Derechos digitales en Iberoamérica: situación y perspectivas

ESTUDIO EXTRACTADO POR AGRIVALCA CANELÓN SILVA

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.

PRÓLOGO

Trinidad Jiménez y José Antonio Sanahuja

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 destacar 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. 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 (…)

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 […] poniendo los intereses de la ciudadanía y sus derechos en el centro de estas cuestiones.

LA PROTECCIÓN DE LOS DATOS PERSONALES EN DEFENSA DE LA DIGNIDAD INDIVIDUAL ANTE LOS RIESGOS DE PÉRDIDA DE PRIVACIDAD

María Mercedes Serrano Pérez

Utilizamos la tecnología y el tratamiento de datos personales buscando un beneficio individual y/o colectivo. En este contexto tecnológico, tanto los poderes 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 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 (…)

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 alineado 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 (…)

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 tecnología (…)

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 personales 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 (…)

La vida de la persona se proyecta ahora en forma de datos que reflejan la salud del sujeto, sus gustos, trabajo, preferencias, relaciones, estudios, etcétera. 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 (…)

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)

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 (…)

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 (…)

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 alineado con nuestros valores.

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, etcétera, 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 (…)

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 dere-

chos de los ciudadanos y reforzar la seguridad de los tratamientos (…)

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 (…)

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 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) (…)

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, etcétera; en el fondo revela aspectos de su personalidad que han de quedar bajo el control de la persona misma (…)

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 (…)

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 encomienda 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, etcétera. 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, etcétera.
- 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 protección de datos debería llevarse a cabo por 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 (…)

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.

EL USO ÉTICO DE LA INTELIGENCIA ARTIFICIAL

Celia Fernández-Aller, Camilla Roveri y Santiago Nardini

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 (…)

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.

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* (…)

Algunos autores (Vinuesa *et al.,* 2020: 2) han llevado a cabo estudios centrados en la contribución positiva y negativa de la IA en los Objetivos de Desarrollo Sostenible (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:

- 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 (…)
- 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 pue-

de 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 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.
- 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.

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.

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 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 la UE está en fase de discusión una regulación sobre IA 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 (...)

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

- 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.

- En un segundo lugar está el riesgo alto, en el que se incluyen usos de la IA en infraestructuras críticas que puedan afectar 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.
- 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.
- 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 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

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 (…)

Algunos autores como Suárez Xavier (2022) entienden que habría que vincular los neuroderechos al derecho a la identidad digital (…)

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)* (…)

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 cómo se gestionan los contenidos y cuáles son los nuevos patrones de regulación (…)

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, etcétera. 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) (…)

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 (…)

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* [cursivas nuestras] (…)

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 (…)

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) (…)

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

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 (…)

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 (…)

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 (...)

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).

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.

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 (…)

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 protocolos5. 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 (…)

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).

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) (…)

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 (…)

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 (…)

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 nternet para el legítimo ejercicio de sus derechos (…)

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 (…)

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 (…)

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.

PARTICIPACIÓN CÍVICA Y RELACIONES CON LA ADMINISTRACIÓN PÚBLICA EN EL MARCO DE SU INNOVACIÓN TECNOLÓGICA

Carlos Affonso Souza y Janaina Costa

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 (…)

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 (…)

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? (…)

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.

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.

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 (…)

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) (…)

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 (…)

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 (…)

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 (…)

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.

LA BRECHA DIGITAL EN AMÉRICA LATINA COMO BARRERA PARA EL EJERCICIO PLENO DE DERECHOS

Renata Ávila

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 (…)

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 (…)

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

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 (…)

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 (…) Ante esta situación, si no se producen cambios incentivados por normativas interna-

cionales, 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) (…)

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

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 (…) 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 (…)

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 (…)

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 (…)

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 (…)

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 (…)

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 (…)

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.

AGRIVALCA CANELÓN

Doctora en Comunicación, área disciplinaria Comunicación Organizacional, por la Universidad de Málaga, España. Magíster en Comunicación Social, opción Comunicación Organizacional, Licenciada en Comunicación Social, mención Periodismo Impreso, por la Universidad Católica Andrés Bello, Venezuela. Miembro del Consejo de Redacción de la revista *Comunicación.*

* Ver el estudio completo en la siguiente dirección electrónica: https://www.fundacioncarolina.es/wp-content/uploads/2023/03/DERECHOS-DIGITALES_FC-2.pdf

AUTORES DEL ESTUDIO

TRINIDAD JIMÉNEZ
Directora de Estrategia Global de Asuntos Públicos en Telefónica.

JOSÉ ANTONIO SANAHUJA
Director de la Fundación Carolina.

MARÍA MERCEDES SERRANO PÉREZ
Profesora doctora de Derecho Constitucional en la Universidad de Castilla-La Mancha (UCLM).

CELIA FERNÁNDEZ-ALLER
Profesora contratada doctora en la Universidad Politécnica de Madrid (UPM) en el área de Ética y Derecho.

CAMILLA ROVERI
Máster en Estrategias y Tecnologías para el Desarrollo de la Universidad Politécnica de Madrid (UPM) y la Universidad Complutense de Madrid (UCM).

SANTIAGO NARDINI
Máster en Estrategias y Tecnologías para el Desarrollo de la Universidad Politécnica de Madrid (UPM) y la Universidad Complutense de Madrid (UCM).

J. CARLOS LARA GÁLVEZ
Miembro de la organización Derechos Digitales de Chile desde 2008. Actualmente es su codirector ejecutivo.

CARLOS AFFONSO SOUZA
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).

JAINAINA COSTA
Investigadora senior del Instituto de Tecnología y Sociedad de Río de Janeiro. Licenciada en Derecho. Máster por el Institut d'Étude du Développement Économique et Social (IEDES) de la Sorbona.

RENATA ÁVILA
CEO de Open Knowledge Foundation, entidad dedicada a reducir las barreras al acceso al conocimiento y los datos. Afiliada al Stanford Institute of Human-Centered Artificial Intelligence (HAI) en California, y socia del Centro de Internet y Sociedad del Centro Nacional para la Investigación Científica (CNRS) en París.