechosDigitales.pdf.

Secretaría de Gobierno y Transformación Digital (2022): "Participar en la Carta Peruana de Derechos Digitales" (26/07/2022). Disponible en: https://www.gob.pe/22543.

5. La brecha digital en América Latina como barrera para el ejercicio pleno de derechos

Renata Ávila[*]

1. Introducción

En el año 2023 la brecha digital va más allá del hecho de tener o no acceso a internet. Esta brecha ya no se puede limitar a reflejar únicamente el porcentaje de personas con acceso potencial o real a la red. La esfera digital y, por tanto, las brechas que esta abre, trascienden a las tecnologías de la información y la comunicación, y se extienden al ejercicio de los derechos civiles y políticos, al acceso a la educación, la libre locomoción, el comercio, la salud, el trabajo digno o la cultura, por mencionar algunos ámbitos.

El despliegue reciente de herramientas digitales ubicuas, que en determinados entornos monitorean y controlan espacios públicos, e incluso participan en procesos de toma de decisiones, plantea necesariamente cambios en la definición de la brecha digital. Ya no se puede hablar de una situación en donde estar excluido del uso y aprovechamiento de las tecnologías sea el único indicador de desigualdad, sino que hay que analizar los efectos que el despliegue de tecnologías digitales no opcionales tiene sobre individuos y colectivos.

[*] CEO de Open Knowledge Foundation, entidad dedicada a reducir las barreras al acceso al conocimiento y los datos. Está afiliada al Stanford Institute of Human-Centered Artificial Intelligence (HAI) en California, y asociada al Centro de Internet y Sociedad del Centro Nacional para la Investigación Científica (CNRS) en París. Cofundó la <A+> Alianza por los Algoritmos Inclusivos, y forma parte del Comité Asesor de Creative Commons, del Directorio de Fiduciarios de Digital Future Society y del Directorio de Open Future.

Existen situaciones en las que el uso de ciertas tecnologías a personas o grupos específicos genera condiciones de desigualdad y exclusión en el ejercicio y goce de ciertos derechos. Esto se plasma, por ejemplo, cuando se produce una mediación automatizada en sistemas de inclusión social basados en datos que pueden estar sesgados, al condicionar la recepción de ayudas a estar registrado en un sistema, o en la obligación que a veces se impone a población adulta mayor de relacionarse con el Estado, o con el sector privado, por medios digitales, por razones pragmáticas, sin suministrar condiciones habilitantes que la ayuden a superar las barreras de acceso a equipos y su empleabilidad.

El incremento de estas brechas puede estar ofuscado por los avances en la digitalización de ciertos países, y con la apariencia que suscita de eficiencia y de impacto en la calidad de vida de las personas. Pero el desarrollo tecnológico debe estar acompañado de un marco jurídico y de políticas públicas que hagan posible el ejercicio pleno de derechos de toda la población. La tecnología en sí misma no lo garantiza en todas las ocasiones y, de hecho, puede conllevar en determinadas ocasiones situaciones de precariedad y erosión de derechos, acrecentando las desigualdades incluso en países desarrollados, aquellos que producen su propia tecnología con capacidad para adaptarla funcionalmente a sus sistemas sociales y culturales.

En el caso de Latinoamérica, los riesgos se agudizan, en virtud de un contexto de desigualdades múltiples. En la actualidad, el continente sufre los efectos de una extrema concentración de riqueza en manos del 10% de su población; y en ocasiones ciertas élites condicionan los mecanismos de inversión, paralizando el aumento de la carga tributaria necesario para desplegar políticas públicas y programas que puedan reducir las brechas digitales y, en consecuencia, la apertura de alternativas para quienes ven el ejercicio de sus derechos bloqueado por la falta de acceso, de habilidades o de capacidades para acceder a la tecnología.

Otra dimensión que genera brechas digitales en la región latinoamericana, con consecuencias sobre el ejercicio de derechos, radica en que a menudo se depende de los gigantes tecnológicos para impulsar la digitalización en el sector público, social o en ámbitos de interés público general. Latinoamérica es un continente que importa la mayoría de la tecnología que consume, pero la mayoría de países carece de una legislación robusta en materia de protección a los consumidores y de defensa de los derechos de la ciudadanía ante posibles situaciones de abuso de sus proveedores. En la región, además, las grandes corporaciones tecnológicas suelen contar con protecciones adicionales, amparadas en distintos acuerdos comerciales, principalmente con Estados Unidos y China.

Lo anterior se evidencia a menudo en el plano de las contrataciones del Estado: la activación de políticas públicas para reducir brechas digitales puede desembocar en la firma de grandes contratos que favorecen a los monopolios tecnológicos de los países desarrollados, sin que se establezcan condiciones de flexibilidad que permitan la adaptación tecnológica a las necesidades locales, auditorías de código en los sistemas, traducción a idiomas originarios, etc.

Ninguna legislación en los países latinoamericanos ha abordado hasta ahora de forma adecuada el control de la responsabilidad y rendición de cuentas de las compañías tecnológicas por los efectos que sus posibles sesgos pueden generar en la población, como tampoco hay reglas adecuadas para las contrataciones y compras directas de los Estados. Es más, la rápida digitalización de ciertos sectores, como el educativo, ha llevado en ocasiones a su privatización de *facto* y a nuevas dependencias tecnológicas que afectan a la seguridad, soberanía e independencia de ciertos países, hasta el punto de dejar en una situación de vulnerabilidad a sus infraestructuras digitales críticas, totalmente privatizadas y controladas desde el exterior.

Por lo demás, existe otra gran brecha digital regional referida a la poca inversión en innovación y capacidades, y a las carencias en las agendas latinoamericanas de investigación y desarrollo (I+D), que afecta a la generación y aprovechamiento de los datos públicos. La pobreza regional de datos se erige como una barrera a superar por parte de los países latinoamericanos para, por ejemplo, participar como actores y no receptores del futuro de la inteligencia artificial (IA).

Este capítulo discute el problema de las múltiples desigualdades digitales en la región, revisando el marco general de sus ordenamientos jurídicos y examinando las políticas públicas nacionales y locales, en su mayoría enfocadas a la conectividad, que se han elaborado e implementado en varios países. Asimismo, se plantea la necesidad de impulsar una agenda positiva para reducir la brecha digital en todas sus dimensiones, además de la de la conectividad, proponiendo reflexiones desde una perspectiva de derechos interdisciplinarios.

En este sentido, habría de definirse una agenda en el plano de cada Estado y en el regional, que abra un proceso de inversión y coordinación continental, para elevar el grado de prosperidad, inclusión, democracia, cultura, conocimiento e investigación, interacción con el servicio público, y buenas prácticas regulatorias. Las estrategias de integración regional, a su vez, deberían idealmente enlazar con políticas de cooperación internacional, para incidir de manera concertada en una agenda de desarrollo sostenible en la que, en lugar de brechas, se logren sociedades más digitales pero también más justas e inclusivas.

2. Una brecha digital más allá del acceso: abrir las posibilidades económicas del futuro

La Unión Internacional de Telecomunicaciones (UIT) define la brecha digital como la distribución desigual de la tecnología, el acceso a la información y las redes de comunicación entre diferentes regiones, comunidades e individuos. A efectos de este capítulo, la brecha digital también se refiere a la distribución desigual de las posibilidades de las sociedades de participar de los beneficios de la datificación y de la economía de plataformas digitales.

Ya en la cuarta década de la web, y casi medio siglo después de la aparición de internet, las brechas de conectividad todavía impiden a una enorme parte del planeta acceder a las oportunidades que la esfera digital ofrece: únicamente el 19% de la población de los países menos desarrollados está conectado a internet (ITU, 2022). La brecha es más notoria respecto a tecnologías punta como el 5G, cuyo acceso permitiría saltos cuantitativos y cualitativos de aprovechamiento y productividad pública y privada en distintos sectores e industrias. Así, por ejemplo, solo el 5% de la población de África y el 10% de la de América Latina están conectados a tecnologías de quinta generación (ITU, 2022). Mientras tanto, la gran mayoría, especialmente las poblaciones rurales, están desconectadas, o conectadas a redes lentas e insuficientes. La instalación de tecnologías de quinta generación afecta notablemente a la provisión de servicios y a la competitividad de sectores productivos enteros, de modo que no poder acceder a ellas multiplica las desigualdades económicas. La inaccesibilidad impide desarrollar servicios y transacciones que se median por distintos aparatos, plataformas y sistemas públicos, privados y sociales, que además a menudo trascienden fronteras.

En consecuencia, la brecha digital supone para sus afectados no poder participar en condiciones equitativas en la nueva economía y detener el avance de la calidad de vida de millones de personas de países y regiones enteras. Por ello, la brecha que se abre ya no se limita a la conectividad: se extiende a una brecha de acceso a datos y aplicaciones, que se agudiza con la llegada de los teléfonos inteligentes y el *hardware* que requieren, y se exacerba con la aparición de la economía de plataformas, creando diferencias que ya no son individuales, sino colectivas y nacionales. Así, por ejemplo, el este de Asia y Estados Unidos concentran el 90% de las aplicaciones, mientras que África y Latinoamérica apenas alcanzan el 1% (OMC, 2022). Ante esta situación, si no se producen cambios incentivados por normativas internacionales, regiones enteras acapararán para sí los beneficios de la datificación, consumando en el futuro una concentración sin precedentes sobre el control de los datos. Se ha argumentado

que este posible "colonialismo de datos" podría allanar el camino para una nueva etapa del capitalismo, definida como el resultado de la apropiación y el comercio de la experiencia humana "datificada" (Couldry y Mejías, 2019).

Los países más pobres del mundo, e incluso los países de ingreso medio, se convertirían entonces en exportadores de datos, sin obtener beneficios económicos para desarrollar sus propias industrias. Asimismo, la conectividad de su ciudadanía a las plataformas de las dos regiones que dominan el sector se convertiría en un subsidio para sus competidores, y castigaría cualquier intento de adopción normativa orientada a la localización de datos (Weber, 2017). El control casi absoluto de la materia prima digital (los datos) para las tecnologías del futuro plantea, pues, importantes retos encaminados a redefinir las leyes antimonopolio y el derecho de la competencia (Shi-Yin, 2022).

Ciertamente, en la literatura sobre brecha digital en Latinoamérica, las y los especialistas se centran en la dimensión del acceso y su interrelación con los derechos humanos, y en los desarrollos legislativos que pretenden establecer el acceso a internet como un derecho humano. Sin embargo, tomando en consideración la brecha derivada del terreno de las aplicaciones y plataformas, consideramos que —para proteger efectivamente los derechos individuales y colectivos— es preciso rebasar el marco de protección de los derechos humanos, y apuntar hacia mecanismos efectivos que detengan la creciente desigualdad digital. Así, la senda para revertir la brecha digital, y lograr resultados con un impacto real y duradero, pasa por acudir a distintas disciplinas del derecho, que deben tomarse como un sistema interdependiente. Se trata de combinar estrategias legislativas, ejecutivas y de litigio jurídico (Ávila, 2018; Couldry, 2022), que incluso trasciendan las fronteras nacionales, tal y como se explicará más adelante. Otro aspecto relevante en este ámbito es la necesidad de formación en habilidades digitales para la región, una cuestión esencial para mejorar la brecha digital y permitir una mayor participación en la economía digital.

3. Consideraciones jurídicas sobre el alcance y contenido del derecho al acceso a internet

La esfera digital, tal y como reza la Declaración para una Internet Justa es:

> Un sitio para el intercambio global de conocimiento e información, un espacio para la libre expresión y asociación, un medio para la deliberación y la partici-

> pación democrática, un canal para la entrega de servicios sociales y públicos esenciales, y un andamio para nuevos modelos de actividad económica y todas las personas tienen el derecho a la habilitación digital básica, que comprende el derecho a: acceder a Internet, a su contenido y sus aplicaciones; participar en el desarrollo de contenidos y aplicaciones; y recibir la formación y capacitación necesarias para un uso efectivo de Internet y otras herramientas digitales (Just Net Coalition, 2014).

Latinoamérica fue una región pionera en el desarrollo de los derechos humanos en la era digital, tanto a través de su legislación como en su jurisprudencia. Costa Rica fue el primer país de la región —y uno de los primeros del mundo, en paralelo a Finlandia y España— en declarar el acceso a internet como un derecho humano, según la Ley de Acceso a la Información Pública y Protección de Datos Personales nº 8968, de julio de 2011. Esta ley reconoce el acceso a la información pública, incluido internet, y la protección de datos personales, como un derecho fundamental.

Casi simultáneamente, el informe presentado en mayo de 2011 por Frank La Rue en calidad de Relator Especial de las Naciones Unidas para la Libertad de Opinión y Expresión, definió el acceso a internet como un derecho humano (OACNUDH, 2011). Según La Rue, dicho acceso es esencial para el ejercicio pleno de los derechos humanos, incluida la libertad de expresión, el derecho a la información, el derecho a la participación política, el derecho a la privacidad y el derecho a la educación. En su informe, argumentó que los Estados tienen la responsabilidad de garantizar el acceso a internet a todas las personas, especialmente a aquellas en situación de vulnerabilidad, y de proteger este derecho de restricciones e interferencias. El informe fue firmado y adoptado por la Relatoría Especial de Libertad de Expresión de la Organización de Estados Americanos, ese mismo año.

Posteriormente, México declaró el acceso a internet como un derecho humano y lo plasmó en su Constitución en 2013, a lo que siguió la aprobación del Marco Civil de Internet en Brasil, en 2014. En Colombia, por citar un último ejemplo, la Ley nº 1753 de 2015 reconoció el derecho al acceso a internet como un derecho humano y estableció medidas para garantizarlo a través de programas y proyectos gubernamentales.

Esta dimensión jurídica y de protección inspiró más adelante en distintos países de la región programas de reducción de la brecha digital centrados en suministrar conectividad a áreas rurales, dotar de capacidades y habilidades básicas digitales a la sociedad por medio del sistema educativo, otorgar subsidios para que

internet sea asequible y crear fondos especialmente enfocados en poblaciones rurales y tradicionalmente excluidas (Affordability Report, 2021) como una reacción y una solución a las poblaciones no cubiertas por el mercado —tras la liberación del mercado de las comunicaciones que siguió al Acuerdo General sobre el Comercio de Servicios (AGCS) de la Organización Mundial del Comercio (OMC)—.

3.1. Brecha digital y pueblos indígenas: el derecho a consulta previa

Enlazando con el acceso en zonas rurales, cabe recordar que la brecha digital es un problema que afecta de forma desproporcionada a los pueblos indígenas de América Latina. Muchos de estos grupos viven en áreas remotas, con acceso limitado o nulo a tecnologías y servicios digitales, lo que les impide participar en la economía digital. Además, los pueblos indígenas también enfrentan barreras culturales y lingüísticas que les impiden utilizar plenamente las tecnologías digitales.

Para afrontar este asunto, debe tenerse en cuenta que la mayoría de los países de la región son signatarios del Convenio sobre Pueblos Tribales de la Organización Internacional del Trabajo (OIT 169), que obliga a los Estados a realizar consultas con las comunidades indígenas sobre cualquier decisión y política pública que les afecte. Junto a ella, las declaraciones de las Naciones Unidas y de la Organización de los Estados Americanos (OEA) sobre los Derechos de los Pueblos Indígenas contienen exhortaciones similares. Estos instrumentos crean obligaciones directas de consulta previa en cuestión de planes para la reducción de la brecha digital, permitiendo que los pueblos indígenas puedan aportar ideas, visiones, conceptos y prácticas más inclusivos. Su participación podría aprovechar las lecciones de, por ejemplo, la iniciativa Maori Data Sovereignty de Nueva Zelanda, o de las estrategias de la Agenda Digital de Bolivia para desarrollar *software* a nivel local. Se trata de contar con las comunidades indígenas en las decisiones que se adopten sobre soberanía digital, que además corrijan las desigualdades estructurales que estas sufren, aborden las injusticias históricas y allanen el camino para un futuro más sostenible.

3.2. Medidas de acceso en contextos de desigualdades socioeconómicas

Como se ha indicado, todos los países de la región cuentan con alguna política pública, legislación o entidad dedicada a la reducción de las brechas digitales, ante todo en su dimensión de acceso a internet. Existen subsidios, fondos y programas, como el Plan Ceibal en Uruguay, que resolvió barreras de conectividad, de habilidades y capacidades, y de acceso a equipos, en uno de los casos más exitosos de la región.

A los esfuerzos legislativos, también se han sumado alianzas público-privadas en las que grandes compañías tecnológicas han participado en proyectos para ofrecer conectividad de forma gratuita, así como equipos y aun plataformas específicas para proveer servicios en distintos países, en una labor filantrópica de la que también han obtenido ganancias. Así, gigantes tecnológicos y de las comunicaciones han invertido, junto con el sector público, en iniciativas de reducción de brechas, como el programa Internet para Todos en Perú (2019), proporcionando ordenadores con *software* de Microsoft e instalación obligatoria de Google Classroom en el sistema educativo público en El Salvador (2022), o el programa Semillas para el Futuro (2022) de desarrollo de habilidades y capacidades, de Huawei.

Sin embargo, incluso en los casos más exitosos de reducción de brechas, los beneficios sociales de la digitalización no se han terminado de concretar y la brecha tampoco se ha reducido de forma significativa. Según datos de la CEPAL (2022), la mitad de los jóvenes de 13 a 25 años de la región no están conectados, ni un cuarto de los adultos mayores de 65 años, a pesar de décadas de declaraciones e inversiones millonarias.

A tenor de lo dicho, ceñirse jurídicamente a establecer el derecho al acceso a internet como un derecho humano resulta insuficiente (Moyn, 2018), y no resuelve el reto de transformar un modelo económico que está amplificando las brechas, más allá de las divisiones Norte-Sur. De ahí la relevancia de entender, como se adelantó anteriormente, la otra cara de la brecha digital, yendo más allá de la conectividad y apuntando al reto de revertir la desigualdad creciente entre aquellos sectores y actores que controlan las infraestructuras digitales y los simples usuarios. En un momento en el que las plataformas están definiendo el modelo dominante de la digitalización, es necesario reflexionar como sociedad y valorar qué acciones y estrategias transversales deben implementarse desde distintas ramas del derecho público. En este sentido, es importante subrayar que el derecho a la competencia y contra los monopolios, y las normativas de protección de los consumidores y usuarios, pueden combinarse para lograr una reducción, no solo de la brecha de acceso, sino de las brechas derivadas del modelo en ciernes de una economía digital que hoy se concentra en unos pocos actores y países.

Esta ruta es la que está siguiendo la Unión Europea (UE), más modestamente, la Federal Trade Commission en Estados Unidos, y ciertas autoridades antimonopolios de China. Por su parte, todavía no existe en ningún país latinoamericano un sistema legislativo robusto y una estrategia política para plantear acciones que desconcentren el poder de las grandes tecnológicas transnacionales y reduzcan la enorme brecha que las separa de las empresas locales. No obstante, algunos mo-

vimientos de base están explorando políticas y dinámicas que apuntan hacia una senda de soberanía o autonomía tecnológica, orientadas a reducir las asimetrías entre los países que controlan las infraestructuras y plataformas y los que no.

Estos esfuerzos buscan nuevas formas de generar equidad en el terreno de la gestión de datos, y parten de la idea de que las personas, las empresas y la sociedad en general, deben poder entender el ecosistema tecnológico que las rodea y ser capaces de delinear su acción y dirección. Ello supone dotar a la ciudadanía de habilidades y capacidades para definir la relevancia y el valor de los datos que les importan, tener acceso y posibilidades de uso y aprovechamiento de los mismos, y determinar cómo se emplean los datos públicos. Estas cuestiones son cruciales para reducir las nuevas brechas digitales que se están produciendo y determinarán la capacidad de países y regiones, como la latinoamericana, para desarrollar un modelo propio de economía digital, inclusiva y sostenible, en lugar de limitarse a ser tanto receptores de tecnología como de normativas. La Tabla 1 refleja las dimensiones y áreas jurídicas a las que es preciso acudir para afrontar dichas brechas.

Tabla 1. Dimensiones y disciplinas jurídicas que atraviesan la brecha digital

<table>
<tr><th>Brecha digital y conectividad a la red</th><th>Brecha digital y desigualdades en las plataformas</th></tr>
<tr><td colspan="2">Acceso a internet como derecho humano

Derecho Universal de los Derechos Humanos (incluidos derechos civiles y políticos, y derechos económicos, sociales y culturales)</td></tr>
<tr><td>Acceso a internet como un derecho constitucional

Derecho Constitucional</td><td>Acceso equitativo a las plataformas como parte del ejercicio de la libertad económica y libre competencia

Derechos de la competencia, y de protección de consumidores y usuarios</td></tr>
<tr><td>Derecho a la consulta previa e informada de pueblos indígenas sobre las medidas legislativas o administrativas que afecten directamente sus derechos colectivos, su existencia física, identidad cultural y su calidad de vida o desarrollo

Derecho de los Pueblos Indígenas</td><td>Acceso equitativo a los datos como parte del derecho al desarrollo y a una vida digna

Derecho Comercial Internacional</td></tr>
<tr><td colspan="2">Derecho a la autodeterminación de los pueblos, soberanía e integración regional

Derecho Internacional Público</td></tr>
</table>

Fuente: Benkler (2006), Shi-Yin (2022), Ortiz Freuler (2021) y elaboración propia.

4. Agendas por compatibilizar: brecha digital, tratados comerciales internacionales y disputas geopolíticas

La investigación sobre derechos digitales en Latinoamérica se ha dedicado ampliamente a estudiar programas y políticas públicas sobre conectividad como el vehículo principal para alcanzar los Objetivos de Desarrollo Sostenible (ODS) en reducción de brecha digital. Sin embargo, estos estudios no han abordado en profundidad el impacto que la liberación del comercio internacional ha supuesto sobre las brechas digitales, y cómo los compromisos internacionales a los que están sujetos los países muchas veces frenan abruptamente políticas públicas destinadas a equilibrar las relaciones de poder entre los grandes conglomerados internacionales y los países de la región.

Una buena ilustración de este fenómeno lo representó en 2017 el caso de Brasil ante la OMC. El gobierno de Brasil activó un programa para financiar sus proyectos de inclusión digital por medio de impuestos a las importaciones digitales de grandes empresas de tecnología, pero la OMC falló en su contra, por considerar que creaba ventajas competitivas injustas (Shi-Yin, 2022). El caso reflejó el alcance real de los tratados comerciales internacionales ante las pretensiones de reducir la brecha digital y el contraste entre una visión utópica del futuro que a menudo promueven multinacionales y gobiernos —en el que la tecnología será un impulsor de saltos exponenciales que reducirán la pobreza—, y una realidad en la que los tratados internacionales, no solo han protegido, sino que han facilitado el mantenimiento del dominio de las grandes tecnológicas. De hecho, no hay datos concluyentes que vinculen el efecto directo del comercio electrónico con una reducción significativa de brechas digitales. Así las cosas, en las actuales circunstancias, regular el futuro digital se está convirtiendo en un juego de dominio geopolítico, con menos de 10 empresas de EE.UU. y China controlando toda la infraestructura digital esencial.

Desde la resistencia, la UE propone como contrapeso a tal concentración de poder un marco regulatorio voluntarioso, pero muchas veces poco realista a efectos de implementación en los países en desarrollo. Por lo demás, fuera de este club de tres actores, muy pocos países (Israel, Corea del Sur y Japón) o regiones, tienen capacidades reales de alcanzar los ODS de acceso a internet[1], preservando su autonomía tecnológica y, a su vez, respetando las obligaciones adquiridas en el marco de tratados internacionales. El resto de los países del mundo —en particular, las

[1] Aunque los ODS se proponen la meta del acceso universal y asequible a internet para 2030, la Web Foundation (2019) ha demostrado que, en las circunstancias actuales, habrá que esperar a 2042.

economías en desarrollo—, no pueden a menudo defender los derechos de sus ciudadanos en las negociaciones comerciales relativas al libre flujo transfronterizo de datos, lo que merma aún más su posición frente a los países que controlan el *hardware*, el *software*, los contenidos y la conectividad.

En gran medida, la transformación digital en América Latina se da en un contexto normativo y comercial rígido, que limita las posibilidades de un diseño realmente inclusivo y favorecedor para la innovación. El marco jurídico internacional configura un sistema anacrónico, y a la vez sobreproteccionista, de patentes y secretos comerciales e industriales que, en América Latina, restringe la capacidad de los sectores público y privado a adaptar y adecuar legalmente las tecnologías que recibe a sus contextos, culturas y lenguajes. Igualmente, impide la apertura de espacios de experimentación que puedan proteger su modelo económico de la influencia de los gigantes tecnológicos derivada de los tratados comerciales bilaterales o regionales. De hecho, las cláusulas de estos tratados, como los suscritos por Chile con Singapur y Nueva Zelanda (Acuerdo de Asociación de Economía Digital, DEPA, por sus siglas en inglés), o por México con Canadá y Estados Unidos (USMCA, por sus siglas en inglés), cierran aún más las puertas a dichos países a determinar libremente su futuro tecnológico y optar por una transición digital alternativa. Por otra parte, las obligaciones normativas que desprenden los tratados comerciales también limitan en la región las posibilidades de auditar y revisar el cumplimiento estricto de estándares nacionales e internacionales de derechos humanos, por parte de tecnologías y sistemas que afectan el ejercicio de otros derechos de las personas.

En suma, a falta de un tratado global que regule las relaciones comerciales digitales, dichos tratados bilaterales o regionales interfieren en leyes y políticas públicas nacionales orientadas a regular su esfera digital y a reducir brechas. Como se ha indicado, hay dos casos representativos de este fenómeno, que afectan a Chile y México.

El DEPA entre Chile, Nueva Zelanda y Singapur es un acuerdo comercial de vanguardia que apunta directamente a establecer un marco para la economía digital. El tratado se compone de diferentes módulos, que podrían expandirse de manera flexible a medida que evolucione la asociación. Entre sus aspectos positivos, se encuentran sus referencias a los instrumentos de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) y otras normas internacionales. No obstante, el acuerdo prohíbe los requisitos de localización y es débil con respecto a la protección de datos. Sus provisiones de ciberseguridad son poco realistas en tiempos de alta interconexión, especialmente con las posibilidades de la tecnología 5G.

El USMCA, que reemplazó al Tratado de Libre Comercio de América del Norte (TLCAN) en julio de 2020, libera totalmente las transferencias fronterizas de datos y las de datos personales. También excluye la posibilidad de que los Estados miembros exijan a los países la localización de datos, con la excepción normativa especial de la localización de datos de servicios financieros, que podría utilizarse como último recurso (condicionado a la colaboración con la entidad financiera y las autoridades reguladoras). El acuerdo también preserva consistentemente las demandas del Gobierno de Estados Unidos de no requerir transferencia o acceso al código fuente, y desarrolla un marco sofisticado de estándares sobre ciberseguridad, con un enfoque excesivamente flexible y referencias ambiguas a las mejores prácticas (Melzer, 2021).

En una estrategia de divide y vencerás, se restringe así el margen normativo de dos de las economías digitales más potentes de la región (Chile y México), limitando las posibilidades de uniformar el espacio digital latinoamericano para que este desarrolle un modelo alternativo que reduzca tanto las brechas de desconexión como las brechas de competitividad, y propiciando la consolidación del modelo actual, en el que "el ganador se lo lleva todo": datos, contratos de infraestructura, contratos públicos de provisión de *software* y *hardware*, y exclusividad en formación de habilidades y capacidades basadas en sus herramientas.

Ante esta situación, para reducir realmente las brechas digitales sería necesario compatibilizar cartas y declaraciones de derechos, que eleven el acceso a internet y otros derechos digitales a lo más alto de la escala de protección de los derechos fundamentales; activar políticas de desarrollo fundamentadas en agendas de cooperación internacional y alianzas público-privadas efectivas para servir a los menos favorecidos; e impulsar medidas comerciales que contrapesen las limitaciones de los países menos desarrollados, para adaptar sus normas y políticas a una transición digital opuesta al "extractivismo de datos" que, en consecuencia, se adecue a las demandas de sus comunidades lingüísticas, étnicas y culturales, además de a sus necesidades económicas. Además, debe prestarse atención a políticas de formación de habilidades para el nuevo entorno digital para todos, con el objetivo de no dejar a nadie atrás.

5. Conclusión: hacia una agenda positiva para reducir la brecha digital

Según indica la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2022), la tecnología debe utilizarse para unir a las personas, no para dividirlas. La transformación digital debería, pues, contribuir a construir una sociedad y una economía digital pero también equitativa, justa e inclusiva.

Sin embargo, Latinoamérica se encuentra hoy en una situación ambigua con respecto a la dirección a seguir para su transformación digital: por un lado, está en una situación rezagada en términos de competitividad, sin una sola empresa que ofrezca servicios digitales a escala global, y con la mayoría de su población trabajando, bien como mano de obra barata para tareas menores y poco cualificadas en las grandes plataformas; bien en minería de datos, proveyendo materiales para construir grandes conglomerados digitales en otra parte, fuera de la región. Además, carece de poder de negociación de cara a los acuerdos comerciales o de seguridad internacional, todo lo cual genera una creciente desigualdad digital, que es también socioeconómica, a lo que se agrega una fragmentación entre distintos intereses, muchas veces encontrados; de modo que parece que la región navega sin brújula o coordinación en el proceso de transformación digital.

No obstante, por otro lado, existen factores que podrían jugar a favor de la región latinoamericana y que favorecerían la posibilidad de articular una agenda coordinada para reducir las brechas digitales en un sentido amplio, a partir del relanzamiento de los espacios de integración subregional y regional, como la Comunidad de Estados Latinoamericanos y Caribeños (CELAC), Mercosur o UNASUR. A ello se suma una población joven y cada vez mejor formada, recursos minerales y energéticos, riquezas naturales, culturales y lingüísticas, y una relativa ausencia de conflictos armados internos o de guerras entre países.

Como indica Lovink (2022), otra esfera digital es posible y quizá la opción —en lugar de correr tras un tren cuyo destino no conocemos y que va más rápido que nuestras instituciones— sea emprender un camino distinto, construido con una lógica diferente, basada en otro modelo económico y social, que permita efectivamente incluir, conectar, producir y transformar, por medio de tecnologías. Después de todo, el código puede ser reescrito, podemos construir nuevos sistemas operativos, los cables y señales satelitales pueden cambiar de ruta, los centros de datos pueden descentralizarse y aún se pueden crear nuevas infraestructuras, modelos de gobernanza, y normas y regulaciones desde la solidaridad y la cooperación regional.

Referencias bibliográficas

ACNUR (2011): Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue, A/HRC/17/27, 16 de mayo, Naciones Unidas.

Alliance for Affordable Internet (2021): Affordability Report, Londres, Web Foundation. Disponible en: https://a4ai.org/research/affordability-report/affordability-report-2021/.

Ávila Pinto, R. (2018): "¿Soberanía digital o colonialismo digital?", *Sur,* nº 27. Disponible en: https://sur.conectas.org/es/soberania-digital-o-colonialismo-digital/.

— (2021): *Shaping the Future of Multilateralism Towards a "digital new deal" for Latin America: Regional unity for a stronger recovery*, Heinrich-Boll Stiftung.

Benkler, Y. (2006): *The wealth of networks: How social production transforms markets and freedom*, New Haven, Yale University Press.

Boletín Oficial de la República Argentina (2020): Decreto 690/2020. DECNU-2020-690-APN-PTE-Ley n° 27.078, 21/08/2020.

CEPAL (2022): *Un camino digital para el desarrollo sostenible de América Latina y el Caribe* (LC/CMSI.8/3), Santiago, Naciones Unidas.

Chu, Y. C. (2020): *Inroads into the Global Cyberspace: The Visions and Prospects of China's Digital Silk Road*, Stanford Digital Repository. Disponible en: https://purl.stanford.edu/zs515dy4419.

Congreso de Colombia (2015): Ley 1753 de 2015. Disponible en: https://www.mintrabajo.gov.co/Normatividad_Trabajo/Ley%201753%20de%202015.pdf.

Constitución Política de los Estados Unidos Mexicanos (s.f.): Disponible en: https://www.senado.gob.mx/constitucion/constitucion.html.

Couldry, N. (2022): "La colonización de los datos desde una perspectiva histórica", *Anuario Internacional CIDOB*, Barcelona, pp. 18-28.

Couldry, N. y Mejías, U. A. (2022): *The Costs Of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism*, Bloomsbury.

Halldenius, L. (2020): "Not Enough: Human Rights in an Unequal World", *Global Intellectual History*, 5: 4, pp. 385-389. Doi:10.1080/23801883.2019. 1603836.

Hurel, L. M. y Couldry, N. (2022): "Colonizing the Home as Data-Source: Investigating the Language of Amazon Skills and Google Actions", *International Journal of Communication* (en línea), 16, 5184.

ITU (2022): *Global Connectivity Report 2022*. Disponible en: https://www.itu.int/itud/reports/statistics/global-connectivity-report-2022/.

Johnson, P. A. y Scassa, T. (2023): "Who owns the map? Data sovereignty and government spatial data collection, use, and dissemination", *Transactions in GIS*, 00, pp. 1-15. Doi: https://doi.org/10.1111/tgis.13024.

Just Net Coalition (2014): Declaración de Delhi por una Internet Justa y Equitativa, Coalición por una Internet Justa y Equitativa. Disponible en: https://justnetcoalition.org/delhi-declaration_es.

Lee, N. T. (2022): *Digitally Invisible: How the Internet Is Creating the New Underclass*, Brookings Institution Press.

Lovink, G. (2022): *Stuck on the Platform*: *Reclaiming the Internet*, Valiz.

Meltzer, J. (2019): "The United States-Mexico-Canada Agreement: Developing Trade Policy for Digital Trade", *Trade, Law and Development* 11, nº 2 (invierno), pp. 239-268.

Moyn, S. (2018): *Not enough: Human rights in an unequal world*, Harvard University Press.

OMC (2014): Brasil. Caso Brasil - Impuestos (DS472, DS497).

— (2020): Work Programme on Electronic Commerce. The E-Commerce Moratorium: Scope and Impact. Doc. WT/GC/W798, Communication from India and South Africa, 10 de marzo.

— (2022): *Aid for Trade at a Glance 2022: Empowering Connected, Sustainable Trade*, OECD, París.

Ortiz Freuler, J. (2021): "The Neutrality Pyramid: A Policy Framework to Distribute Power Over the Net", 11 de marzo. Disponible en: https://decentralizetheweb.org/img/THE_NEUTRALITY_PYRAMID_SECOND_EDITION_JOF.pdf.

— (2022): "The weaponization of private corporate infrastructure: Internet fragmentation and coercive diplomacy in the 21st century", *Global Media and China* 0(0). Doi: https://doi.org/10.1177/20594364221139729.

Redeker, D.; Gill, L. y Gasser, U. (2018): "Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights", *International Communication Gazette*, 80(4), pp. 302-319. Doi: https://doi.org/10.1177/1748048518757121.

Shi-Yin, P. (2022): "The Uneasy Interplay between Digital Inequality and International Economic Law", *European Journal of International Law,* vol. 33, Issue 1 (febrero), pp. 205-236. Disponible en: https://doi.org/10.1093/ejil/chac019.

Tait, M. M.; Dos Reis Peron, A. E. y Suárez, M. (2022): "Terrestrial politics and body-territory: two concepts to make sense of digital colonialism in Latin America", *Tapuya: Latin American Science, Technology & Society*, 5(1), pp. 1-16. Doi: https://doi.org/10.1080/25729861.2022.2090485.

The Affordability Report 2020 (2020): Web Foundation. Alliance for Affordable Internet. Disponible en: https://a4ai.org/affordability-report/report/2020/# (consultado el 11 de junio de 2021).

The Clean Network (s.f.): U.S. Department of State. Disponible en: https://2017-2021.state.gov/the-clean-network/index.html.

Weber, S. (2017): "Data, development, and growth", *Business and Politics*, 19(3), pp. 397-423. Doi: 10.1017/bap.2017.3.

Telefónica y Fundación Carolina presentan, con este volumen, los resultados de la segunda edición de su programa de estudios "Digitalización inclusiva y sostenible en América Latina". Se trata de una línea de actividad centrada en la investigación y el análisis que, en esta oportunidad, se ha detenido a examinar la situación de los derechos digitales en Iberoamérica. El programa refleja la importancia de las alianzas público-privadas para afrontar los retos digitales del futuro inmediato, y plasma la convergencia que, en clave democrática y de respeto a los derechos humanos, une a Europa con América Latina.

Telefónica

Fundación Carolina

AGENDA 2030

Cooperación Española