



Innovación Tecnológica y Derechos Humanos:

un diálogo necesario para
proteger los derechos humanos
sin menoscabar la innovación



IIDH

Instituto Interamericano
de Derechos Humanos

**Ford
Foundation**

© 2025, Instituto Interamericano de Derechos Humanos
Todos los derechos reservados

Instituto Interamericano de Derechos Humanos
Innovación tecnológica y derechos humanos: Un diálogo necesario para
proteger los derechos humanos sin menoscabar la innovación / Instituto
Interamericano de Derechos Humanos --
San José, C.R. : IIDH, 2025

125 p. : 28 x 22 cm.

ISBN 978-9930-514-54-2

1. Inteligencia artificial (derechos humanos). 2. Innovaciones tecnológicas. 3. Ciencia y tecnología. 4. Protección de datos. I. del Campo, Agustina. II. Aguerre, Carolina. III. Chomczyk Penedo, Andrés. IV. Hinestroza Arenas, Verónica. V. Botero, Carolina. VI. Brigard, Juan de.

Las ideas expuestas en este libro son de exclusiva responsabilidad de las personas autoras y no corresponden necesariamente con las del IIDH o las de sus donantes. Se permite la reproducción total o parcial de los materiales aquí publicados, siempre y cuando no sean alterados, se asignen los créditos correspondientes y se haga llegar una copia de la publicación o reproducción al editor.

Equipo Productor de la Publicación:

José Thompson J.
Director Ejecutivo

Jorge Padilla C.
Coodinador Académico

Agustina del Campo, Carolina Aguerre, Andrés Chomczyk Penedo, Verónica Hinestroza Arenas,
Carolina Botero y Juan de Brigard.
Autores

María Devandas C.
Asistente Académica

INCLUSIVE Consultores
Diseño, Diagramación, Portada y Artes Finales

Instituto Interamericano de Derechos Humanos
Apartado Postal 10.081-1000 San José, Costa Rica
Teléfono: (506) 2234-0404
Fax: (506) 2234-0955
www.iidh.ed.cr

ÍNDICE

Tecnologías emergentes y derechos humanos bajo la perspectiva del marco jurídico interamericano.	3
Por: Agustina del Campo	
ANEXOS	32
Anexo 1: Inteligencia Artificial, Innovación y Derechos Humanos. Notas para una marcha cautelosa en América Latina. Por: Carolina Aguerre	33
Anexo 2: Tecnología blockchain: ¿es posible su uso respetando la privacidad y otros derechos humanos? Por: Andrés Chomczyk Penedo	47
Anexo 3: Interfaces ordenador-cerebro: ¿es necesaria la protección de los "neuroderechos" para respetar los derechos humanos? Por: Verónica Hinestroza Arenas	75
Anexo 4: Sonría, usted está siendo vigilado. Los límites y riesgos del reconocimiento facial como herramienta de seguridad. Por: Carolina Botero y Juan de Brigard	88
NORMATIVA Y/O ESTÁNDARES	121
Convención Americana sobre Derechos Humanos (Pacto de San José)	121
PRINCIPIOS GLOBALES DE LAS NACIONES UNIDAS PARA LA INTEGRIDAD DE LA INFORMACIÓN	121
Epílogo	122

TECNOLOGÍAS EMERGENTES Y DERECHOS HUMANOS BAJO LA PERSPECTIVA DEL MARCO JURÍDICO INTERAMERICANO



Por: Agustina del Campo

I. Introducción y objeto del artículo

Las tecnologías emergentes están transformando radicalmente las sociedades actuales y las actividades humanas. Estamos atravesando un periodo de grandes cambios científicos y tecnológicos que despiertan curiosidad, optimismo, esperanza y preocupación. Las posturas frente al desarrollo y el cambio oscilan entre “tecno-solucionistas” que encuentran en la tecnología las soluciones a los problemas sociales más graves y diversos, hasta pánico frente a los posibles impactos de estos desarrollos y cambios en el tejido social.

Las tecnologías emergentes son innovaciones científicas y técnicas en desarrollo que tienen el potencial de transformar significativamente la sociedad, la economía y la interacción humana. Estas tecnologías se caracterizan por su rápida evolución, su impacto disruptivo en diversos sectores, y por plantear nuevos desafíos éticos y regulatorios (OCDE, 2018; ONU, 2019). Incluyen, entre otras, la inteligencia artificial (IA), la robótica, la impresión 3D, la Internet de las cosas, y la biotecnología.

Este artículo busca introducir los principales desafíos que plantean las tecnologías emergentes y destacar algunos estándares de derechos humanos en el marco del Sistema Interamericano de Derechos Humanos (SIDH) que pueden contribuir al debate y guiar las respuestas. Sin aspirar a un análisis exhaustivo, el texto sentará las bases para futuras investigaciones más profundas, identificando áreas críticas de preocupación y los instrumentos jurídicos relevantes dentro del SIDH. Este documento se basa en cuatro ensayos previos, comisionados en el marco del proyecto de la Fundación Ford que el Instituto Interamericano de Derechos Humanos (IIDH) implementó en 2023, que abordaron los desafíos regulatorios (autorregulatorio, normativo, ético, político y jurídico) los temas de blockchain, inteligencia artificial, neuro tecnologías y tecnologías de vigilancia y reconocimiento facial. La propuesta no es replicar o sintetizar los hallazgos de cada uno de estos ensayos, sino hacer una lectura de estos a partir de estándares asentados en materia de derechos humanos en el SIDH, identificando estándares sólidos que permitan orientar soluciones concretas y claves que permitan responder las preguntas que aún quedan abiertas. Reconociendo que se trata de un campo en rápida evolución, identificar las preguntas pendientes es importante.



De este modo, el trabajo introducirá algunos de los desafíos más apremiantes en materia de derechos humanos en el contexto del SIDH, incluyendo:

- El derecho a la privacidad y la protección de datos personales
- El derecho a la libertad de expresión
- El derecho a la igualdad y no discriminación
- El debido proceso legal

Estos derechos están protegidos por diversos instrumentos del SIDH, como la Convención Americana sobre Derechos Humanos (CADH) y la jurisprudencia de la Corte Interamericana de Derechos Humanos (Corte IDH). El artículo examinará cómo estos instrumentos pueden interpretarse de manera evolutiva y aplicarse en el contexto de las nuevas tecnologías.

II. La importancia de una aproximación basada en derechos

En los últimos años, las preocupaciones sobre los desafíos éticos y jurídicos que plantea el rápido desarrollo de las nuevas tecnologías han impulsado la creación gradual de un marco normativo internacional. Se han observado recientes iniciativas multilaterales que abordan estos temas de manera integral.

Diversos mecanismos internacionales han destacado la necesidad de enmarcar el desarrollo tecnológico y su regulación bajo el derecho internacional de los derechos humanos, empezando con la Organización de las Naciones Unidas (ONU) desde la Cumbre Mundial sobre la Sociedad de la Información (WSIS por sus siglas en inglés) y la creación del Foro de Gobernanza de Internet¹.

En la última década, la ONU ha establecido varios mecanismos, como la Relatoría Especial sobre el derecho a la Privacidad en 2015²; el Panel de Alto Nivel para la Cooperación Digital en 2018³;

¹ Naciones Unidas (s.f.). Foro de Gobernanza de Internet (IGF). Recuperado de: <https://publicadministration.desa.un.org/projects/internet-governance-forum-igf-2006-current>

² Consejo de Derechos Humanos de las Naciones Unidas, OHCHR, 2015. El Consejo de Derechos Humanos crea el mandato del Relator Especial sobre el derecho a la privacidad. Recuperado de: <https://www.ohchr.org/en/press-releases/2015/03/human-rights-council-creates-mandate-special-rapporteur-right-privacy>.

³ Naciones Unidas (2018). Panel de Alto Nivel para la Cooperación. Recuperado de: https://www.un.org/en/pdfs/HLP-on-Digital-Cooperation_Press-Release.pdf.



el proyecto B-Tech en 2019⁴, para asesorar Estados y empresas sobre la implementación de los Principios Rectores sobre Derechos Humanos y Empresas; la Oficina del Tech Envoy en 2022⁵; y el Panel de Alto Nivel sobre Inteligencia Artificial convocado en 2023⁶.

La Conferencia General de la UNESCO adoptó en noviembre de 2021 la Recomendación sobre la Ética de la Inteligencia Artificial, con el fin de proteger y promover los derechos humanos. El Consejo de Derechos Humanos de la ONU también, ha abordado los riesgos asociados con las nuevas tecnologías. Un informe de mayo de 2021 del Comité Asesor del Consejo de Derechos Humanos alertaba sobre el impacto discriminatorio de las tecnologías digitales emergentes y las amenazas a la autonomía de la voluntad mental de los usuarios.

La Organización para la Cooperación y Desarrollo Económicos (OCDE) adoptó los Principios sobre la Inteligencia Artificial, que guían a gobiernos, organizaciones e individuos para que, para priorizar los intereses de las personas y garantizar la responsabilidad en el diseño y gestión de sistemas de IA. En septiembre de 2024 en el marco de la Cumbre del Futuro los líderes reunidos por Naciones Unidas adoptaron el Pacto del Futuro, que incluyó el Pacto Digital Mundial, comprometiéndose a respetar, proteger y promover los derechos en el espacio digital.^{7 8}

Estos documentos argumentan en mayor o menor medida la necesidad de proteger y promover los derechos humanos en el entorno digital. El derecho internacional de los derechos humanos constituye una base normativa compartida por todos los países a nivel global, diseñados y adoptados para proteger y promover los derechos básicos de los individuos frente al poder estatal. Aunque las aproximaciones a los derechos humanos pueden variar entre países, la narrativa de derechos humanos constituye un lenguaje común, ideal para lidiar con tecnologías globales, interjurisdiccionales, en muchos casos descentralizadas, como es Internet. Con más de 75 años de desarrollo, ha fortalecido las democracias del mundo, promovido la responsabilidad y el accountability por atrocidades, limitando el ejercicio abusivo del poder.

A pesar de que los desafíos en materia de derechos humanos todavía son muchos y la democracia atraviesa una crisis sin precedentes, a un año de las celebraciones por el 75 aniversario de la Declaración Universal de Derechos Humanos conviene destacar este marco como uno deseable y realizable, más aún, como una guía común durante la transformación tecnológica que estamos viviendo.

⁴ Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (2019). Proyecto B-Tech. Recuperado de: <https://www.ohchr.org/es/business/b-tech-project#:~:text=El%20Proyecto%20B%2DTech%20proporciona,la%20esfera%20de%20la%20tecnolog%C3%ADa>

⁵ Asamblea General de las Naciones Unidas (2020). Roadmap for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation, A/74/821. Recuperado de: <https://documents.un.org/doc/undoc/gen/n20/102/51/pdf/n2010251.pdf>.

⁶ Naciones Unidas (2023). Órgano Asesor sobre Inteligencia Artificial. Recuperado de: <https://www.un.org/techenvoy/ai-advisory-body>.

⁷ Naciones Unidas, El Pacto del Futuro, Resolución aprobada por la Asamblea General el 22 de septiembre de 2024, A/RES/79/1, 22 de septiembre de 2024, Anexo Pacto Digital para el Futuro, disponible en <https://documents.un.org/doc/undoc/gen/n24/272/25/pdf/n2427225.pdf>.

⁸ Íbidem.



i. Aproximaciones técnicas y políticas a las tecnologías emergentes

Las tecnologías emergentes son innovaciones científicas y técnicas que ofrecen un potencial sin precedentes y cuyos riesgos en muchos casos se desconocen. La mayoría de los expertos coinciden en que estas tecnologías se encuentran en una fase experimental. Estas innovaciones transforman significativamente los límites entre los espacios virtuales, físicos y biológicos.

Según el informe del Comité Asesor del Consejo de Derechos Humanos de la ONU (2021), las tecnologías emergentes incluyen:

"la distribución de datos y la toma de decisiones automatizada, como la inteligencia artificial, la Internet de las cosas, la tecnología de cadenas de bloques y la computación en la nube, entre otras"⁹. También se refiere "a una amplitud de respuestas sobre muchos tipos de sistemas diferentes, como la robótica, la automatización, las ondas inalámbricas, el análisis predictivo y varios tipos de tecnologías de la información y la comunicación (TIC) que están presentes en diferentes etapas del ciclo de datificación"¹⁰.

El Foro Económico Mundial (WEF, por sus siglas en inglés), en su informe *Top 10 Emerging Technologies of 2023*, destacan que estas tecnologías pueden caracterizarse por algunas características como:

- **Novedad:** la tecnología está emergiendo y en una etapa inicial de desarrollo incipiente, no se usa ampliamente todavía.
- **Aplicabilidad:** tiene el potencial de ser de uso significativo y beneficio para las sociedades y economías en el futuro; no es solo de interés marginal.
- **Profundidad:** está siendo desarrollada por más de una empresa y es el foco de un creciente interés e inversión dentro de la comunidad experta; probablemente tendrá un impacto significativo en los próximos 3-5 años.
- **Potencia:** es potencialmente poderosa y disruptiva en la alteración de formas e industrias establecidas¹¹.

Actualmente, estamos en un momento caracterizado por la proliferación de marcos regulatorios para la tecnología. La forma de enmarcar el desarrollo tecnológico varía según el sector, el país o instituciones o actores internacionales. Existen múltiples iniciativas paralelas compitiendo por

⁹ Naciones Unidas, ONU (2021), *Impactos, oportunidades y retos que pueden entrañar las tecnologías digitales nuevas y emergentes en relación con la promoción y la protección de los derechos humanos* (Informe del Comité Asesor del Consejo de Derechos Humanos, A/HRC/47/52). Recuperado de: <https://documents.un.org/doc/undoc/gen/n20/102/51/pdf/n2010251.pdf>

¹⁰ Ibidem.

¹¹ Foro Económico Mundial (junio, 2023), *Top 10 Emerging Technologies of 2023*, Recuperado de <https://www.weforum.org/reports/top-10-emerging-technologies-of-2023>



establecerse como modelos para la industria.¹² A la autorregulación empresarial, que otrora era la preferida por diversos actores en el marco de la gobernanza global de la tecnología, se suman iniciativas regionales, globales, éticas, jurídicas, políticas y económicas de distinta índole.

a. Aproximación general vs. aproximación a los usos específicos

Los desafíos que el desarrollo tecnológico plantea han dado lugar a múltiples focos de tensión. Una tendencia común en el derecho comparado e incluso en el derecho internacional parece abordar las tecnologías emergentes de manera integral y atender a las regulaciones, autorregulaciones y co-regulaciones de tecnologías específicas. Así, durante los últimos años surgieron principios, pautas y regulaciones de tecnologías específicas como la Inteligencia Artificial o las neuro tecnologías. La ya mencionada Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO o los Principios de la OCDE sobre la Inteligencia Artificial son ejemplos de ello. En la misma línea parece ir el desarrollo de principios y regulaciones en materia de neuro tecnologías. La UNESCO lanzó un nuevo proceso para generar recomendaciones en materia de neuro tecnologías, siguiendo el modelo del proceso que dio lugar a las recomendaciones de IA.¹³ En el ámbito regional, el Comité Jurídico Interamericano (CJI) de la OEA aprobó en marzo de 2023 los Principios Interamericanos en materia de Neurociencias, Neuro tecnologías y Derechos Humanos, destacando la necesidad de una regulación específica para proteger los derechos de niñas, niños y adolescentes, así como de personas con discapacidad.

Esta aproximación general, centrada en el tipo de tecnología, contrasta con el desarrollo de estándares y principios enfocados en los usos específicos de las tecnologías y su inserción e impacto en prácticas sociales preexistentes, más que en la tecnología misma. Por ejemplo, las tecnologías de reconocimiento facial se regulan considerando su uso posible para vigilancia masiva o persecución policial. Así enfoca su análisis el Parlamento Europeo, por ejemplo, cuando prohíbe, en principio, el uso de tecnologías de reconocimiento facial en la ley de inteligencia artificial de 2023 y establece excepciones para su adopción en casos específicos (aunque las mismas hayan sido fuertemente criticadas por su vaguedad o amplitud).

Esta misma aproximación la reflejan Carolina Botero y Juan de Brigard en su ensayo “Sonría, ud está siendo vigilado” en tanto destacan el uso de la tecnología aplicada a la labor policial y su vinculación con el concepto de seguridad en nuestras sociedades. El foco de atención no es la tecnología misma sino su posible uso por parte del aparato estatal y como se insertan estas prácticas o desarrollos tecnológicos en la historia más amplia de prevención y persecución del delito, estereotipos, seguridad, etc. De la misma manera enfoca Chomczyk Penedo el análisis de la tecnología de *blockchain*, que difiere (o puede diferir) en los 4 usos concretos que el artículo

¹² Órgano Asesor de Alto Nivel de Naciones Unidas sobre IA (2024), *Gobernanza de la IA en Beneficio de la Humanidad*, Recuperado de: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf.

¹³ UNESCO (s.f). *Ética y neurotecnologías*. Recuperado de: <https://www.unesco.org/es/ethics-neurotech>.



describe: sistemas de registro de identidad, votación, registro de propiedad inmueble, y sistema bancario y financiero¹⁴.

A veces, los documentos generales establecen principios y normas respecto de ciertas tecnologías y destacan algunos de los problemas vinculados a algunos de sus usos. La ley europea de IA de 2023 es un ejemplo, ya que establece normas generales sobre IA y también identifica algunas aplicaciones particularmente problemáticas, como la IA en la biometría.

Las diferentes aproximaciones regulatorias tienen ventajas y desventajas. Los principios generales, como las Recomendaciones de la UNESCO sobre la Ética de la Inteligencia Artificial o los Principios Interamericanos en materia de neurociencias ofrecen un marco amplio dentro del cual luego pueden desarrollarse principios concretos para cada uno de sus posibles usos. Sin embargo, uno de los riesgos de la aproximación más amplia es la vaguedad que muchas veces supone un texto general y amplio en términos de derechos humanos. El desarrollo de este tipo de marcos, en algunos casos, también ha colaborado a la percepción de “vacío legal” que rige respecto de algunas tecnologías y sus despliegues. Como señala Hinestroza Arenas¹⁵ en su ensayo anexo sobre neuro derechos, este tipo de aproximaciones puede derivar en reclamos de nuevos derechos o renegociaciones respecto del contenido de derechos existentes. Las aproximaciones por los usos tienden a ser más específicas y permiten un desarrollo más cuidado de los elementos necesarios para la protección y promoción de derechos humanos en el desarrollo, despliegue e implementación de nuevas tecnologías en distintos contextos. Indudablemente las aproximaciones son complementarias.

b. Aproximaciones desde los riesgos y aproximaciones desde los derechos

El carácter experimental y la velocidad con la que se desarrollan las tecnologías emergentes han generado importantes interrogantes sobre su impacto en la sociedad y en el ejercicio y protección de los derechos humanos. Gran parte de este desarrollo tecnológico está en manos del sector privado, el cuál opera bajo los Principios Rectores de las Naciones Unidas sobre Empresas y Derechos Humanos (PRNU). Estos principios, aunque no vinculantes, promueven un enfoque basado en el análisis de riesgos y se integran en la mayoría de los países en el marco de la responsabilidad social empresarial.

Los PRNU fueron el resultado de años de negociación y desencuentros respecto a la aplicabilidad y obligatoriedad de los derechos humanos en el sector privado.¹⁶ En resumen, los Principios reiteran la responsabilidad de los Estados como principales obligados en materia de prevención, protección y promoción de derechos humanos y establecen recomendaciones para que las empresas

¹⁴ Chomczyk Penedo, A. (2023) *Tecnología blockchain: ¿es posible su uso respetando el derecho a la privacidad y otros derechos humanos?* Anexo 4.

¹⁵ Hinestroza-Arenas A. (2023) *Interfaces Ordenador-Cerebro: ¿es necesaria la protección de los neuro derechos para respetar los derechos humanos?* Anexo 2.

¹⁶ Alvarez Ugarte, R. (2020). *ICT and Human Rights: Towards a Conceptual framework of Human Rights Impact Assessments*. Recuperado de: https://www.palermo.edu/Archivos_content/2021/cele/papers/ICT-and-Human-Rights.pdf.



identifiquen, evalúen y mitiguen los posibles impactos de sus actividades en los derechos humanos. Dichas recomendaciones han de implementarse a través de la adopción de mecanismos como la debida diligencia empresarial y los análisis de impacto en derechos humanos. Indudablemente el marco también ofrece recomendaciones para el sector de tecnologías del conocimiento y la información (TIC), incluyendo intermediarios de infraestructura, de protocolos y de contenidos.

Los PRNU están vigentes desde su adopción en 2011 con distintos niveles de adhesión y cumplimiento por parte de las distintas empresas obligadas.¹⁷ El carácter voluntario del cumplimiento y la ausencia de mecanismos efectivos de monitoreo han llevado a varios Estados y organismos internacionales a impulsar regulaciones estatales más directas. Estas regulaciones replican parcialmente el lenguaje de los Principios Rectores e incorporan obligaciones de identificación y monitoreo de riesgos a los derechos humanos generados por el desarrollo, despliegue y aplicación de tecnologías como la IA. Asimismo, establecen obligaciones concretas de mitigación y reparación.

La aproximación basada en riesgos, propuesta por los PRNU ha sido adoptada por varias propuestas legislativas y *soft law* a nivel internacional¹⁹, generando claros beneficios, pero también algunos desafíos importantes. Entre sus ventajas, esta aproximación permite superar la asimetría de información que caracteriza a este campo, donde el sector privado tiene más y mejores herramientas para evaluar el impacto de sus servicios en la sociedad; y efectiviza el principio de “inmediatez” en la medida en que genera obligaciones para quien está en mejores condiciones de conocer, prevenir, y reparar el daño.

Entre los desafíos, sin embargo, delega en el sector privado la identificación y mitigación de riesgos poco claros, sin definiciones concretas, y genera obligaciones de mitigación que indudablemente redundan en muchos casos en limitaciones al ejercicio de ciertos derechos, por ejemplo, la privacidad o la libertad de expresión. Además, en muchos casos, la enunciación de obligaciones basadas en riesgos excede el marco de los derechos humanos y se amplía a todo tipo de riesgos, algunos jurídicamente reconocidos como tales y otros no. La escisión de los riesgos por un lado y el marco jurídico donde estos se definen y conceptualizan por el otro genera enorme amplitud y discrecionalidad tanto en la empresa obligada a identificarlos, mitigarlos y repararlos como en el órgano estatal supervisor, encargado de verificar el cumplimiento y la adecuación de la conducta empresarial a la norma.²⁰

¹⁷ Naciones Unidas (2011). *Principios Rectores sobre Derechos Humanos y Empresas* Recuperado en: https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_SP.pdf.

¹⁸ Del Campo, A., Zara N., y Alvarez Ugarte R., *Are Risks the New Rights: the perils of the risks approach in tech regulation, (forthcoming)* Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5161173.

¹⁹ Reglamento (UE) 2022/2065, Ley de Servicios Digitales de la Unión Europea <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32022R2065>; Reglamento (UE) 2024/1689, Ley de Inteligencia Artificial de la Unión Europea https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=OJ:L_202401689; UNESCO, Directrices para la gobernanza de las plataformas digitales: salvaguardar la libertad de expresión y el acceso a la información con un enfoque de múltiples partes interesadas, 2023, <https://unesdoc.unesco.org/ark:/48223/pf0000387360>; UNESCO, Recomendación sobre la ética de la inteligencia artificial, 2022, https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa; OEA, Relatoría para la Libertad de Expresión, Inclusión digital y gobernanza de contenidos en internet, CIDH/RELE/INF. 28/24, 2024, https://www.oas.org/es/cidh/expresion/informes/Inclusion_digital_esp.pdf.

²⁰ Del Campo, A., Zara N., y Alvarez Ugarte R., *Are Risks the New Rights: the perils of the risks approach in tech regulation, (forthcoming)* Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5161173.



c. Ética y Derechos Humanos

Existe una creciente tensión entre las guías éticas y los instrumentos jurídicos vinculantes en el ámbito de las tecnologías emergentes y los derechos humanos. Por un lado, instrumentos como la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO ofrecen directrices éticas no vinculantes. Por otro lado, los tratados internacionales de derechos humanos, como la CADH, establecen obligaciones jurídicas vinculantes para los Estados.

Esta tensión plantea varias preguntas: ¿Cómo se relacionan estos diferentes tipos de instrumentos entre sí? En caso de conflicto, ¿cuál debería prevalecer? Aunque existe una conexión entre la ética y el derecho, la exigibilidad y el monitoreo de ambos ámbitos difieren significativamente. ¿Cómo puede el soft law (incluyendo aquí a las guías éticas) influir en la interpretación y aplicación de los tratados de derechos humanos en el contexto de las nuevas tecnologías? ¿Están los marcos jurídicos actuales equipados para abordar los desafíos planteados por las tecnologías emergentes? El desarrollo conjunto de principios éticos, morales y jurídicos puede diluir las obligaciones concretas establecidas por el derecho internacional vigente. Este artículo propone identificar áreas donde el derecho ya establece normas precisas que no requieren adaptación, y otras donde se requiere mayor desarrollo y especificidad.

III. Oportunidades y desafíos para la aplicación de estándares interamericanos en el desarrollo de tecnologías emergentes

La incorporación de tecnologías emergentes en la vida cotidiana tiene un impacto significativo en el desarrollo social, político y económico de los países. Es conveniente analizarlas desde una perspectiva de derechos humanos, ya que, aunque abarcan una amplia variedad de avances técnicos y científicos, estas tecnologías afectan directamente el ejercicio y la protección de derechos humanos. El SIDH ofrece un marco robusto para abordar los desafíos planteados por las tecnologías emergentes.

i. Libertad de expresión

La Declaración Conjunta de los Relatores de 2009²¹ ya hacía referencia a la importancia de la libertad de expresión incluso en Internet. Y el primer informe temático de Naciones Unidas en abordar directamente el tema de derechos humanos y tecnología fue el Informe de Frank La Rue de 2011²². La Comisión Interamericana de Derechos Humanos (CIDH) ha reconocido que las nuevas tecnologías e la información y la comunicación han facilitado el ejercicio de la libertad de expresión

²¹ Comisión Interamericana de Derechos Humanos (CIDH) (2011). *Declaración Conjunta sobre Libertad de Expresión e Internet*, Recuperado de: <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849>.

²² La Rue, F. (2011) *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión*, (A/HRC/17/27) 2011 Recuperado de: <https://digitallibrary.un.org/record/706200?ln=en&v=pdf>.



y el acceso a la información, pero también ha advertido sobre los riesgos que estas tecnologías pueden representar para otros derechos (RELE CIDH, Libertad de expresión e internet, OEA/Ser.L/V/II. CIDH/ RELE/INF. 11/13, 2013).

El derecho a la libertad de expresión está consagrado en el artículo 13 de la CADH. El enunciado del artículo 13 difiere en parte del enunciado de los artículos 19 del Pacto Internacional de Derechos Civiles y Políticos y del artículo 10 de la Convención Europea de Derechos Humanos. Es el único de los tres que prohíbe en términos explícitos la censura previa y las restricciones indirectas por parte del estado.

El artículo 13.2 de la Convención Americana dispone expresamente que el ejercicio de la libertad de expresión

no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: (a) el respeto a los derechos o a la reputación de los demás, o (b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas. Según ha expresado la CIDH, la censura previa "(...) tiene lugar cuando, por medio del poder público, se establecen medios para impedir en forma previa la libre circulación de información, ideas, opiniones o noticias, por cualquier tipo de procedimiento que condicione la expresión o la difusión de información al control del Estado, por ejemplo, mediante la prohibición de publicaciones o el secuestro de las mismas, o cualquier otro procedimiento orientado al mismo fin"²³.

La CIDH ha sostenido que *la censura previa es el prototipo de violación extrema y radical de la libertad de expresión, ya que conlleva su supresión.*

La libertad de expresión es la regla y la limitación a la libertad de expresión ha de ser excepcional, a través de responsabilidades ulteriores establecidas por ley, proporcionadas y necesarias²⁴. Las responsabilidades ulteriores tampoco pueden ser discriminatorias o producir efectos discriminatorios.²⁵

Gran parte del desarrollo tecnológico de los últimos años impacta directa o indirectamente el ejercicio de la libertad de expresión o tiene aplicaciones que pueden impactarla. La inteligencia artificial ha permitido la moderación automatizada de contenidos en Internet, curando el contenido en

²³ Organización de los Estados Americanos (OEA), Comisión Interamericana de Derechos Humanos (2019), *Informe Anual de la Comisión Interamericana de Derechos Humanos 2009, Informe de la Relatoría Especial para la libertad de expresión* (OEA/Ser. L/V/II., 30 de diciembre de 2009, p. 272.) Ver también Corte Interamericana de Derechos Humanos, Caso Palamara Iribarne Vs. Chile, 2005, Serie C No. 135, párr. 68. Recuperado de: https://www.corteidh.or.cr/docs/casos/articulos/seriec_135_esp.pdf

²⁴ Organización de los Estados Americanos (OEA), Comisión Interamericana de Derechos Humanos (2015), *Informe Anual de la Comisión Interamericana de Derechos Humanos, Informe Anual de la Relatoría Especial para la Libertad de Expresión*, (OEA/Ser.L/V/II., Doc. 48/15, 31 de diciembre de 2015, párr. 25).

²⁵ Organización de los Estados Americanos (OEA), Comisión Interamericana de Derechos Humanos (2019), *Informe Anual de la Comisión Interamericana de Derechos Humanos 2009, Informe de la Relatoría Especial para la libertad de expresión* (OEA/Ser. L/V/II., 30 de diciembre de 2009, p. 251.)



línea en tiempo real, filtrando y bloqueando ciertos materiales, monitoreando la expresión en una escala nunca vista. Además, la IA generativa ha revolucionado la producción de contenido escrito y audiovisual, ampliando las posibilidades en términos de creación, réplicas, falsificaciones, superposiciones, etc. Este avance, como indica Aguerre en su ensayo anexo, ha generado respuestas inmediatas por parte de sectores privados, Estados, sociedad civil y académicos a nivel global por las oportunidades y riesgos que esta genera.²⁶ Por un lado, la disponibilidad de IA supone cambios radicales en la eficiencia y la velocidad en la producción de contenidos y amenaza con distorsionar distintos escenarios del mundo laboral actual. Por otro lado, la rapidez de su desarrollo y la falta de conocimiento y capacidad técnica para auditar estas tecnologías también genera preocupaciones en torno al debido proceso, la igualdad y no discriminación, incluso en su aplicación a los estándares de libertad de expresión.

Asimismo, las diferencias en la accesibilidad a estas tecnologías y su gobernanza han sido identificadas como amenazas para el desarrollo sostenible de aquellos países excluidos. Solo unas pocas empresas y/o países a nivel global que pueden desarrollar sistemas eficientes de IA, incluso en estado experimental. Según el Órgano Asesor de Alto Nivel de Naciones Unidas sobre IA en su Informe Gobernanza de la IA en Beneficio de la Humanidad, son pocos los países que han participado en la elaboración de los principales documentos de gobernanza de la IA y muchos no han participado en ninguno a pesar de ser impactados directa o indirectamente por estas tecnologías.²⁷ En la misma línea, la tecnología biométrica aplicada al ámbito público también supone amenazas a los derechos al anonimato y la protesta, además de las amenazas a la privacidad y debido proceso que serán abordadas más adelante.

De igual manera, la internet de las cosas supone la apertura con fines de vigilancia del ámbito más restringido y privado de las personas. Las neuro tecnologías, como destaca el Comité Jurídico Interamericano, suponen riesgos para la libertad de expresión y opinión en tanto abre oportunidades de manipulación e injerencias en la voluntad y la dignidad. El CIJ subraya conforme al Principio 7 de la Declaración de Principios Interamericanos en Materia de Neurociencias, Neuro tecnologías y Derechos humanos, la importancia de proteger la integridad neurocognitiva de las personas, señalando que es fundamental evitar un uso ilegítimo y malicioso de las neuro tecnologías, especialmente cuando estas pueden emplearse para intervenir en la actividad cerebral con fines perjudiciales o que limiten el ejercicio de los derechos humanos. Asimismo, se enfatiza que el acceso a la actividad de la persona no debe nunca comprometer la libertad de pensamiento y conciencia, ni hacer que estos dependan de terceros, ya que ello afectaría derechos, seguridad e independencia²⁸.

Las amenazas a la libertad de expresión aparecen de la mano del sector estatal y del sector privado. Respecto del Estado, la tecnología permite un nivel de escrutinio y vigilancia inédito, lo cual les ha dado a los distintos países del mundo una herramienta de monitoreo y observación de la conversación

²⁶ Aguerre, C. (2023) *Inteligencia Artificial, Innovación y Derechos Humanos. Notas para una marcha cautelosa en América Latina*. Anexo 1.

²⁷ Órgano Asesor de Alto Nivel de Naciones Unidas sobre IA (2024), *Gobernanza de la IA en Beneficio de la Humanidad*, pág. 9 Recuperado de: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf

²⁸ Ver en este sentido: **Principio 7 de la Declaración de Principios Interamericanos en Materia de Neurociencias, Neuro tecnologías y Derechos Humanos.**



sin precedentes que amenaza la libertad de expresión y de asociación, entre otros derechos. Además, la capacidad de sistematización de información con la que actualmente contamos permite hacer inteligencia en fuentes abiertas, poco reguladas hasta el momento en las distintas regiones del mundo, incluyendo la región Interamericana.²⁹ Con la socialización de Internet y su adopción masiva, también los Estados han adoptado prácticas que han resultado en muchos casos contraproducentes y problemáticas desde la perspectiva de libertad de expresión, incluyendo campañas de estigmatización y persecución de minorías y disidentes, desinformación estatal, prácticas abusivas en el desarrollo de campañas electorales online, etc.

Desde el sector privado, aquello que una vez parecía completamente descentralizado y neutro, con el correr de los años se volvió más y más concentrado en manos de un grupo de compañías específicas. Esto generó que ciertas prácticas, como la moderación y curación de contenidos en Internet tengan un impacto desproporcionado en la libertad de expresión de un grupo cada vez mayor de usuarios y productores de contenidos, incluyendo periodistas, sociedad civil, artistas e influencers. Las plataformas de redes sociales y otros intermediarios en línea se han convertido en importantes “guardianes” de la libertad de expresión en línea. Sus políticas de moderación de contenidos, a menudo implementadas a través de algoritmos de IA, pueden tener una enorme influencia en el discurso público y la falta de seguimiento por parte de las empresas de criterios claros y respetuosos de los derechos humanos pueden amenazar la fortaleza de la conversación pública necesaria en una democracia.³⁰ La regulación privada del discurso en internet, además, está atravesada por distintas tecnologías, incluyendo tecnologías de vigilancia y monitoreo, automatización e inteligencia artificial.

Por otro lado, el dominio de unas pocas empresas tecnológicas sobre los principales canales de comunicación en línea plantea preocupaciones sobre la diversidad y el pluralismo en el discurso público. La Relatoría Especial para la Libertad de Expresión (RELE) de la CIDH ha entendido que la concentración de la propiedad de los medios de comunicación es una práctica que atenta contra la pluralidad de voces e impide la expresión diversa de los distintos sectores de la sociedad. La concentración en Internet plantea desafíos nuevos, siendo la definición de concentración uno de ellos. ¿A que atender para establecer dominio de mercado? ¿Y en todo caso de cual mercado? Atento la interjurisdiccionalidad de internet, no todos los Estados tienen condiciones similares para regular un mercado global y descentralizado como el que Internet plantea. La Unión Europea adoptó recientemente la Digital Markets Act y el proceso de implementación posiblemente dejará lecciones aprendidas y mejores prácticas tanto para la Unión como para el resto de los países del mundo con mercados más pequeños o capacidades de regulación más limitadas.

El enunciado del artículo 13 de la Convención Americana y los principios esbozados en la jurisprudencia interamericana en materia de libertad de expresión permiten formular algunas afirmaciones

²⁹ Bertoni, E. (2023) Las prácticas OSINT, ¿son amigas o enemigas de los derechos humanos?, CELE. Recuperado de: https://www.palermo.edu/Archivos_content/2023/cele/papers/231115-Bertoni-reporte-inicial-OSINT.pdf, Zara N. (2023). Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay, CELE, Recuperado de: https://www.palermo.edu/Archivos_content/2023/cele/papers/233008-reporte-regional-OSINT.pdf.

³⁰ Naciones Unidas (2011), *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión* (A/HRC/38/35). Recuperado de: <https://digitallibrary.un.org/record/706200?ln=en&v=pdf>



a priori que resultan aplicables tanto a estas como a otras tecnologías que impacten o puedan impactar este derecho. Una primera afirmación, siguiendo lo establecido arriba, es que la libertad de expresión está protegida sin perjuicio del medio que se utilice para ejercerla y que el derecho aplica a las expresiones protegidas en cualquier formato y los Estados tienen la obligación de abstenerse de interferir arbitrariamente en su ejercicio.³¹ Es decir, las expresiones online y offline están protegidas, sean estas generadas orgánica o artificialmente, sean estas verdaderas o falsas.

Sin embargo, el avance tecnológico ha generado nuevos debates relacionados con la libertad de expresión. Por ejemplo, han surgido discusiones sobre derechos de autor, por ejemplo, sobre todo respecto de contenidos generados por IA, así como a los posibles daños que este contenido pueda generar, incluyendo desinformación, discriminación, estigmatización o incluso calumnias e injurias. Frente a estas problemáticas, los principios y la jurisprudencia interamericana permiten afirmar también que, en la resolución de estas cuestiones, toda vez que el Estado limite la libertad de expresión, deberá hacerlo conforme a una ley, de manera clara y conforme los procedimientos legalmente establecidos para su adopción. Dicha ley deberá perseguir un objetivo legítimo, ser necesaria y proporcionada. La forma de abordar las problemáticas surgidas del desarrollo tecnológico y su aplicación o implicancias en el ejercicio de distintos derechos consagrados en la ley dependerá de cada Estado. En ningún caso, salvo las excepciones explícitas que la CADH establece, podrán los Estados ordenar o indirectamente promover la censura previa. Así lo establecen múltiples documentos desarrollados en el seno del SIA, incluyendo el informe sobre libertad de expresión y desinformación electoral encomendado por la Asamblea General de la OEA a la RELE en 2018.³²

Además, según el Observatorio Regional sobre Libertad de Expresión del CELE, el desarrollo tecnológico trajo consigo la reapertura de debates de libertad de expresión que parecían saldados hasta la década del 2010. Entre ellos, los debates en torno al derecho al olvido, calumnias e injurias en internet, discurso discriminatorio, discurso dañino, pero no ilegal. Existe una tendencia a la reapertura de debates legislativos orientados a modificar estándares bien asentados en la jurisprudencia del sistema interamericano, en muchos casos fundamentándose en la velocidad, permanencia y el volumen de contenido disponible en Internet.³³ El mismo esquema se replica en otras regiones del mundo, incluyendo África, Europa y Asia. Si bien en muchos casos los Congresos logran un debate robusto y descartan soluciones contrarias a la libertad de expresión, sobre todo después de la pandemia de COVID 19 y en la crisis democrática que azota distintas regiones desde hace décadas, muchas leyes si fueron aprobadas incluso contrarias a estándares de derechos humanos bien establecidos.

³¹ Así se pronunciaron los relatores de la ONU, OSCE, OEA y CADHP (2017) advirtiendo que “las prohibiciones generales de difusión de información basadas en conceptos imprecisos y ambiguos, incluidos ‘noticias falsas’ (‘fake news’) o ‘información no objetiva’, son incompatibles con los estándares internacionales sobre restricciones a la libertad de expresión” ONU, OSCE, OEA, CADHP, [Declaración Conjunta Sobre Libertad De Expresión Y “Noticias Falsas” \(“Fake News”\), Desinformación Y Propaganda](#), 2017, párr. 2a.

³² OEA, Relatoría Especial para la Libertad de Expresión, Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales, OEA/Ser.D/XV.22, 2019, https://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf.

³³ Del Campo, A. (2023), *Volume, Speed, and Accessibility as Autonomous Harms: Can Modern Legal Systems Deal With Harmful but Legal Content? en New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*. Carnegie Endowment for International Peace. Recuperado de: https://carnegie-production-assets.s3.amazonaws.com/static/files/Feldstein_et_al_-_DDN_spread-UPDATED2.pdf.



Los Estados no sólo tienen obligaciones de respeto, sino que también, en línea con el artículo 13 y el artículo 1 y 2 de la CADH, tienen obligaciones de garantía, sin discriminación, y de adecuación de sus ordenamientos internos a la CADH. La obligación de respeto supone obligaciones negativas por parte del Estado, es decir obligaciones de no hacer. Por otro lado, la obligación de garantía parte supone obligaciones de hacer, incluyendo adoptar leyes que garanticen el legítimo ejercicio de la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, a través de fronteras, por cualquier medio. Esta obligación ha sido destacada recientemente por diversos organismos nacionales e internacionales, como la UNESCO.

En 2023, la UNESCO adoptó las Guías sobre regulación de plataformas para orientar a los Estados en el desarrollo de medidas regulatorias de garantía.³⁴ El trabajo de la UNESCO parece haber estado en gran parte inspirado por la regulación europea que hizo punta de lanza en la materia: la Digital Services Act. Esta ley, aprobada en 2022 es la primera dedicada a la gobernanza de plataformas de redes sociales y buscadores precisamente para ejercer algún control sobre el sector privado dedicado a la curación, hosteo y promoción de contenidos de terceros (buscadores y redes sociales principalmente, pero también ciertas plataformas de e-commerce). Adoptada en el seno del parlamento europeo e implementada en parte por la Comisión Europea en colaboración con los distintos Estados de Unión, la ley propone una aproximación a las plataformas en términos de riesgo e identifica una serie de riesgos en el artículo 34 que las plataformas deben analizar, informar y mitigar. El documento trae consigo la consagración de ciertas obligaciones como el debido proceso, la notificación y la posibilidad de apelación que las empresas que moderen contenidos deberán de ahora en adelante contemplar respecto de sus usuarios. También incluyen obligaciones de transparencia respecto de sus términos y condiciones de servicio y obligaciones de informar regularmente sus prácticas y sus estadísticas en materia de implementación de sus Teorías de Detección de Señales. Estas obligaciones son bienvenidas.

Paralelamente, sin embargo, también traen consigo obligaciones poco concretas respecto de contenidos lícitos. La DSA, al igual que las Guías de la UNESCO, adoptan una aproximación de riesgos a la tecnología, identificando no solo riesgos a los derechos humanos sino también otros riesgos directamente orientados a abordar expresiones lícitas potencialmente dañinas para el espacio cívico o la democracia, mujeres y niñas, niños y adolescentes, entre otras. Estas últimas plantean desafíos particularmente difíciles si la ley de Europa fuera un posible modelo para las leyes locales en la región Interamericana. Las diferencias en la enunciación y el contenido de la libertad de expresión en ambos sistemas será una fuente de disputa indudablemente, sobre todo al momento de interpretar la prohibición absoluta de censura que rige en el marco interamericano y aquel que hace referencia a las restricciones indirectas.³⁵

³⁴ UNESCO. (2023) *Directrices para la gobernanza de las plataformas digitales: salvaguardar la libertad de expresión y el acceso a la información con un enfoque de múltiples partes interesada*. Recuperado de: <https://unesdoc.unesco.org/ark:/48223/pf0000387360>.

³⁵ Del Campo, A., Zara N., y Alvarez Ugarte R., *Are Risks the New Rights: the perils of the risks approach in tech regulation, (forthcoming)* Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5161173.



ii. Privacidad

La privacidad, consagrada en el artículo 11 de la CADH, enfrenta nuevos desafíos en la era digital. Este derecho también está reconocido en el Pacto Internacional de Derechos Civiles y Políticos,³⁶ la Declaración Universal de Derechos Humanos,³⁷ y, a nivel comparado, en el artículo 8 del Convenio Europeo de Derechos Humanos³⁸.

La noción de vida privada *"engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior"*³⁹. La Corte Interamericana de Derechos Humanos, en el caso *Escher y otros vs. Brasil* (2009), señaló que *"el artículo 11 de la Convención prohíbe toda injerencia arbitraria o abusiva en la vida privada de las personas"*⁴⁰ así como que el derecho a la privacidad se extiende a la información digital.

El derecho a la privacidad según la Comisión Interamericana protege al menos cuatro bienes jurídicos: la libertad frente injerencias arbitrarias del Estado o de terceros; el derecho a la autonomía según el proyecto individual de vida de cada uno; el derecho a no difundir lo que en el espacio privado suceda, y la consiguiente prohibición de la divulgación o circulación de la información capturada, sin consentimiento del titular, en dicho espacio; y el derecho a la propia imagen.⁴¹ La Corte IDH sostuvo que el derecho a la privacidad *"incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás, y es una condición indispensable para el libre desarrollo de la personalidad"*⁴².

La privacidad es un derecho habilitante que sustenta el disfrute de otros derechos y el libre desarrollo de la personalidad y la identidad de las personas, y su capacidad para participar en la vida política, económica, social y cultural.

³⁶ Asamblea General de las Naciones Unidas (1966). *Pacto Internacional de Derechos Civiles y Políticos*. Treaty Series, vol. 999, p. 171, Recuperado de: <https://www.refworld.org/legal/agreements/unga/1966/en/17703>

³⁷ Asamblea General de las Naciones Unidas (1948), *Declaración Universal de los Derechos Humanos*, 217 A (III), Recuperado de: <https://www.refworld.org/legal/resolution/unga/1948/en/11563>.

³⁸ Consejo de Europa (1950), *Convenio Europeo de Derechos Humanos, modificado por los Protocolos Nos. 11, 14 y 15* (ETS No. 005, 4 de noviembre de 1950). Recuperado de: <https://www.refworld.org/legal/agreements/coe/1950/en/18688>: "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás"

³⁹ Corte Interamericana de Derechos Humanos (2012), *Artavia Murillo y otros ("Fecundación in vitro") vs. Costa Rica* (Serie C N. 257, párr. 143) Recuperado de: https://www.corteidh.or.cr/docs/casos/articulos/seriec_257_esp.pdf.

⁴⁰ Corte Interamericana de Derechos Humanos. (2009). *Caso Escher y otros vs. Brasil* (Serie C No. 200, párr. 113). Recuperado de https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_esp.pdf

⁴¹ Informe RELE, Internet y Derechos Humanos, 2013, Parr. 131, citando CIDH. Informe No. 82/10. Caso No. 12.524. Fontevecchia y D'Amico. Argentina. 13 de julio de 2010. Párr. 91 y ss. Corte IDH, *Artavia Murillo y otros vs. Costa Rica* (2012), párr. 143.

⁴² Corte Interamericana de Derechos Humanos (2012), *Artavia Murillo y otros ("Fecundación in vitro") vs. Costa Rica* (Serie C N. 257, párr. 143) Recuperado de: https://www.corteidh.or.cr/docs/casos/articulos/seriec_257_esp.pdf.



Así, *“las violaciones o transgresiones del derecho a la privacidad podían afectar al ejercicio de otros derechos humanos, como el derecho a la libertad de expresión y a abrigar opiniones sin injerencias, y el derecho a la libertad de reunión y asociación pacíficas”*⁴³. En particular, es importante resaltar que la privacidad es derecho esencial en una democracia, ya que permite a los individuos formar y expresar sus opiniones libremente, y participar en el debate público sin temor a represalias. Más aún, en el caso *Fontevicchia y D’Amicco vs. Argentina* la Corte estableció que *“el Estado tiene la obligación de garantizar el derecho a la vida privada mediante acciones positivas, lo cual puede implicar, en ciertos casos, la adopción de medidas dirigidas a asegurar dicho derecho protegiéndolo de las interferencias de las autoridades públicas, así como también de las personas o instituciones privadas, incluyendo los medios de comunicación.”*⁴⁴

La protección de datos personales hace parte del derecho a la privacidad y así ha sido abordado en los distintos documentos del SIDH que han abordado este tema, incluyendo el Comité Jurídico Interamericano (CJI) la Comisión y la Corte IDH. Por otra parte, la Asamblea General de la ONU, en su Resolución 68/167 sobre *“El derecho a la privacidad en la era digital”* (2014), enfatizó que *“los derechos de las personas, incluido el derecho a la privacidad, también deben estar protegidos en Internet”* y expresó su preocupación por *“los efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones, incluidas la vigilancia y la interceptación extraterritoriales de las comunicaciones y la recopilación de datos personales, en particular cuando se llevan a cabo a gran escala”*⁴⁵. La recopilación y procesamiento masivo de datos personales por parte de empresas tecnológicas y gobiernos plantea serios desafíos para el derecho a la privacidad.

El uso de tecnologías de vigilancia masiva por parte de los Estados, facilitadas por avances en inteligencia artificial y procesamiento de datos, pero también por el avance de tecnologías que permiten registrar e indexar incluso rasgos faciales en bases de datos configuradas, representa una amenaza significativa para la privacidad y para el ejercicio en general de todos los derechos humanos. Estas prácticas pueden tener un efecto inhibitor en el ejercicio de otros derechos fundamentales, como la libertad de expresión y asociación y plantea un desafío en el contexto de las medidas de seguridad y defensa nacional, donde los Estados muchas veces justifican la vigilancia como necesaria para la protección del orden público y la seguridad ciudadana.

La evolución de la tecnología, la innovación y la digitalización, por otro lado, dan lugar a nuevas actividades modelos empresariales y de negocios que dependen cada vez más del tratamiento de grandes volúmenes de datos personales en formas nuevas y complejas. Como señala un informe reciente de la Relatora de la ONU para la privacidad, *“determinados avances tecnológicos pueden plantear nuevos retos para la aplicación de las leyes de protección de datos y de la intimidad, así*

⁴³ Consejo de Derechos Humanos de la ONU (2017), Resolución 34/7. Recuperado de: https://ap.ohchr.org/documents/s/HRC/resolutions/A_HRC_RES_7_34.pdf

⁴⁴ Corte Interamericana de Derechos Humanos (2011). *Caso Fontevicchia y D’Amico vs. Argentina*. (Serie C No. 238. Parr. 49.) Recuperado de: https://www.corteidh.or.cr/docs/casos/articulos/seriec_238_esp.pdf

⁴⁵ Asamblea General de las Naciones Unidas (2013) *Resolución 68/167, “El derecho a la privacidad en la era digital”*. Recuperado de: <https://documents.un.org/doc/undoc/gen/n13/449/50/pdf/n1344950.pdf>



como causar significativos efectos perjudiciales, tales como proporcionar resultados discriminatorios y sesgados para las personas, o afectar a su capacidad de ejercer sus derechos a la protección de datos y privacidad⁴⁶. La datificación masiva de la vida cotidiana a través de plataformas digitales ha creado un ecosistema donde cada interacción genera datos que pueden ser recopilados, analizados, sistematizados, monetizados.⁴⁷ La escala y la profundidad de la recopilación de datos plantean preguntas fundamentales sobre el consentimiento informado y el control que los individuos tienen sobre su información personal.

A los problemas más tradicionales, como la vigilancia masiva o individualizada, pública o privada, se le suman complejidades propias de sistemas que se nutren de datos para generar nuevas interacciones capaces en sí mismas de afectar o promover el ejercicio de derechos humanos. Este es el caso de los análisis de *big data* y de Inteligencia artificial y sistemas de *machine learning*. El acceso a grandes cantidades de datos es lo que en definitiva permite el desarrollo de estas tecnologías, equitativamente distribuidas en el mundo.⁴⁸ En este esquema empiezan a plantearse ciertas paradojas: cuanto menos estrictas las leyes de protección de datos personales, más capacidad de innovación y desarrollo de tecnologías de IA y menos protecciones frente a posibles violaciones al derecho a la privacidad. En la contracara, a mayor restricción en las leyes de datos personales, más se encarecen los proyectos de desarrollo de este tipo de tecnologías, generando desigualdades en torno a su acceso, menos incentivos para sortear posibles vacíos en los datos de alimentación de estas tecnologías, que a su vez derivan en discriminación, estigmatizaciones, generalizaciones y exclusión.

Por otro lado, estos sistemas permiten inferir información sensible a partir de datos aparentemente inocuos. El Principio 3 de los Principios Interamericanos en materia de neurociencias, neurotecnologías y derechos humanos del CJI destacan los datos neuronales como datos personalísimos. Y el Principio 4 identifica claramente la necesidad de encuadrar el tratamiento neuronal en el marco del consentimiento informado provisto en la teoría de datos personales. Dependiendo de sus usos y aplicaciones, estas tecnologías pueden revelar, predecir, inferir o incluso a partir de la información, incidir, en la orientación sexual, las opiniones políticas, el estado de salud o el comportamiento futuro de una persona sin su conocimiento o consentimiento explícito.

El reconocimiento y la ampliación de lo que puede considerarse un dato personalísimo en la era digital resulta importante, sobre todo atendiendo a la necesidad, que en muchos países de la región se hace evidente, de adoptar o actualizar las leyes de datos personales existentes. Como bien argumenta Hineostroza-Arenas en su ensayo, puede haber nuevos aspectos a tratar en el desarrollo de derechos bajo las nuevas tecnologías, pero es fundamental construir sobre la base normativa vigente. Lo contrario amenaza la vigencia de los derechos ya reconocidos y reabre la negociación en torno a su alcance o definición.

⁴⁶ Consejo de Derechos Humanos de la ONU (2023), *Informe de la Relatora Especial sobre el derecho a la privacidad*, Ana Brian Nougères, Mecanismos legales de salvaguarda para la protección de datos personales y la privacidad en la era digital, A/HRC/55/46, párr. 9, Recuperado de: <https://docs.un.org/en/A/HRC/55/46>

⁴⁷ Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.

⁴⁸ Órgano Asesor de Alto Nivel sobre Inteligencia Artificial de las Naciones Unidas (2024), *Gobernanza de la Inteligencia Artificial en beneficio de la Humanidad: Informe final*. Recuperado de: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf.



Si bien es cierto que todas las interacciones en Internet y las nuevas tecnologías generan datos y utilizan datos, la mera protección y regulación del uso de datos personales no agota los análisis necesarios en materia de derechos para lograr un desarrollo tecnológico respetuoso de los derechos humanos. La lógica de la protección de datos es una lógica en mayor o menor medida de derecho privado, atendiendo a los datos personales desde la perspectiva de la voluntad, la propiedad y el consentimiento. Esta lógica es limitada para abordar cuestiones de interés público e incluso puede ser limitada para procurar un balance adecuado y proporcionado en el ejercicio de derechos. Como sostienen Botero y De Brieger, la datificación de la discusión jurídica puede desnaturalizar las problemáticas más complejas que trae el desarrollo tecnológico y sus variados usos por parte del sector público y privado.

Sobre biometría, por ejemplo, los autores argumentan que *“Esta concepción del rostro como un dato y, por extensión, de los datos biométricos como idénticos a otros datos sensibles, no solo deshumaniza nuestro rasgo identitario por excelencia convirtiéndolo en una moneda transable y asociándolo de la persona dueña de ese rostro, sino que circunscribe la cuestión sobre los límites que deberían imponerse a esta tecnología al dominio de la protección de datos personales. En este caso, como en muchos otros en que las implicaciones sociales de la datificación son particularmente apremiantes, la concepción legalista es insuficiente para comprender el fenómeno y para protegernos efectivamente de sus consecuencias negativas, pues las categorías de la ley no son capaces de captar la realidad con todos sus matices e implicaciones.”*⁴⁹ La integración de tecnologías biométricas en sistemas de identificación y autenticación plantea nuevos riesgos para la privacidad. La recopilación y almacenamiento de datos biométricos, que son únicos e inmutables, aumenta el riesgo de robo de identidad y uso indebido de información personal. El CJI ha expresado preocupación por estos riesgos⁵⁰. Por ejemplo, la implementación de cámaras equipadas con tecnología de reconocimiento facial en tiempo real permite el seguimiento y etiquetado de individuos, lo que otorga a las autoridades la capacidad de mantener registros detallados de los movimientos de un gran número de personas, posiblemente categorizándolas según diversas características.⁵¹

La responsabilidad de los Estados frente al derecho a la privacidad y a la protección de datos en la era digital supone, además de abstenerse de violar estos derechos y de respetarlos, la necesaria inclusión de medidas positivas para el disfrute efectivo de estos. Esto implica no solo la creación de marcos legales adecuados, sino también la implementación de políticas y prácticas que protejan la privacidad.⁵²

⁴⁹ Botero, C y De Brigard, J. (2023). “Sonría, Ud está siendo filmado”, anexo 3.

⁵⁰ Organización de Estados Americanos (OEA), Comité Jurídico Interamericano (2021), *Principios actualizados sobre la privacidad y la protección de datos personales*, (CJI/RES. 266, 2021), Recuperado de: https://www.oas.org/es/sla/cji/docs/CJI-RES_266_ESP.pdf

⁵¹ Consejo de Derechos Humanos de la ONU. (2019). Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión (A/HRC/41/35, párr. 12), Recuperado de: <https://digitallibrary.un.org/record/3814512?ln=en>

⁵² Comité Jurídico Interamericano (2023), *Declaración de Principios Interamericanos en Materia de Neurociencias, Neurotecnologías y Derechos Humanos*, (CJI/RES. 281 (CII-O/23) corr.1, 9 de marzo de 2023). Recuperado de: https://www.oas.org/es/sla/cji/docs/CJI-RES_281_CII-O-23_corr1_ESP.pdf.



En el marco del desarrollo del derecho a la privacidad en el SIA se han adoptado estándares puntuales para proteger al individuo frente a injerencias directas del estado. Entre ellas, la necesidad de que cualquier injerencia esté contemplada en la ley sea proporcionada y necesaria. La vigilancia masiva es en general considerada desproporcionada y si bien en algunos casos puede estar justificada, las medidas tienen que cumplir con estándares de proporcionalidad, ser evaluadas en el tiempo para determinar su continua necesidad y no afectar desproporcionadamente otros derechos, incluyendo el derecho al anonimato, a la asociación y reunión, y a la libertad de expresión.

Las medidas que se adoptaren para la vigilancia individual de la persona han de estar sujetas a control judicial, garantizando el debido proceso y las garantías del juez natural, independiente e imparcial, y el derecho al recurso. El derecho de defensa en juicio supone además el derecho a ser notificado de las medidas que se adopten respecto de uno y su privacidad, salvo en ciertas excepciones que deben interpretarse de manera restrictiva y superar el test de necesidad y proporcionalidad. Estos estándares permiten a priori, construir pisos mínimos, incluso para tecnologías emergentes, cuando estas sean utilizadas por el propio estado. Pero incluso respecto del deber de garantía, también establece criterios básicos que la regulación ha de seguir, incluyendo obligaciones de comunicación y transparencia, protección de datos personales y derechos de acceso, rectificación, cancelación y oposición cuando corresponda. Además, permiten inferir ciertas obligaciones y potestades del estado respecto del sector privado. Por un lado, los estados deben permitir la comunicación al usuario cuando sus datos sean requeridos por parte de este y pueden exigir a las empresas del sector privado que notifiquen expresamente en qué casos se están registrando datos, como se sistematizan, para qué fines, y cuando tengan incidentes de seguridad sobre las bases de datos que puedan comprometer su seguridad o privacidad.

iii. Igualdad y no discriminación

La igualdad y no discriminación son principios fundamentales del derecho internacional de los derechos humanos. Los artículos 1.1 y 24 de la Convención Americana establecen los derechos a la igualdad y no discriminación. El artículo 1.1. establece la obligación de respetar y garantizar el ejercicio de derechos humanos *"sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social."*⁵³ Y el artículo 24 establece *"Todas las personas son iguales ante la ley. En consecuencia, tienen derecho, sin discriminación, a igual protección de la ley."*⁵⁴ La Corte Interamericana además sostuvo que cada uno de los derechos contenidos en la Convención han de respetarse y garantizarse sin discriminación alguna.⁵⁵ La obligación de respeto supone que el Estado no discrimine ni directa ni indirectamente; y la de garantía supone que adopte

⁵³ Organización de los Estados Americanos (OEA) (1969) *Convención Americana sobre Derechos Humanos*, artículo 1.1. Recuperado de: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf

⁵⁴ *Ibidem*, artículo 24.

⁵⁵ Corte IDH, *Caso Apitz Barbera y otros ("Corte Primera de lo Contencioso Administrativo") vs. Venezuela*, Sentencia de 5 de agosto de 2008, Excepción Preliminar, Fondo, Reparaciones y Costas, Serie C No. 182, párr. 209.



medidas para proteger a las personas bajo su jurisdicción de discriminaciones arbitrarias.⁵⁶ Además, la obligación supone la adopción proactiva de medidas para subsanar situaciones de discriminación preexistentes.⁵⁷

En este sentido, la adopción de sistemas de inteligencia artificial en ámbitos como la educación, el trabajo, y el acceso a servicios públicos puede profundizar desigualdades estructurales y generar nuevas formas de exclusión social. Por ejemplo, algoritmos de selección automatizada pueden discriminar indirectamente a personas por motivos de género, raza o situación socioeconómica, afectando el derecho al trabajo y a la educación en condiciones de igualdad. Asimismo, la brecha digital y la falta de acceso a tecnologías emergentes limitan el ejercicio efectivo de los DESCAs, especialmente en comunidades rurales, indígenas o en situación de vulnerabilidad. Los Estados deben adoptar medidas proactivas para garantizar que el desarrollo y despliegue de la IA no perpetúe ni amplifique discriminaciones históricas y que contribuya a la realización progresiva de los derechos económicos, sociales, culturales y ambientales.

Por otra parte, la RELE sostuvo en su Informe Principios para una Internet libre, abierta e inclusiva (2016) que *“Los derechos a la igualdad y no discriminación informan tanto los principios rectores que han de orientar la política pública en materia de internet como cada uno de los derechos humanos descritos en el presente informe. La obligación de garantía de los distintos derechos requerirá en su caso la adopción de medidas positivas específicas a la luz de las exigencias de cada uno de los derechos.”*⁵⁸

En materia de tecnología, tanto la RELE como otros organismos internacionales sostienen desde hace años la necesidad de proteger y garantizar los derechos a la no discriminación y la igualdad en el acceso a la tecnología y en el ejercicio de derechos humanos a través de medios tecnológicos, como Internet. La RELE sostiene que *“La obligación de igualdad y no discriminación también implica la obligación del Estado de garantizar a las personas el ejercicio de los derechos humanos en internet en condiciones de igualdad. Los artículos 1.1 y 24 rigen tanto “online” como “offline” y las personas tienen derecho a ejercer sus derechos de reunión, asociación, libertad de expresión, acceso a la información, libertad de religión, entre otros, sin discriminación. Internet constituye una herramienta esencial para que las comunidades vulnerables o históricamente discriminadas obtengan información, expongan sus agravios, hagan oír sus voces y participen activamente en el debate público y contribuyan en la construcción de políticas públicas tendientes a revertir su situación.”*⁵⁹ Y la Convención sobre los Derechos de las Personas con Discapacidad (CDPD) establece *“los Estados Partes adoptarán medidas pertinentes para asegurar el acceso de las personas con discapacidad,*

⁵⁶ Corte IDH, *Caso Yatama vs. Nicaragua*, Sentencia de 23 de junio de 2005, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C No. 127.

⁵⁷ CIDH, Informe Anual 2008, Informe de la Relatoría Especial para la Libertad de Expresión, Capítulo III (Marco Jurídico Interamericano del Derecho a la Libertad de Expresión), OEA/Ser. L/V/II.134. Doc 5 rev. 1 (25 de febrero de 2009), Párr. 230, disponible en: <http://www.cidh.oas.org/annualrep/2008sp/indice2008.htm>

⁵⁸ Relatoría Especial para la Libertad de Expresión (RELE) (2016), *Estándares para una Internet libre, abierta e incluyente*, Recuperado de: https://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf.

⁵⁹ *Ibidem*.



en igualdad de condiciones con las demás, [a] la información y las comunicaciones, incluidos los sistemas y las tecnologías de la información y las comunicaciones⁶⁰ [...] incluso mediante internet.⁶¹ [Y] “[p]romover el diseño, el desarrollo, la producción y la distribución de sistemas y tecnologías de la información y las comunicaciones accesibles en una etapa temprana, a fin de que estos sistemas y tecnologías sean accesibles al menor costo”.⁶²

Aunque las tecnologías emergentes tienen el potencial de promover la igualdad en algunos aspectos, también pueden reforzar y amplificar los sesgos sociales existentes, perpetuando la discriminación⁶³. Las desigualdades en el acceso a Internet y a las tecnologías digitales pueden exacerbar las disparidades existentes en el ejercicio de los derechos humanos online. El Relator Especial sobre libertad de opinión y de expresión ha enfatizado que los Estados tienen la obligación positiva de promover o facilitar el derecho a la libertad de expresión y los medios necesarios para ejercer este derecho, lo que incluye Internet.⁶⁴

En materia de políticas de acceso a Internet u a otras tecnologías, la Comisión sostuvo que *“La garantía de no discriminación incluye la obligación estatal de atender a las necesidades específicas de acceso a internet que puedan tener algunos grupos particularmente vulnerables. La Relatoría Especial sostuvo que “deben ser establecidos mecanismos regulatorios –que contemplen regímenes de precios, requisitos de servicio universal y acuerdos de licencia para fomentar un acceso amplio a Internet, incluyendo a los sectores vulnerables y las zonas rurales más alejadas. Para tales efectos, deben ser realizados todos los esfuerzos necesarios para brindar apoyo directo para facilitar el acceso, a través, por ejemplo, como se ha mencionado, de programas de distribución de computadoras asequibles y de la creación de centros comunitarios de tecnologías de la información y otros puntos de acceso público”⁶⁵* En la misma línea, más adelante el informe aborda la necesidad de combatir la discriminación contra las mujeres y niños, niñas y adolescentes, personas con discapacidad, y personas históricamente excluidas o vulnerables y adoptar medidas concretas para evitarlo. El Pacto del Futuro y el Pacto Digital global destacan la necesidad y el compromiso de los estados firmantes de trabajar para acortar la brecha digital y así promover los objetivos del desarrollo sustentable.⁶⁶ La desigualdad en el acceso a Internet y ahora en el acceso⁶⁷ y el desarrollo de tecnologías emergentes plantea desafíos importantes para acortar dicha brecha, amenazan la paz y la estabilidad global.⁶⁸

⁶⁰ Convención sobre los Derechos de las Personas con Discapacidad, Artículo 9.1, disponible en: <http://www.un.org/esa/socdev/enable/documents/tccconvs.pdf>

⁶¹ Convención sobre los Derechos de las Personas con Discapacidad, Artículo 21, disponible en: <http://www.un.org/esa/socdev/enable/documents/tccconvs.pdf>

⁶² Convención sobre los Derechos de las Personas con Discapacidad, Artículo 9, disponible en: <http://www.un.org/esa/socdev/enable/documents/tccconvs.pdf>

⁶³ Geneva International Center for Justice, *Digital Rights: The Impact of AI and Emerging Technologies on Human Rights*, 17 de junio de 2024.

⁶⁴ ONU, *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, 2017.

⁶⁵ Relatoría Especial para la Libertad de Expresión (RELE) (2016), *Estándares para una Internet libre, abierta e incluyente*, Recuperado de: https://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf.

⁶⁶ ONU, El Pacto del Futuro, Resolución aprobada por la Asamblea General el 22 de septiembre de 2024, A/RES/79/1, 22 de septiembre de 2024, Anexo Pacto Digital para el Futuro, disponible en <https://documents.un.org/doc/undoc/gen/n24/272/25/pdf/n2427225.pdf>.

⁶⁷ ONU, El Pacto del Futuro, Resolución aprobada por la Asamblea General el 22 de septiembre de 2024, A/RES/79/1, 22 de septiembre de 2024, Anexo Pacto Digital para el Futuro, disponible en <https://documents.un.org/doc/undoc/gen/n24/272/25/pdf/n2427225.pdf>.

⁶⁸ Gobernanza de la IA en Beneficio de la Humanidad, Órgano Asesor de Alto Nivel de Naciones Unidas sobre IA (2024), pag. 9 https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf.



Por otro lado, el despliegue de tecnologías emergentes experimentales ha demostrado que pueden tener un impacto en la educación, la cultura, el trabajo, el acceso al ejercicio de goce de derechos humanos y de otros derechos. *“A pesar de la sensación generalizada de que las tecnologías digitales emergentes son neutrales y objetivas en su funcionamiento, la raza y el origen étnico determinan el acceso a los derechos humanos y su disfrute en todos los campos en los que estas tecnologías están actualmente generalizadas”*⁶⁹ Como destaca el CJI, las neurotecnologías, aplicadas sin controles y límites necesarios suponen un riesgo, sobre todo, para niños, niñas y adolescente, incapaces y otros grupos vulnerables.

Los sistemas de IA y aprendizaje automático pueden perpetuar o exacerbar patrones de discriminación existentes, contribuyendo a fenómenos como los discursos de odio y la desinformación. La inteligencia artificial aplicada a la biometría también está atravesada por factores que contribuyen a la discriminación y el prejuicio. La IA se nutre de datos disponibles, en muchos casos dispares respecto de la representatividad de estos en distintos grupos poblacionales. El creciente empleo de sistemas de reconocimiento facial y tecnologías de vigilancia para monitorear y gestionar grupos poblacionales específicos ha generado una serie de preocupaciones significativas en el ámbito de los derechos humanos, incluyendo el derecho a la privacidad, la libertad de reunión pacífica y asociación, la libertad de expresión y la libertad de circulación.⁷⁰ La creación automatizada o no de perfiles personales que la tecnología biométrica permite puede en muchos casos desproporcionadamente acentuar sesgos raciales, de género, o religiosos que impacten el ejercicio y promoción de los derechos humanos.⁷¹

Los impactos concretos, sin embargo, dependen en muchos casos de los usos que de dichas tecnologías se haga y de quien haga uso de esta. Así, no es lo mismo el uso estatal de biometría e IA en el espacio público por parte de agentes policiales, situación que describen Botero y De Brigard, que la aplicación de IA a la toma de decisiones judiciales o la toma de decisiones en torno a beneficio de la seguridad social. El Comité para la Eliminación de la Discriminación de la ONU ha señalado que *“existe un riesgo real de sesgo algorítmico cuando se utiliza la inteligencia artificial en la adopción de decisiones en el contexto de la aplicación de la ley. La elaboración de perfiles algorítmicos plantea serias preocupaciones y las consecuencias con respecto a los derechos de las víctimas podrían ser muy graves”*⁷².

Desde el sector privado también existen usos problemáticos que otros en esta materia y pueden afectar el derecho a la libertad de expresión, la cultura, la educación, el trabajo, etc.⁷³. Como señala el mencionado informe de la Relatora de ONU sobre las formas contemporáneas de racismo,

⁶⁹ ONU, *Informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, La discriminación racial y las tecnologías digitales emergentes: un análisis de los derechos humanos*, A/HRC/44/57, 2020, párr. 5.

⁷⁰ ONU, Comité para la Eliminación de la Discriminación Racial (CERD), Recomendación General No. 36 (2020), párr. 35.

⁷¹ El Comité para la Eliminación de la discriminación racial ha reconocido que grupos específicos, como los migrantes, los refugiados y los solicitantes de asilo, las personas afrodescendientes, los pueblos indígenas y las minorías nacionales y étnicas son los más vulnerables a la elaboración de perfiles raciales. CERD/C/CAN/CO/21-23, párrs. 15 y 16 a) a d); y CERD/C/ITA/CO/19-20, párrs. 27 y 28

⁷² ONU, Comité para la Eliminación de la Discriminación Racial (CERD), Recomendación General No. 36 (2020), párr. 12.

⁷³ ONU, A/HRC/41/35, párr. 12.



discriminación racial, xenofobia y formas conexas de intolerancia, *“La tecnología nunca es neutra, pues refleja los valores e intereses de quienes influyen en su diseño y uso, y está fundamentalmente conformada por las mismas estructuras de desigualdad que operan en la sociedad”* (A/HRC/44/57, párr. 7). El desarrollo tecnológico viene promovido principalmente desde un sector privado pujante, concentrado en países desarrollados en general.⁷⁴ Estos desarrollos son desplegados a veces en plataformas de información y conocimiento, como redes sociales, buscadores o juegos en Internet, otras veces destinados a otro tipo de implementaciones, científicas, educativas, en materia de salud, finanzas, sistema bancario, etc. incluso muchas veces el sector privado es prestador de servicios del propio estado. El diseño de estas tecnologías también entonces ha de estar atento a determinados estándares de derechos humanos. Se ha señalado que *“si el sesgo está implícito en las decisiones de diseño, un algoritmo puede contribuir a obtener resultados sesgados, aunque los datos introducidos en el algoritmo sean perfectamente representativos”*⁷⁵

Por ejemplo, en un Reporte del NIST de 2019 se afirma que la precisión de las herramientas de software de reconocimiento facial para identificar a personas de diferentes sexos, edades y antecedentes raciales depende del algoritmo que se encuentra en el núcleo del sistema, la aplicación que lo utiliza y los datos que procesa⁷⁶. En el reporte se destaca que, si bien los algoritmos de reconocimiento facial son cada vez más certeros y que no es posible hacer afirmaciones generales, algunos de éstos presentaron diferencias demográficas⁷⁷. Algunos ejemplos son mayores falsos positivos en asiáticos, afroamericanos, nativos americanos y mujeres⁷⁸.

Los estándares interamericanos ya sugieren que el análisis ha de ser holístico y los derechos a la igualdad y no discriminación han de ser evaluados en relación con otros, como el derecho de acceso a la justicia (Artículo 25 CADH), el derecho al debido proceso (Artículo 8 CADH), el derecho a la integridad y la libertad (Artículo 5 y 9 CADH), etc. Los Estados deben tomar todas las medidas apropiadas para garantizar la transparencia respecto del uso de sistemas de perfilado algorítmico, o incluso de neuro tecnologías. Esto incluye la divulgación pública del uso de tales sistemas y explicaciones significativas sobre cómo funcionan, los conjuntos de datos que se utilizan y las medidas implementadas para abordar los riesgos que la implementación de estas tecnologías supone para el ejercicio de derechos humanos sin discriminación⁷⁹.

Estos estándares obligan a los estados también a adecuar la legislación y verificar su implementación para evitar no solo leyes discriminatorias sino también impactos discriminatorios de prácticas, políticas o regulaciones estatales. Las obligaciones de garantía que el estado tiene en materia de

⁷⁴ Gobernanza de la IA en Beneficio de la Humanidad, Órgano Asesor de Alto Nivel de Naciones Unidas sobre IA (2024), pag. 9 https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_es.pdf.

⁷⁵ ONU, *Informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, Formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia*, A/HRC/56/68, párr. 17

⁷⁶ National Institute of Standards and Technology, U.S. Department of Commerce, 2019, <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

⁷⁷ Diferencia demográfica se refiere a que la capacidad de un algoritmo para emparejar dos imágenes de la misma persona varía entre diferentes grupos demográficos.

⁷⁸ CERD/C/MUS/CO/20-23 y Corr.1, párr. 20; y CERD/C/RUS/CO/23-24, párrs. 15 b) y 16 c);

⁷⁹ ONU, Comité para la Eliminación de la Discriminación Racial (CERD) (2020), Recomendación General No. 36, párr. 61.



derechos humanos permiten afirmar que puede hacer exigibles determinadas obligaciones por parte del sector privado e incluso limitar el despliegue de ciertas tecnologías en espacios o para usos especialmente sensibles para el abuso de derechos humanos. Y el acceso a la justicia cuando alguno de estos derechos se vea vulnerado.

iv. Debido Proceso y Acceso a Justicia

Los artículos 8 y 25⁸⁰ de la Convención Americana consagran el derecho de toda persona al debido proceso y acceso a justicia. El artículo 8 establece una serie de garantías aplicables tanto a los procesos judiciales en general como a los procesos penales en particular atendiendo a la vulnerabilidad del acusado frente al poder punitivo del Estado.⁸¹ El artículo no solo impacta sobre procesos eminentemente judiciales sino sobre todos los órganos del Estado que “ejercen funciones de naturaleza materialmente jurisdiccional[...] pese a que el artículo 8.1 de la Convención alude al derecho de toda persona a ser oída por un “juez o tribunal competente” para la “determinación de sus derechos”, dicho artículo es igualmente aplicable a las situaciones en que alguna autoridad pública, no judicial, dicte resoluciones que afecten la determinación de tales derechos.”⁸²

Las medidas estatales que restrinjan derechos han de estar precedidas por autorización judicial conforme a las garantías de debido proceso y cuando por motivos excepcionales dicho control no pueda realizarse a priori, han de ser luego evaluadas posteriormente por una autoridad judicial competente.

El debido proceso incluye garantías fundamentales como el derecho a ser oído en un plazo razonable por un juez competente, independiente e imparcial, establecido con anterioridad por la ley⁸³, el derecho a la defensa, a la presunción de inocencia, a ser informado y participar activamente del proceso, a contar con abogado o defenderse por sí mismo, a contar con traductor, y a apelar la decisión judicial. Además, exige que las resoluciones sean motivadas, lo que contribuye tanto a la legitimidad y transparencia de la actuación estatal como a la protección frente a la arbitrariedad y la ilegalidad.⁸⁴

Ese derecho se intersecta con otros derechos fundamentales, como el de igualdad y no discriminación, y el derecho a la privacidad. Las violaciones a este último pueden impactar directamente en las garantías de debido proceso, sobre todo a medida que los procesos van incorporando desde la etapa de prevención e investigación misma desde el Estado, distintas tecnologías emergentes como

⁸⁰ Organización de los Estados Americanos (OEA) (1969) *Convención Americana sobre Derechos Humanos*, artículos 8 y 25. Recuperado de: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf.

⁸¹ Medina Quiroga, C. (2005), *La Convención Americana, teoría y jurisprudencia. Vida, integridad personal, libertad personal, debido proceso y recurso judicial*. Recuperado de: <https://www.corteidh.or.cr/tablas/23072.pdf>

⁸² Corte IDH (2001), *Caso Ivcher Bronstein Vs. Perú. Sentencia de Reparaciones y Costas*. Serie C N. 74 parr. 105 y 106. Recuperado de: https://www.corteidh.or.cr/docs/casos/articulos/Seriec_74_esp.pdf

⁸³ Organización de los Estados Americanos (OEA) (1969) *Convención Americana sobre Derechos Humanos*, artículo 8.1. Recuperado de: https://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf

⁸⁴ Ibañez Rivas, J.M. (2014), *Artículo 8, Garantías Judiciales*, en *Convención Americana sobre Derechos Humanos, Comentario*, Ed.Eudeba. .



la biometría, la IA o las neurociencias. La preocupación, sin embargo, no es nueva. En 2016 la Electronic Frontier Foundation (EFF) realizó un estudio en seis países de América Latina analizando y evaluando el régimen de vigilancia estatal y la tecnología y su impacto en los derechos fundamentales. En ese momento, se prestaba especial atención al acceso estatal a datos de acceso, conexión, metadatos, registros electrónicos, así como a los requisitos que el Estado debía cumplir para acceder a dicho acceso.⁸⁵ En América Latina la mayoría de las jurisdicciones estudiadas requieren autorización judicial previo a la adopción de medidas de vigilancia estatal y control judicial en torno a su duración y procedencia. Sin embargo, un problema recurrente y común en todo el continente versaba en torno a la opacidad de los mecanismos estatales de vigilancia, la falta de controles adecuados para garantizar el control judicial y la falta de transparencia en torno a estas medidas, particularmente en materia de inteligencia, aunque también en materia de investigación penal.⁸⁶

La proliferación del uso de tecnologías emergentes en procesos judiciales y administrativos supone importantes desafíos para la garantía de debido proceso tanto en los procesos de investigación como en los procesos de prueba. Por ejemplo, el uso de IA en biometría o vigilancia masiva es per se problemática; de la misma manera el uso de biometría en el espacio público supone importantes desafíos para la presunción de inocencia que ha de regir la actuación estatal. Tanto Aguerre como De Brigard y Botero destacan algunos de los problemas que estos usos pueden generar.

El uso de biometría en el espacio público fue motivo de litigio en algunas ciudades. Este es el caso de la Ciudad de Buenos Aires, donde el Observatorio de Derecho Informático (ODIA) y luego el Centro de Estudios Legales y Sociales (CELS) argumentaron que el uso del sistema de biometría en la ciudad afectaba los derechos a la privacidad, igualdad y no discriminación y presunción de inocencia. Además, carecía de los controles suficientes para regular su uso conforme a derecho. La Cámara de Apelaciones de la Ciudad confirmó en abril de 2023 la suspensión del uso de este sistema hasta tanto se establecieran los mecanismos adecuados de control y se diera publicidad suficiente sobre el funcionamiento del sistema.⁸⁷ En la misma medida el uso de neurotecnologías en el proceso penal puede atentar contra el derecho a no autoincriminarse o declarar contra uno mismo.

La implementación de sistemas de IA en la administración pública, por ejemplo, en la asignación de beneficios sociales, subsidios o recursos educativos, puede dar lugar a exclusiones arbitrarias o errores sistemáticos que afecten el derecho a la seguridad social, la educación y el combate a la pobreza. Para ello, los Estados deben garantizar mecanismos efectivos de transparencia, revisión y aplicación en los procesos automatizados que impactan los DESCAs, asegurando el acceso a la justicia y reparación frente a posibles vulneraciones de derechos.

La adopción de tecnologías emergentes, como la IA en distintas facetas de la actividad procesal puede por supuesto traer beneficios en materia de acceso a la justicia y a garantizar el derecho a ser

⁸⁵ Electronic Frontier Foundation (EFF) (2016). Unlinking Eyes, the state of government surveillance in Latin America. Recuperado de: <https://www.eff.org/deeplinks/2016/10/unblinking-eyes-latinamerica-surveillance>.

⁸⁶ Ibidem.

⁸⁷ Centro de Estudios Legales y Sociales (CELS) (2023). Confirman la inconstitucionalidad del uso del sistema de reconocimiento facial. Recuperado de: <https://www.cels.org.ar/web/2023/04/confirman-la-inconstitucionalidad-del-uso-del-sistema-de-reconocimiento-facial/>



oído en un plazo razonable. Este argumento, que ha sido utilizado en los países que han adoptado o fomentan la adopción del uso de inteligencia artificial en distintos momentos de la actividad jurisdiccional, es indudablemente importante. Al fin y al cabo, justicia retardada es justicia denegada. Sin embargo, el uso de estas tecnologías ha de ser instrumental y no determinante en el resultado. En la elaboración de políticas públicas y normativas para la adopción de tecnologías emergentes, estos puntos fundamentales requieren de extenso debate público y transparencia a fin de procurar que en la determinación de estas no primen una lógica de suma cero donde la eficiencia y la oportunidad sean opuestas a la protección de garantías fundamentales. O donde la lógica implique el sacrificio de unas en pos de las otras. En todos los casos, sin embargo, conforme los estándares interamericanos de debido proceso y acceso a la justicia, el uso de herramientas tecnológicas en el proceso judicial ha de ser transparente, sujeto a control suficiente, y respetuoso de los derechos de las partes en los distintos procesos. Además, en todos los casos las decisiones surgidas de los tribunales y órganos determinantes de derechos han de estar suficientemente motivadas y pasibles de apelación.



CONCLUSIÓN



El desarrollo de tecnologías emergentes ofrece oportunidades significativas para el progreso en áreas como la ciencia, el conocimiento, la cultura, el trabajo, y otras disciplinas fundamentales de la vida cotidiana. El acceso a estas tecnologías es fundamental para el cumplimiento de los Objetivos de Desarrollo Sostenible de Naciones Unidas (ODS). Dado su potencial transformador estas tecnologías requieren atención de todos los sectores. En ese contexto, han proliferado documentos, guías, declaraciones y principios que buscan regular su desarrollo tanto a nivel local, comparado e internacional. Sin perjuicio de ello, también traen consigo desafíos. En algunos casos amplifican o perpetúan problemas preexistentes; en otros generan nuevos retos derivados por la propia expansión de las fronteras tecnológicas.

El avance científico y tecnológico viene necesariamente acompañado de consideraciones éticas, políticas, sociales, económicas, y también de regulaciones jurídicas. Uno de los elementos comunes en muchos de los documentos que actualmente circulan en torno al desarrollo tecnológico es que confluyen en ellos consideraciones de naturalezas distintas. Si bien todas ellas son necesarias, pertenecen en muchos casos a órbitas distintas de la sociedad y les corresponde a distintas instituciones, públicas, privadas y mixtas sentar reglas claras para su desarrollo, despliegue y monitoreo. El diálogo entre estos actores es imprescindible para garantizar un marco normativo coherente. Los sistemas universales y regionales de derechos humanos destacan que cualquier limitación a estos derechos sean conforme al principio de legalidad, necesidad y proporcionalidad. La misma norma obliga a los Estados a establecer normas claras respecto de aquellas medidas que tengan un impacto en los derechos humanos, sea en materia de acceso a tecnologías o al desarrollo y ejercicio de derechos humanos a través de ciertas tecnologías.

La proliferación de instrumentos regulatorios a nivel global trae consigo cierto nivel de certezas, pero también grandes desafíos interpretativos. Por ejemplo, el Órgano Asesor de Naciones Unidas sobre IA concluía en su informe final que:

“En la actualidad hay un gran déficit de gobernanza global de la IA. A pesar de los numerosos debates sobre ética y principios, el mosaico de normas e instituciones es aún incipiente y está lleno de lagunas. La rendición de cuentas suele brillar por su ausencia, en particular cuando se despliegan sistemas de IA que son difícilmente explicables y que afectan a los demás. El cumplimiento suele basarse en la voluntad; la práctica desmiente el discurso.”

No faltaron críticas al informe final de este grupo de expertos, por la vaguedad de sus recomendaciones en algunos casos, por lo ambicioso de su propuesta y por la aproximación holística a un tipo



de tecnología específico, en su caso a la IA. Como en muchos otros temas, aparecen en este Informe ciertas referencias a la excepcionalidad de los riesgos generados por estas tecnologías y cierta falta de granularidad en cuanto a las necesidades propias de la gobernanza de estas tecnologías de acuerdo con sus usos, sus actores y sus beneficiarios. Sin embargo, el Informe, en línea con muchos otros, sí destaca la necesidad de construir estándares de gobernanza desde el marco existente de derechos humanos.

Este artículo está centrado en el potencial del marco jurídico interamericano para abordar los desafíos más grandes que las tecnologías emergentes plantean a los derechos reconocidos a las personas. Una primera conclusión del análisis realizado es que las herramientas que el SIDH propone son jurídicas, por lo menos para todos los Estados que reconocen al derecho internacional de los derechos humanos como parte integral de sus sistemas nacionales. Este es el caso de la mayoría de los países de América Latina que han incluido en sus textos legales y/o constitucionales los enunciados de los principales tratados internacionales en la materia. Una segunda conclusión quizás obvia es que las obligaciones generadas en los marcos de derechos humanos impactan primera y directamente al Estado, e indirecta o secundariamente al sector privado. Son los Estados los llamados a ser garantes de los derechos humanos conforme a los artículos 1 y 2 de la CADH. Ello sin perjuicio del reconocimiento que algunos Estados hacen de la transversalidad y horizontalidad del derecho internacional de los derechos humanos, haciéndolos exigibles incluso en el ámbito privado, que en última instancia depende de cada jurisdicción y de la vigencia de sistemas e instituciones que así lo reconozcan y hagan exigibles.

El carácter vinculante o no del derecho internacional de derechos humanos sobre las empresas siguen siendo objeto de discusión doctrinaria. Los PRNU adoptados en 2011 son un ejemplo clave en este sentido. Asimismo, esfuerzos recientes, como la Digital Service Act (DSA) europea, han buscado incorporar algunas obligaciones empresariales relacionadas con derechos humanos a sus marcos legales.

Una segunda conclusión que permite este ensayo es que los regímenes son distintos dependiendo de quien desarrolle, despliegue y haga uso de la tecnología. Y también pueden ser distintos de acuerdo con los usos que a los que la tecnología se afecte. De esta manera, la neurotecnología dedicada al desarrollo de medios de comunicación para personas con dificultades neurológicas no tiene las mismas reglas jurídicas que el despliegue de neurotecnologías al servicio de la rehabilitación de presos o la educación pública. Las obligaciones son distintas, los actores son distintos, las relaciones generadas son distintas y se rigen por distintas ramas del derecho e implican afectaciones a derechos humanos distintos también. En la misma línea, no es lo mismo la biometría desplegada para controlar o monitorear manifestaciones públicas que la biometría implementada por el club barrial para verificar la membresía.

El SIDH establece límites claros respecto de los usos y procesos que los propios Estados pueden hacer de las tecnologías emergentes en el ejercicio de sus funciones públicas. Garantías como el debido proceso, juez imparcial, decisiones fundadas que supone el derecho de acceso a la justicia contenido en el artículo 25 indudablemente imponen límites y guías para el Estado que, por ejemplo,



quiera adoptar tecnologías de IA en el ejercicio de su labor judicial. Además, el SIDH hace exigible al Estado acceso a la información, por ejemplo, respecto de la adquisición, desarrollo, despliegue y uso de tecnologías emergentes. Particularmente cuando estas tecnologías están en estado experimental y se afectan a usos públicos que impactan el ejercicio de derechos humanos, imponiendo obligaciones concretas sobre el monitoreo judicial necesario para su despliegue, notificaciones, etc.

Finalmente, sin juzgar sobre la procedencia o conveniencia del abordaje de riesgos para este tipo de tecnologías, las aproximaciones de riesgo, tan comunes en el sector TIC, deben estar estrictamente ligadas a un marco de derechos humanos que permita nutrir el análisis de dichos riesgos del marco sustantivo y estándares desarrollados en la materia hasta la fecha.⁸⁸ La asimetría en la información disponible, principalmente en torno a los impactos de la tecnología en la sociedad, ha sido un catalizador de aproximaciones más desde los riesgos que desde los derechos. Muchos de los documentos y principios que apuntan a regular el desarrollo tecnológico lo hacen desde cada una de las nuevas tecnologías y desde una perspectiva de riesgos. Incluso de riesgos técnicos, que pueden impactar en la ética o la legalidad de ciertas prácticas en algunos casos pero que indudablemente se rigen por otros protocolos y principios. En el desarrollo de este tipo de aproximaciones, los estándares de legalidad, proporcionalidad y necesidad constituyen límites claros y necesarios frente a la discrecionalidad legislativa, regulatoria o judicial, sobre todo en lo que respecta a guiar las prácticas y conductas del sector privado en relación con los derechos de usuarios.

Las aproximaciones generales desde perspectivas éticas o morales pueden alimentar la sensación de disolución jurídica, y la percepción de ausencia de derechos donde en realidad hay pisos mínimos y estándares claros, sobre todo para el Estado. Incluso los documentos que refieren explícitamente los derechos humanos como marco, que no es el caso siempre, la vaguedad y la falta de granularidad en las obligaciones concretas y concisas que existen atentan contra la vigencia del régimen como marco orientador tanto de la conducta estatal como de la conducta privada en este proceso de cambio y desarrollo tecnológico.

El fortalecimiento del marco jurídico interamericano en materia de tecnologías emergentes requiere una visión integral que incluya los DESCAs como eje transversal de la gobernanza tecnológica. La protección y promoción de estos derechos debe ser prioritaria en la regulación y supervisión de la inteligencia artificial, asegurando que la innovación tecnológica no se traduzca en nuevas formas de exclusión o vulneración de derechos básicos. Se recomienda que los Estados realicen evaluaciones de impacto en derechos humanos, con énfasis en los DESCAs, antes de implementar sistemas de IA en servicios públicos y políticas sociales.

El SIDH es un sistema que ha sido importante a nivel regional. Los Estados son permeables al derecho internacional de los derechos humanos y en especial al derecho interamericano. A diferencia de Europa donde existe un órgano político y económico regional, en América Latina el derecho común se limita al marco interamericano de derechos humanos que permite cierta armonización de

⁸⁸ Del Campo, A., Zara N., y Alvarez Ugarte R., *Are Risks the New Rights: the perils of the risks approach in tech regulation*, (forthcoming) Recuperado de: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5161173.



principios y estándares. Ha probado ser un sistema útil para abordar algunas de las complejidades que planteó la tecnología hasta el momento. Uno de los desafíos más grandes para mantener la vigencia de este marco tan viva como hasta ahora es la revalidación y el desarrollo de estándares claros a medida que los desafíos van mutando, acompañados de jurisprudencia actualizada y pormenorizada. En definitiva, el derecho vive a partir de la interpretación que de él hagan los distintos actores de un sistema político, pero sobre todo sus tribunales. El rol de la Comisión Interamericana en el desarrollo y sistematización de estándares ha sido fundamental y conviene promoverlo hasta su incorporación como estándar jurídico tanto en la Corte Interamericana como en la jurisprudencia de los distintos tribunales locales que hacen al SIDH y nutren su interpretación.





ANEXOS



ANEXO 1

INTELIGENCIA ARTIFICIAL, INNOVACIÓN Y DERECHOS HUMANOS. NOTAS PARA UNA MARCHA CAUTELOSA EN AMÉRICA LATINA



Por: Carolina Aguerre

Los efectos y los riesgos de la IA ya no son una preocupación de algunos especialistas, sino que abundan los procesos y discusiones sobre este fenómeno. El momento de la tecnología de IA dejada únicamente en manos del sector privado no es más una opción viable para las sociedades contemporáneas. Este documento aborda el fenómeno creciente de cuestionamiento de la “innovación sin barreras de contención” y lo enmarca en tres procesos de gobernanza, uno regulatorio en la Unión Europea, otro de gobernanza regulatoria a partir de las iniciativas del G7 y otro con los derechos humanos como fundamento que debe traccionar a la gobernanza de la IA en este contexto. Por último, se esbozan algunos lineamientos para América Latina.

I. Introducción

El 30 de noviembre de 2022 la empresa OpenAI lanzó una versión gratuita de su Inteligencia Artificial (IA) generativa basada en Grandes Modelos de Lenguaje (LLM por su acrónimo en inglés). Este hecho puede considerarse como el momento en el que se disparó la conciencia pública a nivel internacional sobre el fenómeno de la IA. De acuerdo a Google Trends, el servicio de tendencias de búsqueda de Google que muestra los términos de búsqueda más populares, la búsqueda del término “Chat Gpt” arroja que a nivel mundial la búsqueda de información en el buscador pasó de 2% en la semana del 27 de noviembre al 2 de diciembre de 2022 a una atención de entre 90-100% desde la semana del 19 de marzo al 17 de junio de 2023, y sin bajar del 69% desde entonces.

Chat GPT marcó un antes y un después de una tecnología de propósito general como es la Inteligencia Artificial. Esta aplicación popularizó la versión ‘generativa’ de la IA esto es, una IA con la capacidad de generar textos, imágenes o palabras. Efectos similares de popularización tecnológica tuvo la Internet con la World Wide Web (www). Hasta principios de la década de 1990, la Internet era utilizada en ámbitos especializados, pero la serie de protocolos que componen a la Web dinamizó la expansión de esta tecnología. La analogía entre estos dos momentos críticos se produce para ilustrar cómo algunas innovaciones sobre ciertas tecnologías de propósito general existentes, ya sea en formato de suite de protocolos abiertos como los de la web, o de plataformas cerradas como Chat GPT, lograron expandir masivamente el interés de las personas.



Sin embargo, lo más relevante de estos acontecimientos no son las tecnologías en sí. Estos casos son hechos de innovación en el ámbito tecnológico, pero son eventos directamente vinculados con cambios en los mercados, en las relaciones laborales y en la transformación social y cultural más amplia en la que se encuentra buena parte del mundo. Una clara prueba de esto fue la carta publicada el 22 de marzo de 2023 organizada por el *Future of Life Institute*, a la que adhirieron casi de inmediato científicos y empresarios centrales vinculados con el desarrollo de esta tecnología como Geoffrey Hinton, Steve Wozniak, Y. N. Harari y Elon Musk, donde especialmente desarrollaron preguntas centrales vinculadas al futuro de esta tecnología:

Los sistemas de inteligencia artificial contemporáneos ya compiten con los humanos en tareas generales, y debemos preguntarnos: ¿Debemos dejar que las máquinas inunden nuestros canales de información con propaganda y falsedades? ¿Debemos automatizar todos los trabajos, incluidos los más gratificantes? ¿Debemos desarrollar mentes no humanas que con el tiempo nos superen en número, inteligencia, obsolescencia y reemplazo? ¿Debemos arriesgarnos a perder el control de nuestra civilización? Estas decisiones no deben delegarse en líderes tecnológicos no elegidos. Los sistemas de IA potentes sólo deben desarrollarse cuando estemos seguros de que sus efectos serán positivos y sus riesgos controlables (Pause Giant AI Experiments, Future of Life, 2023).

Estas preguntas no son sólo esenciales por su preocupación por el futuro de la humanidad tal como la conocemos, sino también porque abren la posibilidad de cuestionar el sentido y la dirección de este supuesto progreso que buena parte del espíritu del tiempo contemporáneo ha abrazado con tecnologías digitales y sistemas de IA desde el corazón de estos centros de producción mundial de saberes y plataformas vinculadas con estas tecnologías.

Varios autores denuncian los grandes procesos de transformación política y económica global y una desigual distribución de los beneficios y riqueza debido a la expansión de las tecnologías digitales, especialmente aquellas basadas en IA y sistemas tecnológicos asociados. Entre estos trabajos se encuentra la publicación de Darren Acemoglu y Simon Johnson (2023) “Poder y Progreso. Nuestra lucha de 1000 años sobre la tecnología y la prosperidad” (traducción propia)⁸⁹, o los trabajos sobre el fenómeno de la configuración institucional y espacial de la globalización con la creciente concentración de capitales financieros y conocimiento que señala Saskia Sassen (2014, 2018). En estos abordajes, la innovación tecnológica se encuentra retratada como un proceso provocado por incentivos científicos y tecnológicos, pero también por la influencia de estímulos económicos organizados en torno a los mercados contemporáneos del occidente más rico. Estos trabajos permiten situar con una lente más crítica a la innovación en un contexto de mayor concentración de riqueza y de poder a nivel global.

Desde 2016 se despliegan una serie de instrumentos vinculados con la conducción controlada de la Inteligencia Artificial, enmarcada bajo principios éticos mayormente en sus comienzos (Fjeld, 2020). Sin embargo, estos avances desarrollados con el objetivo de generar consenso en torno a

⁸⁹ Power and Progress: Our Thousand-Year Struggle Over Technology and Prosperity. (título original)



los principios éticos, tales como la transparencia, la no-discriminación y la justicia, invocan muchas veces directamente a los derechos humanos como sustento de estas declaraciones, como es el caso de las Recomendaciones de UNESCO para la ética de la IA (2021). A medida que una tecnología como la IA se vuelve más visible, y accesible, las políticas que buscan encausar su desarrollo se vuelven menos declarativas y buscan desplegar procesos normativos más formales, incluyendo regulaciones específicas en esta materia (Smuha, 2021). Tal es el caso de la propuesta de la Unión Europea con la ley de IA.

El trabajo explora la gobernanza de la IA a nivel internacional y el papel de los derechos humanos en este proceso con el trasfondo de las reacciones a las innovaciones en el ámbito de las tecnologías vinculadas a la IA generativa, y los crecientes despliegues que en una década han pasado de tendencias éticas y normativas a procesos legislativos y regulatorios. El documento aborda una parte cada vez más visible del discurso contemporáneo que comienza a desarrollar una mirada más cautelosa en relación a los avances de la IA. Estas miradas matizan, y cuestionan el optimismo de hace unos años sobre los beneficios a gran escala de los sistemas de IA, y exploran los aportes de los derechos humanos para enriquecer esta marcha más cautelosa que orientan las incipientes políticas y el espíritu de la época actual. El trabajo se realiza mediante el análisis documental de algunos de los principales acontecimientos y procesos recientes en la materia, incluyendo declaraciones, normativas, y referencias bibliográficas.

A continuación, el documento se desarrolla en tres partes. En la primera se abordan argumentos esbozados por académicos centrados en las características de la innovación contemporánea de los sistemas de IA. En la segunda parte se desarrollan algunos de los principales lineamientos de políticas internacionales, incluyendo las crecientes discusiones sobre regulación de la IA y las bases en los derechos humanos y en principios éticos. En la tercera se discuten tres sectores clave para América Latina en los que la perspectiva de los derechos humanos es particularmente pertinente a la hora de desarrollar políticas públicas.

II. La crisis de la confianza en la innovación propiciada por la Inteligencia Artificial

¿Debemos dejar que las máquinas inunden los canales de información con propaganda y falsedades? ¿Debemos automatizar todos los trabajos, incluidos los más gratificantes? ¿Debemos desarrollar mentes no humanas que con el tiempo nos superen en número, inteligencia, obsolescencia y reemplazo? ¿Debemos arriesgarnos a perder el control de nuestra civilización? Estas preguntas se desprenden del trabajo de Acemoglu y Johnson (2023) quienes argumentan que estas decisiones no deben delegarse en líderes tecnológicos que no han sido electos. En la misma tónica que la carta de los emprendedores y científicos que pedía una moratoria en el avance de la IA generativa, los autores argumentan que los sistemas de IA potentes sólo deben desarrollarse cuando estemos seguros de que sus efectos serán positivos y sus riesgos controlables.



Tras años de tecno-optimismo el “capitalismo digital” se enfrenta a una crisis de legitimidad. Los gigantes tecnológicos, durante mucho tiempo proclamados como agentes que llevarían adelante la transformación del capitalismo, el progreso, y el bienestar fueron descriptos como los tipos BAADD: “grandes, anticompetitivos, adictivos y destructivos para la democracia” (acrónimo de *Big Anti-Competitive, Addictive and Destructive to Democracy*) (The Economist, 2018). Desde entonces académicos como políticos piden más regulación, y llaman la atención a los gigantes tecnológicos por sus prácticas empresariales dañinas, extractivas y monopolísticas (Nachtwey y Seidl, 2020).

Si bien la industrialización de los últimos tres siglos ha generado un mayor bienestar de la población y expectativa de vida, esto no ocurrió por la innovación tecnológica en sí misma, sino porque hubo un esfuerzo realizado por personas y organizaciones que trabajaron para que esos beneficios no quedaran cerrados a las élites, sino que se derramaran en la población (Acemoglu y Johnson, 2023; Zuboff, 2019). La expansión de los beneficios de innovación tecnológica, especialmente aquella basada en sistemas de IA, con la cual contrastan sus trabajos esos autores, tiene un vínculo estrecho con la propia conceptualización de la innovación en la actualidad.

Los modelos que describen la innovación como un proceso lineal de los factores causales que intervienen no son viables (Kline y Rosenberg, 2010). La innovación tecnológica es compleja, variable y difícil de medir. Exige una estrecha coordinación de conocimiento técnico adecuado y excelentes criterios de mercado. Como señalan varios estudios, la mayor parte de las innovaciones que se registran en las oficinas de patentes del mundo están motivadas como resultado de la percepción de las necesidades del mercado, en una proporción mucho más alta que la percepción de las oportunidades técnicas percibidas (Kline y Rosenberg, 2010). Si la innovación tecnológica, uno de los motores centrales de la economía contemporánea, está basada en criterios de mercado fundamentalmente y no tiene capacidad de desarrollar una mirada más sistémica sobre los efectos negativos que indudablemente se manifiestan, es relevante apelar para que otros criterios puedan incluirse en la toma de decisiones vinculadas a estos temas. Motivaciones vinculadas a la promoción de los derechos humanos, el desarrollo de las personas y el desarrollo sostenible son cada vez más relevantes a la hora de pensar en los rumbos de la innovación.

Por ello, es fundamental re-enfocar este avance en tiempos de expansión de la IA generativa en la cual se está ante un umbral de cambios radicales en la conformación de diversas industrias y sectores, desde las creativas hasta las informáticas, con un potencial de desplazamiento de fuentes de trabajo y concentración de la riqueza en aquellos que capturan los datos y los procesan con su IA. “Esto debe comenzar confrontando el tecno-optimismo ciego de nuestro tiempo y desarrollando nuevas formas de usar la ciencia y la innovación” (Acemoglu y Johnson, 2023: 34).



III. La gobernanza internacional de la IA y los derechos humanos ante la percepción creciente de las amenazas de la IA

En esta sección se abordan dos ámbitos de referencia internacional que sustentan una visión más cautelosa de la IA. Estos reparos sobre los efectos sociales, económicos y políticos de la IA se inscriben en una perspectiva que, sin dejar de lado el potencial de innovación, consideran plenamente la necesidad de desarrollar mecanismos de contención para su desarrollo. Estos dos casos son: el recorrido de la UE en materia de datos e Inteligencia Artificial y el del ámbito del G7. Ambos ejemplos fueron seleccionados por la relevancia que asumen los datos personales y los derechos humanos en las opciones de gobernanza de la IA, y porque son contextos institucionales relevantes con efectos sobre el contexto de América Latina. En la última parte se analiza el papel de los derechos humanos.

i. El contexto jurídico y normativo europeo

La preocupación normativa por la evolución de las tecnologías digitales, el big data y las redes ubicuas ha estado presente en la UE durante al menos tres décadas. La Directiva sobre protección de datos de 1995 y el Convenio de Bioética de Oviedo de 1997 fueron precursores de las incertidumbres y los retos que las tecnologías de uso intensivo de datos crearían para los derechos de las personas, en particular los relativos a su dignidad humana como piedra angular fundamental que se relaciona con el derecho a la intimidad, así como a la autonomía y la agencia. En 2009 se aprueba la Carta de Derechos Fundamentales de la Unión Europea.

Casi dos décadas más adelante, el tecno-optimismo es puesto bajo bajo escrutinio en esa región cuando el entonces estudiante de derecho austríaco Max Schrems presentó su primera denuncia ante el Comisionado de Protección de Datos de Irlanda, que luego condujo a una decisión del Tribunal de Justicia de la Unión Europea de descartar el acuerdo de *Safe Harbour* entre EE.UU. y la UE en 2015. La expansión de las tecnologías de IA aceleró los desafíos emergentes, incluyendo la protección de los derechos humanos a las nociones de igualdad, justicia y participación. En este escenario, el cuestionamiento de la captura, el procesamiento y la monetización de los datos en línea se hizo cada vez más frecuente.

Desde la UE se adoptaron medidas para abordar la protección y la mejora de los derechos humanos en la era digital, especialmente a través del Reglamento General de Protección de Datos (RGPD) aprobado en 2016 y aplicado en mayo de 2018 con efectos extraterritoriales relevantes, y elevando los estándares de privacidad y protección de datos. El RGPD es una piedra angular de las estrategias de IA de la UE ya que regula los datos, y sitúa la dignidad humana como piedra angular de todos los desarrollos en torno a la protección de datos. Sus efectos trans-jurisdiccionales también son relevantes para este trabajo, ya que afecta a un elemento clave para el desarrollo de



la IA como es el tratamiento de datos en entornos y sectores fuera de la UE, como se ha visto en la adaptación de varias legislaciones de la región de América Latina de los últimos años.

Como unión política basada en el Estado de Derecho, un rasgo distintivo de este sistema es que la persona humana es el centro de las protecciones legales y constitucionales. Cualquier innovación debe cumplir este principio fundamental que prevalece en la Carta de los Derechos Fundamentales de la Unión Europea de 2009 y consagra en la legislación de la UE una amplia gama de derechos fundamentales. La propuesta de Ley de la IA señala características específicas de la IA, como la opacidad, la complejidad de la dependencia de los datos y el comportamiento autónomo que pueden afectar negativamente a varios derechos fundamentales consagrados en “la Carta”.

Continuando con esta línea regulatoria, la propuesta de ley europea para la IA todavía bajo negociación en el parlamento europeo, tiene cuatro objetivos específicos: (i) garantizar que los sistemas de IA comercializados y utilizados en la Unión sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión; (ii) garantizar la seguridad jurídica para facilitar la inversión y la innovación en IA; (iii) mejorar la gobernanza y la aplicación efectiva de la legislación vigente sobre derechos fundamentales y requisitos de seguridad aplicables a los sistemas de IA; (iv) facilitar el desarrollo de un mercado único de aplicaciones de IA legales, seguras y fiables y evitar la fragmentación del mercado.

La propuesta de ley europea para la IA se basa en valores y derechos fundamentales. Sostiene que la IA debe ser una herramienta para las personas, así como una fuerza para el bien social, con el objetivo último de aumentar el bienestar humano. Este abordaje contradice el espíritu tecno-optimista que fue consignado como problemático en el comienzo del trabajo por su escasa consideración sobre el derrame de estos beneficios a más sectores, así como por sus escasas consideraciones sobre su ética sistémica.

En general, las estrategias políticas y el enfoque jurídico de la IA adoptados por la UE en los últimos años tienen un denominador común y es que no dan por sentado que los derechos humanos y las instituciones democráticas puedan mantenerse firmes para abordar algunos de los cambios de paradigma que se están produciendo con el avance de la IA en la sociedad.

ii. El G7, un enfoque de gobernanza regulatoria

Este espacio, a diferencia del ejemplo anterior, carece aún de mecanismos institucionales sólidos para la gobernanza de tecnologías digitales que contemple un único resultado regulatorio. Sin embargo, representa una fuente de acciones políticas fundamentales con impactos insoslayables a nivel mundial. El G7 nuclea a algunos de los países centrales en la producción de sistemas de IA, a la vez se define como un espacio donde interactúan estados que adhieren a los principios democráticos y de respeto por los derechos humanos. La Cumbre del G7 de mayo de 2023 se



embarcó de lleno en la Inteligencia Artificial. Aún cuando hay diferencias de abordajes entre los estados que componen a este grupo, estos comparten valores como el pluralismo político, la democracia y el respeto por los derechos humanos. China es en cambio el país con mayor desarrollo de patentes y artículos científicos de IA (Live Data from OECD), pero no se adhiere a los valores democráticos, ni al respeto por los derechos humanos como sus fundamentos políticos.

A pesar de las afinidades en torno a los valores políticos, los países del G7 abordan la gobernanza de la IA de forma diferente, desde leyes estrictas y exhaustivas como es el caso de la Unión Europea con su proyecto de ley, hasta directrices sectoriales como las que propone Estados Unidos o el Reino Unido. Algunas de las razones que explican estas diferencias son la inclinación hacia mecanismos de autoregulación y la confianza en los mercados. Sin embargo, esta posición no intervencionista, representa una visión peligrosa ante los avances de una IA que se encuentra concentrada en una elite de empresas y empresarios, y científicos con una visión solucionista de la tecnología (Seidl y Nachtwey, 2020; Morozov, 2013).

El comunicado del G7 (Ministerial Declaration 2023) destaca los riesgos potenciales de la IA, como el acoso en línea, el odio y el abuso, y las amenazas a la seguridad y la privacidad de los niños. Este texto también señala en el ámbito de la IA generativa el peligro de la manipulación de la información extranjera, que implica la difusión de desinformación. La declaración amplía esta lista, advirtiendo sobre el mal uso y abuso de la IA para socavar los valores democráticos, suprimir la libertad de expresión y amenaza con el ejercicio y goce de los derechos humanos. De forma relevante para este trabajo, enfocado en un análisis de las consecuencias más sistémicas de estas innovaciones tecnológicas, las declaraciones del G7 expresan una mayor preocupación por la posibilidad de que la IA produzca y difunda contenidos que pongan en peligro valores fundacionales como los derechos humanos y la libertad, más que por los riesgos inherentes a la propia IA, como la falta de previsibilidad o explicabilidad (Habuka, 2023).

En el marco de esta fragmentación en el enfoque de la gobernanza de la IA, los miembros del G7 acordaron que las políticas y normativas deberían basarse en el riesgo y tener visión de futuro. Sin embargo, el horizonte regulatorio “basado en el riesgo” tiene diferencias de interpretación. Esta variación entre países puede no diferir significativamente del principio general de regulación necesario y proporcional (Habuka, 2023), con el horizonte de los derechos humanos como el abordaje para encausar las políticas regulatorias. El camino que propone este grupo es lograr la interoperabilidad en los marcos de gobernanza de la IA. Además, la declaración subraya que las políticas y normativas deben tener en cuenta no sólo las características técnicas e institucionales, sino también las repercusiones sociales y culturales.

Finalmente, los documentos del G7 de 2023 retomaron elementos del Data Free Flow with Trust (DFFT) o también conocido como “Osaka Track” de 2019, cuando en la cumbre del G20, también organizada en Japón, se propuso la tarea de buscar armonizar los marcos de gobernanza de datos para favorecer el libre flujo de datos transfronterizos. En tanto los sistemas de aprendizaje automatizado dependen de los datos, la libre circulación de datos de alta calidad es esencial. Sin embargo, las políticas de datos en todo el mundo son muy divergentes y abarcan ámbitos, sectores



e intereses diversos. Las declaraciones del G7 coinciden en el establecimiento de un Acuerdo Institucional de Asociación (IAP) para hacer operativo el DFFT. Se trata de una iniciativa de cooperación multistakeholder, basada en principios, orientada a soluciones y pruebas. El hecho de estar orientada a las soluciones sugiere que esta iniciativa no se centra en conceptos específicos como la privacidad o la equidad, sino en soluciones prácticas a problemas existentes en la aplicación de estos principios. Más concretamente, se espera que el proyecto aborde la mejora de la accesibilidad a la información reglamentaria, la cooperación en tecnologías de mejora de la privacidad, las cláusulas contractuales tipo, las credenciales digitales y las identidades. Estos esfuerzos están directamente relacionados con una IA confiable.

La agenda del G7 en materia de gobernanza de la IA tiene una clara impronta de búsqueda de mecanismos de “gobernanza regulatoria internacional” (Abbott y Snidal, 2009; Drezner, 2008), a partir del impulso al diálogo sobre normas y principios compartidos que deben preservarse - por ejemplo, el entendimiento sobre regulación basada en riesgos, los mecanismos de interoperabilidad y estándares técnicos, entre los que se encuentran los mecanismos para estimular el DFFT. Los abordajes que se proponen tienen múltiples vías para su realización, y los derechos humanos son uno de los fundamentos, pero no son los únicos. La innovación y la preservación de los mercados internacionales son también bases centrales de la orientación de estas políticas que deben reconocer los crecientes obstáculos y resistencias en materia de interpretación de la dirección de los avances de la IA generativa y a gran escala.

iii. Gobernanza de la IA con base en los derechos humanos: tan bueno como parece

El derecho internacional de los derechos humanos es una cristalización de principios éticos en normas, cuyos significados e implicaciones se han ido desarrollando a lo largo de los últimos setenta años. Estas normas cuentan con un amplio consenso internacional, son relativamente claras y pueden desarrollarse para adaptarse a nuevas situaciones. Ofrecen un método bien calibrado para equilibrar los derechos de la persona con los derechos e intereses contrapuestos mediante pruebas de necesidad y proporcionalidad. Los derechos humanos proporcionan procesos de gobernanza para empresas y gobiernos, y un ecosistema para la provisión de remedios en caso de infracción (Jones, 2023; Sikkink, 2017).

Los derechos humanos vinculados a la privacidad, la protección de datos, la igualdad y la no discriminación son fundamentales para la gobernanza de la IA, al igual que la protección de la autonomía, y de los derechos económicos, sociales y culturales que permiten garantizar que la IA beneficie a todos. Las normas de derechos humanos no sólo imponen a los gobiernos la obligación de respetarlas, sino también a las empresas y organizaciones la responsabilidad de cumplirlas, así como la exigencia de recursos legales y reparación de daños (Jones, 2023).



Otros conjuntos de principios y valores pueden tener una relevancia más matizada para los sistemas de IA en particular. Pero, cuando se trata de opciones de referencia actuales con legitimidad internacional para abordar los daños de la IA, los derechos humanos pueden ser la mejor opción disponible (Latonero, 2020). Inclusive las Recomendaciones para la ética de la IA de UNESCO (2021), el instrumento de recomendaciones éticas más relevante a nivel internacional por su adopción por los 193 estados miembro de la ONU toma en cuenta el respeto a los derechos humanos como su primer valor.

De acuerdo a Raso et al (2018), la privacidad es el derecho que se ve más afectado por las aplicaciones actuales de la IA. Otros derechos que también se ven vulnerados por la IA son los derechos a la igualdad, a la libre expresión, a la asociación, a la reunión y al trabajo. Hasta la fecha el impacto de la IA en estos derechos ha sido más negativo que positivo (Latonero, 2020).

Ante la proliferación de principios éticos y mecanismos de evaluación, las empresas, los gobiernos y la sociedad civil están volviendo a tratar el tema de los derechos humanos para abordar la gobernanza de la IA. Como se mencionó con los ejemplos anteriores de la trayectoria normativa de la UE vinculada con la IA, y algunas de las medidas del G7, estos son el fundamento para el desarrollo de sus mecanismos de gobernanza. Estos son un instrumento con un alcance sobre la gobernanza de la IA que pueden otorgarle una forma y una protección más definida, entre otros porque las empresas son objeto de cumplimiento de los mismos y no sólo los Estados, como ha sido abordado por los Principios Ruggie (McGregor et al, 2019). Estos visibilizan el papel central que tiene el sector privado en particular en ámbitos de la IA y tecnologías afines. Los Principios Ruggie proponen que las empresas, para demostrar y aplicar el respeto a los derechos humanos, tomen medidas como comprometerse públicamente a respetar los derechos humanos; identificar, mitigar y rendir cuentas de los daños causados a los derechos humanos; y disponer de procedimientos para remediar las consecuencias negativas sobre los derechos humanos que causan o contribuyen a causar.

IV. Apuntes para una marcha cautelosa en América Latina

En el apartado anterior se discutieron diversos enfoques internacionales que abordan con instrumentos de gobernanza normativa, regulatoria y una revisión de la relevancia de los derechos humanos en este contexto. La revisión del sentido de época actual incluye no sólo el análisis del instrumento de gobernanza de la IA, sino también de sus implicancias para los arreglos sociales contemporáneos. El sentido de época ha cambiado con respecto a la década pasada, cuando se expandían los sistemas de aprendizaje automatizado en un marco de innovación que si bien sigue vigente, se encuentra mucho más enmarcado en torno a los riesgos y las consecuencias éticas.

Esta conciencia sobre la definición de acciones de gobernanza normativa y regulatoria en consonancia con los distintos avances internacionales mencionados no es sólo apremiante en los países centrales donde se desarrollan gran parte de estas tecnologías. Es aún más urgente en una



región como la latinoamericana, donde persisten grandes desigualdades económicas y sociales, y donde aún hay mucho trabajo por consolidar los sistemas e instituciones democráticas. En este contexto se espera que los gobiernos tomen riendas mucho más claras en el devenir de estos desarrollos e innovaciones de la IA para preservar y promover el interés público, y no dejar vacíos políticos o normativos en el desarrollo de la IA al sector privado como principal actor (Acemoglu y Johnson, 2023).

En base al Índice Latinoamericano de Inteligencia Artificial (2023) en su capítulo sobre la percepción de la IA en la región se destacan la invasión a la privacidad, el daño socioambiental, la ética, los desórdenes informativos, la discriminación de género y el reemplazo y la precarización laboral emergen como los principales nudos problemáticos que se desprenden las menciones en redes sociales y medios de opinión pública a nivel regional. En sintonía con los análisis que han realizado otros autores en ámbitos internacionales (Acemoglu y Johnson, 2023; Nachtwey y Seidl, 2020; Sassen, 2018), el escepticismo crece en el ámbito de los usuarios de distintas tecnologías basadas en IA, a pesar de que los medios de comunicación suelen tener visiones más optimistas centradas en su potencial de innovación. Este índice destaca que en América Latina el 42% de las opiniones en medios digitales son optimistas, y el 13% son pesimistas. Al contrario, en redes sociales el 31% de las opiniones son pesimistas, y sólo el 23% son optimistas.

Si bien este informe del índice latinoamericano en su edición 2023 señala varias áreas de oportunidad, se tomarán dos sectores fundamentales en este trabajo que inscriben esta necesidad de reencausar los valores y las políticas basados en los derechos humanos. En primer lugar, se encuentra el uso de la IA con fines de vigilancia. La vigilancia es un área en la que se aplica cada vez más la IA a nivel mundial y América Latina no es una excepción, particularmente en las grandes ciudades. Si bien los gobiernos de la región no parecen hacer un uso significativo de los sistemas de reconocimiento facial por medio de la IA en comparación con otras (OECD y CAF 2022), esta práctica está aumentando en la región, como también aumenta la resistencia de la sociedad civil (Arroyo, 2020). En algunos países de ALC, se está haciendo un uso experimental de la IA para analizar imágenes de rostros juntamente con otros videos, imágenes y audio, y en la mayoría hay sectores donde ya se implementan sin una actualización de los marcos legales y los resguardos de los derechos humanos pertinentes (DATYSOC, 2022, Relator Especial, 2019, Alto Comisionado, 2019). Los valores en tensión que emergen de las fuerzas de seguridad y orden público de los estados con las entidades que buscan promover los derechos humanos y un uso más reflexivo y medido de estas tecnologías que promueven un paradigma permanente de la vigilancia deben ser abordados como problemáticas sociales más amplias y no como una decisión oportunista sobre innovaciones tecnológicas sin más.

Otra revisión que considerar es el futuro del trabajo ante la automatización. Si bien América Latina presenta una realidad demográfica donde los problemas de envejecimiento poblacional recién estarán apareciendo a mediados del siglo 21 (Lewandoski et al, 2020), los desafíos asociados al desempleo tecnológico y/o la polarización laboral serán menos relevantes que en los países desarrollados. “Sin embargo, este escenario representaría un nuevo episodio de aceleración tecnológica que la región no lograría capitalizar a los efectos de potenciar su crecimiento y reducir



las importantes brechas de productividad que la separan de las economías de mayor desarrollo” (Zunino, 2022). Si bien este tema aparece vinculado a la falta de productividad y la pérdida de oportunidades en materia de crecimiento económico, por falta de capacidad de innovación e incentivos económicos, en la práctica esto también resulta en un problema en el que el ejercicio de los derechos económicos, sociales y culturales (DESC) se ven potencialmente amenazados si no hay mejores posibilidades de crecimiento y desarrollo (CESR et al, 2018).

Los derechos humanos no solo son esenciales para darle una forma y fuerza vinculante a los principios éticos contemporáneos, sino también porque es imperativo encontrar un nuevo espíritu de época más compartido, que contemple oportunidades y también una mirada cautelosa sobre los riesgos y problemas, y que permita garantizar un horizonte compartido de la gobernanza para estas tecnologías.





BIBLIOGRAFÍA

Access Now (2020). Access Now's submission to the Consultation on the "White Paper on Artificial Intelligence - a European approach to excellence and trust".

Acemoglu, Darren & Johnson, Simon. (2023). Power and Progress: Our Thousand-Year Struggle Over Technology and Prosperity. PublicAffairs.

Alto Comisionado de las Naciones Unidas para los Derechos Humanos, «Informe sobre el impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas», A/HRC/44/24, parr. 38. (Asamblea General de las Naciones Unidas, 24 de junio de 2020), <https://undocs.org/es/A/HRC/44/24>

Arroyo, V. (2020, December 16). Facial recognition in Latin America: Why civil society must fight back. <https://www.accessnow.org/facial-recognition-latin-america/>

Carta de los Derechos Fundamentales de la Unión Europea. <https://eur-lex.europa.eu/summary/EN/I33501>.

Center for Economic and Social Rights (CESR), for, Oxfam, Instituto de Estudos Socioeconômicos (INESC), Conectas Derechos Humanos, C., Justiça Global, Ministerio Público de la Defensa de la Ciudad Autónoma de Buenos Aires, Asociación Civil por la Igualdad y la Justicia (ACIJ), Centro de Estudios Legales y Sociales (CELS), Centro de Estudios de Derecho, Justicia y Sociedad (Dejusticia), Foro Salud, & Asociación Pro Derechos Humanos (APRODEH). (2018). Políticas fiscales y garantía de los Derechos Económicos, Sociales y Culturales en América Latina. <https://www.cels.org.ar/web/publicaciones/politicas-fiscales-y-garantia-de-los-derechos-economicos-sociales-y-culturales-en-america-latina/>

DATYSOC. (2022). Fuera de control. Uso automatizado del reconocimiento facial automatizado en Uruguay. <https://datysoc.org/wp-content/uploads/2022/03/Informe-reconocimiento-facial-automatizado-Uruguay-2022-Datysoc.pdf>

G7 Hiroshima Leaders' Communiqué (2023). https://www.g7hiroshima.go.jp/documents/pdf/Leaders_Communique_01_en.pdf

Índice Latinoamericano de Inteligencia Artificial (2023) <https://indicelatam.cl/>

Jones, K. (2023). AI governance and human rights: Resetting the relationship. Royal Institute of International Affairs. <https://doi.org/10.55317/9781784135492>



Latonero, M. (2020). AI Principle Proliferation as a Crisis of Legitimacy. Carr Center for Human Rights Policy. Harvard Kennedy School of Government, 2020–011.

Lewandowski P, A Park y S Schotte. (2020). The Global Distribution of Routine and Non-Routine work. Discussion papers series. IZA DP No 13384

Live data from OECD.AI - OECD.AI. (n.d.). <https://oecd.ai/en/data?selectedArea=ai-research&selectedVisualization=ai-publications-time-series-by-country>

Mantelero, A (2022) Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI, Springer.

McGregor, L., Murray, D., & Ng, V. (2019). International human rights law as a framework for algorithmic accountability. *International and Comparative Law Quarterly*, 68(2), Article 2.

Ministerial Declaration: The G7 Digital and Tech Ministers' Meeting | EEAS. (30.04.2023). https://www.eeas.europa.eu/delegations/japan/ministerial-declaration-g7-digital-and-tech-ministers%E2%80%99-meeting_en

Morozov, E. (2013). To Save Everything, Click Here: The Folly of Technological Solutionism. PublicAffairs.

Nachtwey, O., & Seidl, T. (2020). The Solutionist Ethic and the Spirit of Digital Capitalism. <https://doi.org/10.31235/osf.io/sgjzq>

OECD & CAF Development Bank of Latin America. (2022). Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe. OECD. <https://doi.org/10.1787/5b-189cb4-es>

Pause Giant AI Experiments: An Open Letter. (2023.). Future of Life Institute. <https://futureoflife.org/open-letter/pause-giant-ai-experiments/>

Raso, Filippo, Hannah Hilligoss, Vivek Krishnamurthy, Christopher Bavitz, y Kim Levin. (2018). Artificial Intelligence & Human Rights: Opportunities & Risks. Berkman Klein Center for Internet & Society Research Publication.

Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. «Informe sobre la vigilancia y los derechos humanos», A/HRC/41/35. (Asamblea General de las Naciones Unidas, 28 de mayo de 2019). <https://www.undocs.org/es/A/HRC/41/35>

Rosenberg, N. (2009). Schumpeter and the Endogeneity of Technology. (pp. 303–328). https://doi.org/10.1142/9789814273596_0015



Sassen, S. (2016). *Expulsiones*. Katz editores.

Sassen, S. (2018). *Cities in a World Economy*. Sage.

Sikkink, Kathryn (2017). *Evidence for Hope: Making Human Rights Work in the 21st Century*. Princeton University Press.

Smuha, N. A. (2021). From a 'Race to AI' to a 'Race to AI Regulation': Regulatory competition for Artificial Intelligence. *Law, Innovation and Technology*, 13(1).

UNESCO. (2021). *Recomendación sobre la ética de la inteligencia artificial*. https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa

Zunino, G. (2022, 25 de julio). El futuro del trabajo: Una mirada desde América Latina. *la diaria*. <https://ladiaria.com.uy/economia/articulo/2022/7/el-futuro-del-trabajo-una-mirada-desde-america-latina>



ANEXO 2

TECNOLOGÍA BLOCKCHAIN: ¿ES POSIBLE SU USO RESPETANDO LA PRIVACIDAD Y OTROS DERECHOS HUMANOS?



Por: Andrés Chomczyk Penedo ⁹⁰

Abstract

La tecnología blockchain, en su esencia más básica, es un simplemente una manera de organizar información de forma distribuida entre miembros de una red que no confían entre sí, evitando la existencia de una autoridad central confiada por todos. Las crisis de confianza en instituciones que han actuado como terceros de confianza para llevar registros -desde bancos hasta Estados nacionales- ha sido un catalizador para el surgimiento de soluciones tecnológicas que permitan evitar a estas entidades y lograr relaciones de confianza entre pares. En sus más de diez años de desarrollo, esta tecnología y sus desarrolladores han realizado muchas promesas sobre el empoderamiento de sus usuarios en diferentes áreas, desde recuperar el control sobre sus datos personales mediante sistemas de identidad digital hasta evitar la censura en la expresión de sus ideas gracias a sistemas no estatales de dinero.

Como tal, esta tecnología apunta a facilitar el ejercicio y la protección de ciertos derechos humanos claves para la sociedad digital, frente a los avances de estos terceros de (des)confianza mencionados antes. Ahora bien, también existen ciertos potenciales riesgos que la propia tecnología podría traer consigo misma. El propósito de este artículo es explorar cuatro aplicaciones concretas (identidad digital, votación electrónica, registración de propiedad, y dinero digital) para identificar potenciales riesgos, así como también posibles beneficios en la adopción de soluciones basadas en la tecnología *blockchain*. Mediante este análisis, se buscará explicar que es esta tecnología y como la misma puede realizar o deshacer la protección de ciertos derechos humanos.

Palabras clave

Blockchain; derechos humanos; identidad digital; votación electrónica; propiedad; dinero digital; Bitcoin.

⁹⁰ Andrés Chomczyk es investigador doctoral del grupo de investigación Law, Science, Technology and Society de la Vrije Universiteit Brussel (Universidad Libre de Bruselas) y *fellow* del Brussels Privacy Hub. Es Marie Skłodowska-Curie *fellow* en el proyecto ITN PROTECT (Grant agreement ID: 813497). Asimismo, es experto del Observatorio y Foro Blockchain de la Unión Europea.



1. Introducción: ubicando blockchain dentro de las nuevas tecnologías digitales

Una de las tecnologías que más promesas han generado durante la última década es la tecnología *blockchain*.⁹¹ Como puede apreciarse en la imagen 1 más abajo, *blockchain*, y muchas de las aplicaciones que serán exploradas en este artículo, son parte de un cambio tecnológico mayor y con implicancias significativas para la configuración de nuevos modelos socioeconómicos basados en el uso intensivo de datos y la distribución de la toma de decisiones sobre ello. Sin embargo, muchas de estas promesas han comenzado a caer hacia una desilusión sobre sus supuestos beneficios, en buena medida por los desafíos que las aplicaciones presentan⁹². Al respecto de ello, las incertidumbres regulatorias podrían tener una influencia sobre este proceso.

Como veremos en este breve artículo de discusión, *blockchain* es una tecnología que es utilizada para organizar bases de información de diversos tipos de forma distribuida entre varias entidades que pueden conocerse o no y que no necesariamente confían entre sí; mediante un protocolo de trabajo, es posible registrar operaciones sobre activos digitales, evitando que los mismos se dupliquen de forma indebida y sin la necesidad de contar con una entidad central a cargo de controlarlo. Sin embargo, así como es posible encontrar adeptos,⁹³ también es posible ver una gran cantidad de voces críticas, particularmente en círculos académicos.⁹⁴ Uno de los principales puntos de discusión sobre esta tecnología radica en su relación, o supuesta falta de, con el sistema jurídico.⁹⁵

⁹¹ Deepak Puthal et al., «Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems», *IEEE Consumer Electronics Magazine* 7, n.o 4 (julio de 2018): 13-14, <https://doi.org/10.1109/MCE.2018.2816299>.

⁹² Nitin Upadhyay, «Demystifying Blockchain: A Critical Analysis of Challenges, Applications and Opportunities», *International Journal of Information Management* 54 (1 de octubre de 2020): 13, <https://doi.org/10.1016/j.ijinfomgt.2020.102120>.

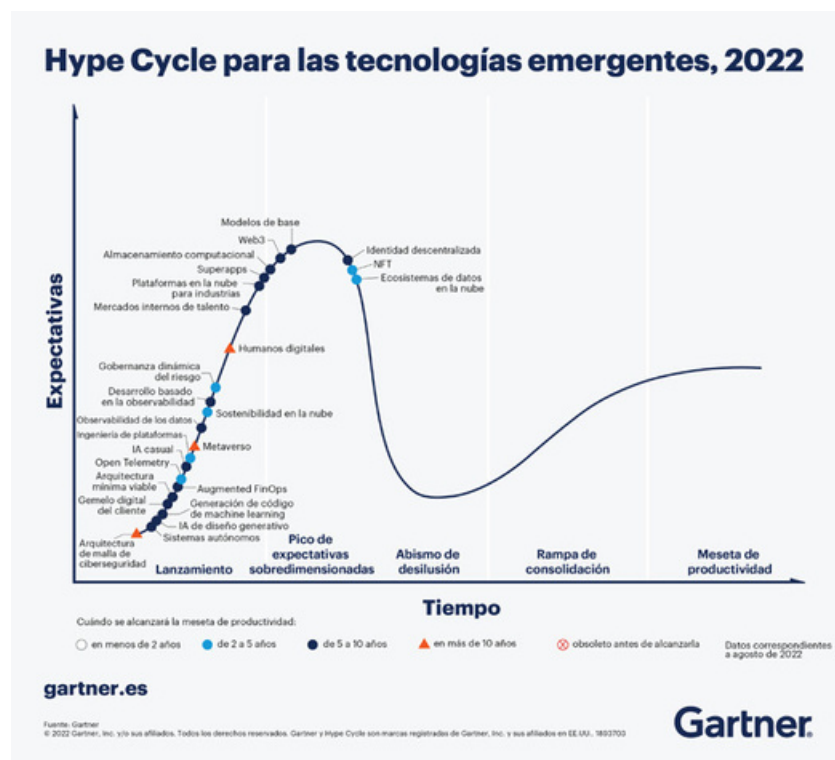
⁹³ Andreas M. Antonopoulos, *The Internet of Money: A collection of talks by Andreas M. Antonopoulos: Volume 1* (Vereinigste Staaten von America, 2016); Don Tapscott y Alex Tapscott, *La revolución blockchain: Descubre cómo esta nueva tecnología transformará la economía global*, trad. Juan Manuel Salmerón Arjona, 2017.

⁹⁴ Upadhyay, «Demystifying Blockchain».

⁹⁵ Robert Herian, *Regulating Blockchain: Critical Perspectives in Law and Technology* (Routledge, 2018); J. P. Quintais et al., «Blockchain and the Law: A Critical Evaluation», *Stanford Journal of Blockchain Law & Policy* 2 (2019), <https://dare.uva.nl/search?identifier=38a8394a-ed48-46d5-b71c-9d42357074e7>.



Imagen 1 – Ciclo de expectativas sobre tecnologías emergentes de Gartner



Fuente: <https://emtemp.gcom.cloud/ngw/globalassets/intl-es/information-technology/images/hype-cycle-para-las-tecnologias-emergentes-2022-es.png>

En concreto, estas voces señalan que las promesas de descentralización y empoderamiento que son pregonadas desde los defensores de esta tecnología no son más que declaraciones de (buenas) intenciones; la realidad de la sociedad digital, dominado por el llamado capitalismo de vigilancia,⁹⁶ pone al individuo en una situación donde la cantidad de interacciones que le son demandadas son demasiadas y, la posibilidad de tener control sin intermediarios a los cuales exigirles cuentas no deja de ser una mera ilusión. Dada esta situación, pueden darse situaciones donde ciertos derechos se vean vulnerados por la introducción de las tecnologías que prometían mayor control por parte de los usuarios.

En este sentido, el propósito de este breve artículo es discutir sobre el impacto del uso de la tecnología *blockchain* en ciertos casos de uso que han visto desarrollo regional con relación a los derechos humanos que pueden estar en juego en cada situación. El artículo pretende abordar la

⁹⁶ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).



pregunta de investigación que hace de título al mismo, a saber: “¿Es compatible el uso de tecnología *blockchain* respetando la privacidad y otros derechos humanos?”. Para responder a ella, la sección 2 abordará nociones básicas sobre la tecnología. La sección 3 explorará cuatro casos de uso donde esta tecnología ha sido usado en proyectos regionales (identidad digital, votación electrónica, registración de propiedad, y dinero digital) y sus posibles implicancias, tanto positivas como negativas. Finalmente, la sección 4 hará unas consideraciones finales.

2. ¿Qué es blockchain? Entendiendo sus orígenes, los problemas que resuelve y sus principales características

Si bien existe una gran cantidad de definiciones sobre que es *blockchain*,⁹⁷ es posible apoyarse en el trabajo de Andreas Antonopoulos, quien la define como “[u]na lista de bloques validados, cada uno vinculado a su predecesor hasta el bloque de génesis.”⁹⁸ En otras palabras, una *blockchain* es simplemente una base de datos distribuida entre diferentes actores que se encuentra organizada de tal forma que la información se almacena de forma secuencial en bloques de datos, donde cada uno tiene un resumen -en forma de hash- del bloque anterior.⁹⁹ El origen de esta palabra está íntimamente atada al protocolo Bitcoin.

En el año 2008, una persona o grupo de personas, bajo el seudónimo de Satoshi Nakamoto, publicó/aron un documento titulado “Bitcoin: A Peer-to-Peer Electronic Cash System”.¹⁰⁰ La introducción del *white paper* en cuestión pone de manifiesto el problema que se buscaba resolver: la sociedad digital del presente seguía usando un sistema monetario basado en la confianza sobre las instituciones a cargo de velar por la integridad de ese sistema. Lejos de una coincidencia, la aparición de Bitcoin responde a la crisis de confianza sobre el sistema financiero durante la debacle económica de los años 2008/2009.¹⁰¹

Nakamoto propuso el uso de una cadena de bloques como un registro público y distribuido en el que todas las transacciones de Bitcoin se registran de manera segura y transparente, en clara contraposición a los libros cerrados de los bancos. Bitcoin, tal como fue propuesto por Nakamoto, implicaba el desarrollo de un sistema monetario con una cantidad limitada de circulante, con un

⁹⁷ Mohammad Hossein Tabatabaei, Roman Vitenberg, y Narasimha Raghavan Veeraragavan, «Understanding Blockchain: Definitions, Architecture, Design, and System Comparison» (arXiv, 27 de noviembre de 2022), 2-3, <http://arxiv.org/abs/2207.02264>.

⁹⁸ Andreas M. Antonopoulos, *Mastering Bitcoin: programming the open blockchain*, Second edition (Sebastopol, CA: O'Reilly, 2017), xxiii.

⁹⁹ Andrés Chomczyk, «Regulación de blockchain e identidad digital en América Latina: El futuro de la identidad digital», 2020.a ed. (Banco interamericano de Desarrollo, 18 de diciembre de 2020), 26, <https://doi.org/10.18235/0002935>.

¹⁰⁰ Satoshi Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System», 31 de octubre de 2008, <https://bitcoin.org/bitcoin.pdf>.

¹⁰¹ Vasilis Kostakis y Chris Giotitsas, «The (A)Political Economy of Bitcoin», *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 12, n.o 2 (2014): 431-40, <https://doi.org/10.31269/triplec.v12i2.606>. Es particularmente interesante señalar que el bloque génesis (concepto que será explicado a continuación) tiene el siguiente mensaje incorporado “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks” (The Times 03/Enero/2009 Canciller al borde del segundo rescate para bancos, traducción del autor) en alusión a los rescates financieros, a costa de los contribuyentes, realizados en el Reino Unido, y otros países, durante la crisis económica del 2008/2009; este mensaje puede verse en <https://www.blockchain.com/explorer/blocks/btc/00000000019d6689c085ae165831e934ff763ae46a2a6c-172b3f1b60a8ce26f>, fecha de acceso 27 de junio de 2023.



ritmo de emisión predecible y sin la necesidad de un tercero de confianza para la gestión de la red.¹⁰² A diferencia del sistema monetario basado en moneda fiduciaria donde ciertos bancos, tanto centrales como comerciales, son quienes controlan el circulante físico y digital en una determinada economía, la red *blockchain* distribuye este control entre pares que no necesariamente se conocen y, por lo tanto, confían entre sí. Ello permite que múltiples participantes lleguen a un acuerdo sobre el estado de las transacciones y evita la posibilidad de fraudes o manipulaciones.

Nakamoto logró combinar conceptos previos y crear un sistema descentralizado y confiable para el intercambio de valor en línea. En este sentido, Bitcoin representa la consolidación de años de desarrollo en diferentes problemas informáticos: desde el uso de árboles de Merkle¹⁰³ hasta la implementación de mecanismos de gobernanza para lograr confianza entre actores desconocidos en un sistema informático distribuido.¹⁰⁴ En última instancia, el protocolo Bitcoin, mediante lo que se ha denominado consenso de Nakamoto,¹⁰⁵ logró encontrar una solución al problema de los generales bizantinos.¹⁰⁶

La gestión de activos digitales es una tarea compleja que ha sido resuelta principalmente mediante la centralización.¹⁰⁷ Ello se debe a que los activos digitales pueden ser duplicados y transmitidos con relativa facilidad; pensemos brevemente en una canción que es copiada de una computadora a otra por medio de un programa de intercambio de archivos, como sucedido en la década de los '90 con Napster. Una respuesta a este problema, como mencionamos, fue la centralización mediante plataformas como iTunes, y luego Apple Music o Spotify, que mediante ciertas tecnologías podían controlar como eran usados esos activos digitales. En particular, mediante estos, se pudo evitar que un recurso digital sea usado dos (o más) veces por personas no autorizadas a ello por el legítimo titular del activo, problema conocido en los entornos monetarios como doble gasto.¹⁰⁸

¹⁰² Al respecto de ello, es interesante señalar que ciertos autores han señalado que esto no es tan claro como los más férreos defensores de Bitcoin señalan sino que implica una transferencia de donde se confía y como se hace ello (ver Primavera De Filippi, Morshed Mannan, y Wessel Reijers, «Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance», *Technology in Society* 62 (1 de agosto de 2020): 101284, <https://doi.org/10.1016/j.techsoc.2020.101284>.)

¹⁰³ Un árbol de Merkle, llamado así por su inventor, es una base de datos organizada en forma de árbol donde cada punto de información guarda un hash de los puntos anteriores de información hasta llegar a un primer punto (ver Ralph C. Merkle, «A Digital Signature Based on a Conventional Encryption Function», en *Advances in Cryptology – CRYPTO '87*, ed. Carl Pomerance, Lecture Notes in Computer Science (Berlin, Heidelberg: Springer, 1988), 369-78, https://doi.org/10.1007/3-540-48184-2_32.)

¹⁰⁴ Alan T. Sherman et al., «On the Origins and Variations of Blockchain Technologies», *IEEE Security & Privacy* 17, n.o 1 (enero de 2019): 73, <https://doi.org/10.1109/MSEC.2019.2893730>.

¹⁰⁵ Aljosha Judmayer et al., «Nakamoto Consensus», en *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms*, ed. Aljosha Judmayer et al., Synthesis Lectures on Information Security, Privacy, and Trust (Cham: Springer International Publishing, 2017), 61-86, https://doi.org/10.1007/978-3-031-02352-1_6.

¹⁰⁶ El problema de los generales bizantinos es un concepto desarrollado en la teoría de la computación y se basa en una situación hipotética, donde un grupo de generales bizantinos lidera un ejército y deben coordinar un ataque o retirada conjunta. Sin embargo, algunos de los generales podrían ser traidores y enviar mensajes contradictorios para confundir a los demás. El desafío radica en encontrar un algoritmo o protocolo que permita a los generales leales llegar a un acuerdo común, a pesar de la presencia de generales traidores y mensajes engañosos. Esta situación es común en ambientes digitales donde las partes que interactúan pueden no conocerse y, por lo tanto, existir dudas sobre la confianza de una entidad. Para profundizar en ello, ver Cristina Pérez Solà y Jordi Herrera Joancomartí, «Bitcoins y el problema de los generales bizantinos» (Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información, Alicante: Universidad de Alicante, 2014), 241-46, <http://rua.ua.es/dspace/handle/10045/40444>.

¹⁰⁷ Elizabeth Ferguson Keathley, *Digital Asset Management* (Berkeley, CA: Apress, 2014), 16, <https://doi.org/10.1007/978-1-4302-6377-7>.

¹⁰⁸ Kose John, Maureen O'Hara, y Fahad Saleh, «Bitcoin and Beyond», *Annual Review of Financial Economics* 14, n.o 1 (1 de noviembre de 2022): 96, <https://doi.org/10.1146/annurev-financial-111620-011240>.



En este campo, el problema de los generales bizantinos cobra una clara aplicación práctica. Mediante el consenso de Nakamoto, es posible llevar un control que impida el doble gasto de un recurso nativo digital, bitcoins en el caso de este protocolo, sin la necesidad de contar con una autoridad central, o conjunto de ellas, que controle la circulación de estos. De esta manera, la tecnología *blockchain* es un sistema de registro digital que permite la creación y el mantenimiento de registros de transacciones de forma segura, transparente y distribuida.

Ahora bien, desde la publicación del *white paper* de Bitcoin ha habido una gran cantidad de desarrollos que han tomado el protocolo y modificado de diferentes formas. Ello ha dado lugar a otras implementaciones que pueden englobarse bajo la denominación de “tecnologías de registros distribuidos” -*distributed ledger technologies* (DLTs), en inglés-, siendo *blockchain* un caso particular dentro de estos. En este sentido, es posible realizar las siguientes distinciones sobre ambas:

1. Estructura de Datos: La tecnología *blockchain* utiliza una estructura de cadena de bloques, donde cada bloque contiene un conjunto de transacciones vinculadas en orden cronológico. En contraste, las tecnologías de registro distribuido pueden tener estructuras de datos diferentes, como grafos o registros dirigidos por eventos.¹¹⁰

2. Consenso: En la tecnología *blockchain*, se utiliza un mecanismo de consenso, como la prueba de trabajo -*proof of work*, en inglés- (PoW) o la prueba de participación -*proof of stake*, en inglés- (PoS), para alcanzar un acuerdo sobre la validez de las transacciones y la incorporación de nuevos bloques. En las tecnologías de registro distribuido, el mecanismo de consenso puede variar según la implementación específica.¹¹¹

3. Privacidad y Confidencialidad: La tecnología *blockchain* se caracteriza por su transparencia y visibilidad de las transacciones, ya que generalmente todos los participantes, tanto activos como pasivos, de la red tienen acceso a la cadena de bloques completa; dependiendo del tipo de protocolo puede haber grados de seudonimidad o anonimato, pero rara vez una plena asociación con la identidad real del participante activo de la red. Por otra parte, las tecnologías de registro distribuido pueden permitir diferentes niveles de privacidad y confidencialidad, permitiendo el cifrado de datos o la gestión selectiva de la visibilidad de la información, pero, en general, manteniendo un registro de identidad sobre quienes forman parte de la red.¹¹²

¹⁰⁹ Harish Natarajan, Solvej Krause, y Helen Gradstein, «Distributed Ledger Technology and Blockchain», *Fintech Note* (World Bank Group, 2017), 1, <http://hdl.handle.net/10986/29053>.

¹¹⁰ Luis Vargas, Jean Bacon, y Ken Moody, «Event-Driven Database Information Sharing», en *Sharing Data, Information and Knowledge*, ed. Alex Gray, Keith Jeffery, y Jianhua Shao, vol. 5071, *Lecture Notes in Computer Science* (Berlin, Heidelberg: Springer Berlin Heidelberg, 2008), 113-25, https://doi.org/10.1007/978-3-540-70504-8_11; Xing Liu, Bahar Farahani, y Farshad Firouzi, «Distributed Ledger Technology», en *Intelligent Internet of Things: From Device to Fog and Cloud*, ed. Farshad Firouzi, Krishnendu Chakrabarty, y Sani Nassif (Cham: Springer International Publishing, 2020), 393-431, https://doi.org/10.1007/978-3-030-30367-9_8.

¹¹¹ Ver Arshdeep Singh et al., «A Survey and Taxonomy of Consensus Protocols for Blockchains», *Journal of Systems Architecture* 127 (1 de junio de 2022): 102503, <https://doi.org/10.1016/j.sysarc.2022.102503>.

¹¹² Sara Barj, Aafaf Ouaddah, y Abdellatif Mezrioui, «A Review of Privacy-Preserving Cryptographic Techniques Used in Blockchain Platforms», en *Digital Technologies and Applications*, ed. Saad Motahhir y Badre Bossooui, *Lecture Notes in Networks and Systems* (Cham: Springer Nature Switzerland, 2023), 230-40, https://doi.org/10.1007/978-3-031-29857-8_23.



4. Escalabilidad: La escalabilidad es un desafío común en la tecnología *blockchain*, ya que el crecimiento de la cadena de bloques puede ralentizar el rendimiento y aumentar los costos de almacenamiento; ciertos protocolos, como el PoW demandan más recursos por las características propias del mismo. Algunas tecnologías de registro distribuido están diseñadas con enfoques alternativos para abordar la escalabilidad, como la fragmentación o el uso de estructuras de datos más eficientes.¹¹³

Dentro de esta visión de eliminar intermediarios, también cobra relevancia la noción de *smart contract*, los cuales fueron propuestos bajo este nombre por Nick Szabo en la década de los 90s,¹¹⁴ pero que recién con la aparición de la tecnología *blockchain* vieron un desarrollo substancial.¹¹⁵ De forma sintética, un contrato inteligente es un programa informático que ejecuta y hace cumplir automáticamente ciertos términos codificados como lenguaje informático. Estos contratos están diseñados para ser autoejecutables y autónomos, lo que significa que se activan automáticamente cuando se cumplen ciertas condiciones predefinidas. Además, los contratos inteligentes eliminan la necesidad de confiar en terceros, ya que la lógica y las reglas del contrato están codificadas en el código del programa y se ejecutan de acuerdo con las reglas establecidas.

En lo que concierne al derecho, y particularmente con foco en la protección de derechos humanos, es posible remarcar una doble perspectiva sobre este fenómeno. Por un lado, se ha remarcado la capacidad de estas tecnologías para proporcionar un registro inmutable y verificable de transacciones ha llevado a explorar su aplicación en áreas como la protección de la identidad digital, la capacidad de crear registros inmutables puede ser utilizada para documentar y proteger los derechos de las personas, especialmente en países con instituciones débiles o donde el acceso a la justicia es limitado, la votación electrónica y la protección de los derechos de propiedad intelectual, entre otros. Al mismo tiempo, las preocupaciones sobre las posibles violaciones han crecido y las supuestas incompatibilidades de la tecnología con estos derechos.

En particular, cuando estas tecnologías son usadas por individuos, es muy probable que sus datos personales se encuentren involucrados.¹¹⁶ Es fundamental recordar que una *blockchain* no deja de ser una forma técnica para organizar el almacenaje y uso de cierta información. Teóricamente, el uso de *blockchain* puede dar lugar a una situación donde el derecho a la protección de los datos personales se encuentre reforzado y menoscabado al mismo tiempo. Ciertas aplicaciones que

¹¹³ Muhammad Hassan Nasir et al., «Scalable Blockchains — A Systematic Review», *Future Generation Computer Systems* 126 (1 de enero de 2022): 136-62, <https://doi.org/10.1016/j.future.2021.07.035>.

¹¹⁴ Nick Szabo, «Smart Contracts», *Nick Szabo's Essays, Papers, and Concise Tutorials* (blog), 1994, <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>.

¹¹⁵ Anna Vacca et al., «A Systematic Literature Review of Blockchain and Smart Contract Development: Techniques, Tools, and Open Challenges», *Journal of Systems and Software* 174 (1 de abril de 2021): 110891, <https://doi.org/10.1016/j.jss.2020.110891>.

¹¹⁶ Michèle Finck, European Parliament, y Directorate-General for Parliamentary Research Services, «Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?», (European Parliamentary Research Service, julio de 2019), 14-36, http://publications.europa.eu/publication/manifestation_identifier/PUB_QA0219516ENN.



serán exploradas en este comentario, como la identidad digital basada en esta tecnología, se alinea perfectamente con la idea de control sobre los datos que el derecho a la protección de datos personales busca efectivizar.¹¹⁷ Ahora bien, la inmutabilidad que caracteriza a estos protocolos podría entrar en choque directo con ciertos derechos relativos a la protección de datos personales, como el derecho al olvido. Volveremos sobre esta problemática en el primer estudio de caso de este comentario en la sección 3.A.

A. Tipos de protocolo

El tipo de infraestructura puesta en funcionamiento es clave para determinar el posible impacto a los derechos humanos en juego. En ese sentido, el siguiente apartado hará, de forma sucinta, una recopilación de las principales variaciones de esta tecnología. Al respecto de ello es posible distinguir entre las redes irrestrictas y las permitidas;¹¹⁸ generalmente también suele usar los términos de redes abiertas y cerradas.¹¹⁹ En el medio de ambos extremos, es posible encontrar situaciones híbridas; en la región, por ejemplo, el esquema de LACChain puede ser enmarcado bajo el mismo.¹²⁰

Respecto de los registros permitidos, se exige que los participantes sean autorizados antes de unirse a la red. Los permisos y roles de los participantes están claramente definidos, lo que permite un mayor control y gobernanza. Por otro lado, un registro no permitido o irrestricto, tal como su nombre lo indica, no requiere tal autorización para formar parte de la red. Cualquier persona puede unirse, participar en la validación de transacciones y acceder a la información almacenada. Este tipo de red se alinea con los principios de apertura y descentralización, lo que puede ser especialmente relevante en el ámbito de los derechos humanos, donde la transparencia y la inclusión son fundamentales, tal como exploraremos en la siguiente sección. La utilización de este tipo de *blockchain* puede facilitar la participación ciudadana y la protección de los derechos fundamentales.

B. Roles y control

Las bases de datos y redes de transmisión de información pueden adoptar diferentes formas. Los estudios al respecto de este tema pueden remontarse al análisis de Paul Baran, quien había distinguido entre las redes centralizadas, descentralizadas y distribuidas.¹²¹ El foco del análisis

¹¹⁷ Andrés Chomczyk Penedo, «Self-Sovereign Identity Systems and European Data Protection Regulations: An Analysis of Roles and Responsibilities», vol. P-312, Lecture Notes in Informatics (LNI) - Proceedings (Open Identity Summit 2021, Denmark: Gesellschaft für Informatik, 2021), 104.

¹¹⁸ Natarajan, Krause, y Gradstein, «Distributed Ledger Technology and Blockchain», 11-14.

¹¹⁹ Puthal et al., «Everything You Wanted to Know About the Blockchain», 11-12.

¹²⁰ Ver <https://www.lacchain.net/the-blockchain>, fecha de acceso 27 de junio de 2023.

¹²¹ Paul Baran, «I. Introduction to distributed communications networks», Memorandum, On Distributed Communications (Santa Monica, California: The RAND Corporation, agosto de 1964), 2, https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf.



giraba sobre la vulnerabilidad que representaba la menor cantidad de puntos centrales para la información en caso de un ataque a la red que pudiera comprometer la base de datos.

También es posible distinguir entre los roles que pueden ocupar los diferentes participantes de la red. Se puede comenzar con los mineros, quienes son los encargados de verificar y validar las transacciones; para ello, utilizan su poder de cómputo para resolver complejos problemas matemáticos y agregar nuevos bloques a la cadena. Como contrapartida a cambio de su trabajo, los mineros reciben recompensas, como criptomonedas, por ejemplo, en el caso de Bitcoin.¹²² Su función principal es asegurar la integridad de la cadena de bloques y mantener la seguridad de la red. Dependiendo del protocolo, puede ser que la función de los mineros varíe y, por extensión, cambie como se generan nuevos bloques.

En segundo lugar, tenemos a los nodos validadores, quienes son participantes de la red que se encargan de verificar y validar las transacciones sin la necesidad de resolver problemas matemáticos complejos como lo hacen los mineros.¹²³ Estos nodos participan en el proceso de consenso de la red y se aseguran de que las transacciones cumplan con las reglas establecidas. Los nodos validadores pueden tener diferentes niveles de autoridad en la red, dependiendo de su reputación y participación en la validación de transacciones. En aquellas redes que operan bajo PoS es común encontrar este tipo de nodos dado el giro del minado a la tenencia de 'participaciones'.

En tercer lugar, es posible encontrar a los nodos plenos, quienes son participantes de la red que almacenan una copia completa de la cadena de bloques y la mantienen actualizada.¹²⁴ Estos nodos se encargan de transmitir y propagar las transacciones y bloques a través de la red. Los nodos completos verifican la integridad de la cadena de bloques y realizan comprobaciones de consenso para garantizar que la información sea precisa y confiable.

Por último, están los usuarios, que suelen ser denominados también nodos ligeros, ya que son participantes de la red que no almacenan una copia completa de la cadena de bloques.¹²⁵ En lugar de eso, confían en otros nodos de la red para obtener información y verificar transacciones. Los nodos ligeros son más livianos en términos de almacenamiento y recursos computacionales, lo que los hace adecuados para dispositivos con capacidades limitadas, como teléfonos móviles, o cuando no es necesario o relevante operar como nodo completo.

¹²² «OECD Blockchain Primer» (OECD), 7, accedido 28 de junio de 2023, <https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf>.

¹²³ Puthal et al., «Everything You Wanted to Know About the Blockchain», 11-12.

¹²⁴ Dylan Yaga et al., «Blockchain Technology Overview» (Gaithersburg, MD: National Institute of Standards and Technology, octubre de 2018), 3, <https://doi.org/10.6028/NIST.IR.8202>.

¹²⁵ Yaga et al., 3.



V. Estudio de casos

Ahora bien, el estudio de una tecnología en abstracto puede resultar adecuado en ciertas condiciones, pero, al mismo tiempo, puede dar lugar a resultados de investigación que no sean los más adecuados. Por ejemplo, y en relación con la temática de este informe, se han producido gran cantidad de trabajos académicos, particularmente en el campo del derecho humano a la privacidad, que han arribado a conclusiones opuestas por analizar la tecnología fuera de una aplicación concreta.¹²⁶

Considerando que numerosos proyectos han sido financiados por organismos multilaterales, ello puede tomarse como una apuesta por explorar la tecnología y comprobar si, efectivamente, las promesas realizadas pueden ser cumplidas. En este sentido, expondremos brevemente los principales casos de uso explorados en la región y reflexionaremos sobre los desafíos que los mismos importan para diferentes derechos humanos bajo el prisma de la legislación latinoamericana.

Es por ello por lo que los casos de estudio seleccionados tienen por objetivo explorar el uso concreto de la tecnología con relación a un determinado derecho humano en juego en el contexto del Sistema Interamericano de Derechos Humanos ("SIDH").

A. Identidad y derechos a la privacidad y la protección de datos

La identidad es un elemento esencial de la personalidad humana. Siguiendo una estructura utilizada previamente, la identidad humana se encuentra compuesta por elementos inherentes a la persona, como sus características físicas, adquiridos por esta, como una habilidad desarrollada por medio de la práctica, y asignados por terceros, como un número de identificación.¹²⁷ Nuestra identidad es lo que nos permite, por medio de la combinación de los elementos antes mencionados, distinguarnos de otras personas y configurar nuestra personalidad. Tal es la importancia de la identidad que ella ha sido reconocida como un derecho humano en diferentes instrumentos internacionales,¹²⁸ en este sentido, el SIDH no es una excepción a ello ya que en sus artículos 11, 18, y 20 reconoce diferentes elementos de la identidad humana como elementos jurídicamente protegidos.

¹²⁶ A modo de ejemplo, se pueden citar los trabajos de Finck y de Moerel, quienes llegan a conclusiones totalmente opuestas (ver Finck, European Parliament, y Directorate-General for Parliamentary Research Services, «Blockchain and the General Data Protection Regulation»; Lokke Moerel, «Blockchain & Data Protection...and Why They Are Not on a Collision Course», *European Review of Private Law* 6 (2019): 825-52.)

¹²⁷ Chomczyk, «Regulación de blockchain e identidad digital en América Latina», 16.

¹²⁸ Yussef Al Tamimi, «Human Rights and the Excess of Identity: A Legal and Theoretical Inquiry into the Notion of Identity in Strasbourg Case Law», *Social & Legal Studies* 27, n.o 3 (junio de 2018): 283-98, <https://doi.org/10.1177/0964663917722598>; Chomczyk, «Regulación de blockchain e identidad digital en América Latina», 16.



Ahora bien, los elementos que conforman la identidad de cada persona también pueden ser considerados como datos personales.¹²⁹ Con lo cual, la identidad esta doblemente protegida por dos derechos diferentes. Sin embargo, el derecho a la protección de datos personales no siempre posee el rango de derecho humano. En lo que concierne al SIDH, no encontramos cláusulas que contemplen tal protección, sin perjuicio del Artículo 11.2 sobre la protección de la vida privada.¹³⁰

Por las características propias de los diferentes procesos de digitalización, los sistemas de identidad se han caracterizado por ser puesto en marcha de forma centralizada por actores públicos y privados, principalmente a los efectos de contar con certeza sobre quien es la contraparte con la que se está interactuando en un momento determinado. En este sentido, registros nacionales de identidad se han ocupado de identificar a los “recursos” humanos en cada jurisdicción latinoamericana a los efectos de (i) conocer la población sobre la cual diseñar y aplicar políticas públicas y (ii) permitir la correcta identificación de las personas con relación a las actividades que realizan con el Estado.¹³¹ Por otra parte, las compañías privadas, particularmente aquellas cuya operatoria es digital, necesitan identificar a sus usuarios para la correcta asignación de derechos y la exigencia de obligaciones, según el caso.

En la era digital, los sistemas de identidad digital auto-soberana -self sovereign identity (SSI) systems, en inglés- han surgido como una alternativa innovadora a los modelos de identidad tradicionales.¹³² Tal como su nombre lo señala, la premisa basal de estos sistemas de identidad es poner a la persona en total control de sus atributos que hacen a su identidad, facilitando la identificación de quien tiene acceso a los mismos y bajo que condiciones. En otras palabras, estos sistemas permiten a los individuos tener un mayor control sobre su propia identidad en línea, empoderándolos para gestionar y compartir su información personal de manera segura. Si bien es posible trazar conexiones con propuestas anteriores, la actual configuración de los sistemas SSI está basada en el modelo de Christopher Allen.¹³³

Aunque las configuraciones pueden variar de sistema a sistema,¹³⁴ su aspecto central radica en el uso de “(...) repositorios personales portables en los que podemos almacenar y administrar todas nuestras claves privadas, nuestros autenticadores y nuestros tokens y credenciales digitales de manera segura y confiable.”¹³⁵ En función de la estructuración del sistema, nos podemos

¹²⁹ Chomczyk, «Regulación de blockchain e identidad digital en América Latina», 18.

¹³⁰ Al respecto de ello, es menester señalar que el derecho a la privacidad es un derecho diferente del derecho a la protección de datos personales, particularmente en el sistema europeo, a pesar de compartir una raíz común (ver Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer Science & Business, 2014); Felix Bieker, *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law*, vol. 34, Information Technology and Law Series (The Hague: T.M.C. Asser Press, 2022), <https://doi.org/10.1007/978-94-6265-503-4>.)

¹³¹ Mia Elisabeth Harbitz, Juan Carlos Benítez Molina, y Iván Arcos Axt, «Inventario de los registros civiles e identificación de América Latina y el Caribe» (Banco interamericano de Desarrollo, septiembre de 2010); Chomczyk, «Regulación de blockchain e identidad digital en América Latina», cap. 4.

¹³² Marcos Allende López, *Identidad digital auto-gestionada: El futuro de la identidad digital: Auto-gestión, billeteras digitales y blockchain* (Inter-American Development Bank, 2020), 28, <https://doi.org/10.18235/0002635>.

¹³³ Christopher Allen, «The Path to Self-Sovereign Identity», *Blog, Life With Alacrity (blog)*, 25 de abril de 2016, <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>.

¹³⁴ Daniela Pöhn, Michael Grabatin, y Wolfgang Hommel, «EID and Self-Sovereign Identity Usage: An Overview», *Electronics* 10, n.o 22 (enero de 2021): 17-22, <https://doi.org/10.3390/electronics10222811>.

¹³⁵ Allende López, *Self-Sovereign Identity*, 28.



encontrar con que la funcionalidad central sea guardar los datos y permitir únicamente lectura de los mismos o simplemente ser una interfaz para el ejercicio de derechos asociados a los datos. En todo caso, su común denominador está dado por el uso de tecnología blockchain o DLT para permitir el control directo por parte de los usuarios.

El proyecto DIDI en Argentina¹³⁶

En 2018, Bitcoin Argentina y el laboratorio de innovación del Grupo Banco Interamericano de Desarrollo (BID Lab) se unieron para crear el Proyecto DIDI, oficialmente conocido como “Inclusión cívica, social y económica de habitantes de barrios vulnerables en Buenos Aires mediante modelos de Blockchain”. El objetivo de este proyecto era investigar, implementar y evaluar los beneficios de un modelo de identidad digital autogestionada aplicado a la inclusión social, cívica y económica de residentes en barrios vulnerables de Argentina.

Como parte de este proyecto, se desarrolló una aplicación móvil llamada ai-di, que funciona como un porta-documentos digital y permite a las personas almacenar credenciales relacionadas con aspectos sociales, cívicos y económicos. La aplicación ai-di, construida siguiendo los principios de la identidad digital autogestionada o self-sovereign identity (SSI), se implementó, principalmente, en poblaciones no bancarizadas de barrios populares del Gran Buenos Aires.

Los principales desafíos regulatorios fueron analizados en un informe separado, que sirven de base a las consideraciones legales a continuación.¹³⁷

Como señalamos previamente, los sistemas de identidad pueden comprometer dos derechos: el derecho a la protección de datos y el derecho a la identidad. Respecto del primero, su consideración como derecho humano, dentro del SIDH, es más complejo; en la actualidad, y sin perjuicio del dictado de normativas sobre la materia, pocos países de la región han elevado este derecho al rango de derecho constitucional, mucho menos al de derecho humano.¹³⁸ A pesar de ello, la región se encuentra haciendo avances sobre la materia. Por el otro lado, el derecho a la identidad cuenta con plena incorporación, por medio de diferentes provisiones, al SIDH. En atención a ello, cabe reparar como los sistemas SSI pueden comprometer estos derechos en juego.

¹³⁶ «Proyecto DIDI: Aprendizajes, resultados y desafíos de la identidad digital auto-gestionada para la inclusión» (Banco Interamericano de Desarrollo, 10 de abril de 2023), <https://didi.org.ar/2023/04/10/proyecto-didi-aprendizajes-resultados-y-desafios-de-la-identidad-digital-auto-gestionada-para-la-inclusion/>.

¹³⁷ Ver Chomczyk, «Regulación de blockchain e identidad digital en América Latina».

¹³⁸ Tannia C. Mayorga Jácome et al., «Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos», *Dominio de las Ciencias* 5, n.o 1 (2019): 518-37.



Respecto del derecho a la protección de datos personales, es posible que estos sistemas pueden fortalecer el mismo ya que permiten a los individuos tener un mayor control sobre su información personal, lo cual está en línea con los principios básicos de este derecho. Gracias a ello, estos sistemas pueden proporcionar una mayor seguridad en la gestión de la identidad, lo que ayuda a prevenir el fraude y el robo de identidad. Al permitir que los individuos tengan un control más sólido sobre su información personal, se reduce la vulnerabilidad a posibles ataques o mal uso de datos de identidad. Sin embargo, puede ocurrir que esto sea una ilusión y los usuarios terminen más cargados con obligaciones que en situaciones anteriores, particularmente si el consentimiento es usado como base legal.

En línea con esto, el derecho a la identidad guarda íntima relación con la autodeterminación informativa.¹³⁹ Pero, al igual que en la situación anterior, la falta de capacidades para ejercer este derecho puede ser un lastre innecesario que solo sirva para perpetuar o ampliar las desigualdades existentes si no se implementan de manera inclusiva y accesible para todos los individuos.

¿Cómo es posible paliar estos problemas y mejorar las posibilidades desde los marcos normativos? Considerando que el derecho a la protección de datos personales se encuentra en una posición más “débil”, es menester poner el foco allí. En ese sentido, es fundamental la revisión y actualización de leyes y regulaciones relacionadas con la privacidad, la protección de datos y los derechos digitales para abordar los desafíos y las oportunidades planteadas por estos sistemas.¹⁴⁰

B. Votación y el ejercicio de los derechos políticos

Otro caso de uso que ha sido explorado en la región son los sistemas de votación basados en tecnología *blockchain* que han surgido como una innovadora solución para mejorar la transparencia, la seguridad y la eficiencia de los procesos electorales. Estos sistemas permiten la votación en línea, utilizando la tecnología *blockchain* para garantizar la integridad de los votos y proteger la confidencialidad de los electores. Las propuestas de soluciones de votación sobre tecnología *blockchain* o DLT, según el caso, vienen a responder a muchas de las críticas existentes sobre los sistemas de votación electrónica.

La premisa central de estos es que el uso de una cadena de bloques para registrar y asegurar los votos en un entorno digital, al tratarse de un registro inmutable y transparente de cada voto emitido, es posible que cada transacción sea verificable y auditada por los participantes de la red, lo que aumenta la confianza en el proceso electoral. Considerando el uso de técnicas de criptografía y algoritmos de consenso para proteger los votos de posibles alteraciones o manipulaciones. La descentralización y la distribución de la información en la cadena de bloques también contribuyen

¹³⁹ Alexandra Giannopoulou, «Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity», *Digital Society* 2, n.o 2 (11 de mayo de 2023): 7, <https://doi.org/10.1007/s44206-023-00049-z>.

¹⁴⁰ Oportunamente habíamos realizado sugerencias en Chomczyk, «Regulación de blockchain e identidad digital en América Latina», 127.



a su seguridad. Técnicamente, los sistemas de votación basados en *blockchain* o DLT deberían permitir preservar la privacidad y confidencialidad de los electores, garantizando el anonimato del voto y evitando cualquier posibilidad de identificar o rastrear la elección de un individuo.

Conforme el Artículo 23.b), toda persona tiene el derecho “(...) [d]e votar y ser elegidos en elecciones periódicas auténticas, realizadas por sufragio universal e igual y por voto secreto que garantice la libre expresión de la voluntad de los electores, (...)”. Esta caracterización del derecho a sufragar da algunas pautas que impactan directamente sobre el diseño del proceso electoral. En primer lugar, todo individuo tiene que poder emitir su voto y todos ellos deben estar en igualdad de condiciones. Esto implica que el método no puede discriminar, por ejemplo, en función de la ubicación de la persona; por ejemplo, las personas que están fuera de su país pueden, por lo general, emitir su voto por correo. Por otra parte, el mismo debe ser secreto, a fin de evitar coerciones sobre la expresión de la opinión política.

Por lo tanto, todo sistema de votación electrónico que pretenda resguardar estas garantías necesita, como mínimo aunque no exclusivamente, de lo siguiente: (i) secreto y libertad del voto, junto con la imposibilidad trazar el voto a su emisor; (ii) independencia del software; (iii) papeletas verificables por los votantes así como también la verificación de la identidad de estos; (iv) impugnabilidad, donde haya varias entidades involucradas en velar por el control; y (v) auditoría, particularmente transparencia de los actos en torno al procesos electoral.¹⁴¹ Ahora bien, ciertas investigaciones revelan que algunos proyectos propuestos de sistemas de votación basados en *blockchain* no logran reunir estos requisitos.¹⁴²

Elecciones estudiantiles en Colombia usando blockchain¹⁴³

En el año 2018 y 2019, se realizaron dos pruebas piloto en colegios de la ciudad de Bogotá en el marco del proceso de votación del Gobierno Escolar; en particular, los estudiantes votaron mediante tecnología blockchain a las personas para el cargo de Personero Estudiantil. El piloto implicó un doble desarrollo: por un lado, una interfaz web para facilitar la emisión del voto en un formato ajustado a las características del electorado; y, por el otro, un desarrollo en Ethereum para la votación en sí misma.

¹⁴¹ Sunoo Park et al., «Going from Bad to Worse: From Internet Voting to Blockchain Voting», *Journal of Cybersecurity* 7, n.o 1 (16 de febrero de 2021): 3, <https://doi.org/10.1093/cybsec/tyaa025>; Friðrik P. Hjálmarsson et al., «Blockchain-Based E-Voting System», en *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, 983, <https://doi.org/10.1109/CLOUD.2018.00151>.

¹⁴² Jun Huang et al., «The Application of the Blockchain Technology in Voting Systems: A Review», *ACM Computing Surveys* 54, n.o 3 (17 de abril de 2021): 10-11, <https://doi.org/10.1145/3439725>.

¹⁴³ «Informe Final de Resultados Prototipo Blockchain» (Alcaldía Mayor de Bogotá D.C. - Universidad Nacional de Colombia - ViveLab Bogotá, 31 de julio de 2018), <https://tic.bogota.gov.co/documentos/informe-final-resultados-prototipo-blockchain>; «Implementación del prototipo Blockchain para procesos electorales en colegios públicos segunda edición» (Alcaldía Mayor de Bogotá D.C., 23 de abril de 2019), <https://tic.bogota.gov.co/documentos/blockchain-elecciones-estudiantiles>.



Si bien los informes publicados por la Alcaldía de Bogotá hacen un gran énfasis en los desafíos tecnológicos detrás de estos proyectos, hay pocas referencias a los desafíos regulatorios que ellos han implicado. Los únicos reparos del sistema de voto electrónico usando tecnología *blockchain* han sido sobre el uso de datos personales. En ese sentido, las autoridades involucradas consideraron oportuno que “(...) las fotografías de los candidatos, sus nombres y apellidos, y cualquier otra información que pueda suponer un riesgo para su integridad sean tratados de forma privada.”¹⁴⁴ Tal es así que la arquitectura tecnológica fue ajustada para ello, además de adoptar medidas de carácter organizativo, en concreto “(...) un contrato de protección de datos entre la Universidad Nacional y cada una de las instituciones educativas participantes en este proceso, para poder utilizar la información de cada estudiante y así identificarlos en el sistema como individuos únicos habilitados para votar.”¹⁴⁵ Al respecto de las posibles implicaciones sobre el derecho al voto, los informes no dan cuenta de análisis alguno llevado a cabo sobre posibles afectaciones; todo lo contrario, una lectura global de los documentos lleva a considerar que estos pueden ser un facilitador para el ejercicio del derecho al voto.

La tecnología *blockchain* puede contribuir a garantizar la integridad electoral al proporcionar un registro transparente y a prueba de manipulaciones, a expensas de introducir mayor complejidad.¹⁴⁶ Ello no exclusivo de este tipo de implementaciones sino que se trata de una problema común con los sistemas electrónicos de voto,¹⁴⁷ los cuales han tenido malas experiencias en la región.¹⁴⁸ Sin embargo, dada la mayor cantidad de variables que pueden ser introducidas, ciertos estudios argumentan la imposibilidad de compatibilizar esta tecnología con el proceso electoral.¹⁴⁹

A pesar de ello, los sistemas de votación basados en tecnología *blockchain* pueden mejorar la transparencia y la confianza en los procesos electorales, al permitir la verificación y auditoría de los votos por parte de los ciudadanos y los observadores. Esto puede contribuir a fortalecer la confianza en la democracia y en los resultados electorales.

¹⁴⁴ «Informe Final de Resultados Prototipo Blockchain», sec. 2.3. Es menester remarcar que muchas normativas latinoamericanas de protección de datos personales, se encuentran estructuras sobre el binomio de información pública/privada, dando menor protección a los datos de acceso público (ver []).

¹⁴⁵ «Informe Final de Resultados Prototipo Blockchain», sec. 2.3.

¹⁴⁶ Park et al., «Going from Bad to Worse», 9-10.

¹⁴⁷ Park et al., 1.

¹⁴⁸ Miguel González Madrid, «El voto electrónico en el mundo. Breve historia de experiencias acerca de un ascenso desigual», *Revista Mexicana de Estudios Electorales* 5, n.o 25 (25 de enero de 2021): 195; Marcelo José García Farjat, «Nuevas tecnologías, promesas y alienación tecnológica: una mirada crítica del fenómeno del voto electrónico como dispositivo técnico moderno», *ArtefactoS. Revista de estudios sobre la ciencia y la tecnología* 10, n.o 2 (29 de noviembre de 2021): 71-99, <https://doi.org/10.14201/art20211027199>.

¹⁴⁹ William Crumpler, Marti Flacks, y Amith Mandavilli, «The Human Rights Risks and Opportunities in Blockchain», 2021, 25-29.



En este sentido, los sistemas de votación basados en tecnología *blockchain* pueden fortalecer el ejercicio del derecho al voto libre y secreto, al proporcionar un entorno seguro y protegido para emitir los votos. Por otro lado, el uso de medios tecnológicos remotos permitiría facilitar la emisión del voto. En este sentido, pueden facilitar la participación política al permitir a los ciudadanos votar en línea, eliminando las barreras geográficas y mejorando la accesibilidad. Sin embargo, se debe tener en cuenta que no todos los ciudadanos tienen acceso a la tecnología o las habilidades digitales necesarias para participar en estos sistemas, lo que podría generar una brecha digital y afectar la inclusión de ciertos grupos en el proceso electoral.

C. Registro propiedad inmueble y el derecho a la propiedad

En línea con mejorar ciertos procesos, también se ha sugerido el uso de sistemas de registro de propiedad inmueble basados en tecnología *blockchain* como una alternativa innovadora para mejorar la eficiencia, la seguridad y la transparencia en la gestión de los registros de propiedad. Estos sistemas utilizan la tecnología *blockchain* para almacenar y gestionar la información relacionada con los derechos de propiedad de los bienes inmuebles. En este sentido, ha habido numerosas pruebas en diferentes jurisdicciones.¹⁵⁰

Explorar las particularidades de cada sistema jurídico en torno a los derechos de propiedad pueden ser una tarea titánica. En todo caso, los registros de la propiedad buscan responder ciertas preguntas que hacen a la seguridad jurídica, a saber: (i) ¿qué ocurre cuando una transacción es nula según la legislación pertinente? ; (ii) ¿cómo se debe tratar una transmisión válida cuando el vendedor no tiene el poder para disponer de ella debido a que no es el propietario?; (iii) ¿qué sucede cuando se declara nula una transferencia anterior en la cadena de transacciones?; (iv) si existen cargos ocultos o intereses superiores, ¿cómo afectarán a la persona que ha inscrito su derecho o contrato?; (v) ¿quién estará protegido en caso de una doble venta, es decir, si un vendedor ha vendido la misma propiedad a diferentes compradores?; y (vi) ¿quede el comprador registrado ser desalojado si alguien tiene un derecho o interés anterior sobre el terreno?¹⁵¹

Como respuesta a esto, existen dos grandes modelos: (i) el modelo de registración de escrituras, donde el registro tiene un efecto de publicidad; y (ii) el modelo de titularidad, donde el registro tiene un efecto constitutivo de derechos.¹⁵² Por otro lado, los registros pueden ser completos o incompletos; en este caso, la mayoría de los proyectos propuestos operan la bajo la lógica que la *blockchain* tendrá toda la información necesaria.¹⁵³

¹⁵⁰ Marina Vega Maza, «El auge de blockchain y sus posibilidades reales de aplicación en los registros de las administraciones públicas», *IDP. Revista de Internet, Derecho y Política*, n.o 28 (17 de febrero de 2019): 115-17, <https://doi.org/10.7238/idp.v0i28.3154>.

¹⁵¹ Nicolás Noguerol Peiró y Eduardo J. Martínez García, «Blockchain and Land Registration Systems», *European Property Law Journal* 6, n.o 3 (20 de diciembre de 2017): 297-98, <https://doi.org/10.1515/eplj-2017-0017>.

¹⁵² Georg von Wangenheim, «Blockchain-Based Land Registers: A Law-and-Economics Perspective», en *Disruptive Technology, Legal Innovation, and the Future of Real Estate*, ed. Amnon Lehavi y Ronit Levine-Schnur (Cham: Springer International Publishing, 2020), 108, https://doi.org/10.1007/978-3-030-52387-9_6.

¹⁵³ Benjamin Verheye, «Land Registration in the Twenty-First Century: Blockchain Land Registers from a Civil Law Perspective», en *Disruptive Technology, Legal Innovation, and the Future of Real Estate*, ed. Amnon Lehavi y Ronit Levine-Schnur (Cham: Springer International Publishing, 2020), 126-28, https://doi.org/10.1007/978-3-030-52387-9_7.



La tecnología *blockchain* permite crear un registro inmutable de los derechos de propiedad. Una vez que se registra una transacción en la cadena de bloques, no puede ser modificada o eliminada, lo que brinda mayor seguridad y confianza en la información registrada. Por otro lado, los sistemas de registro de propiedad basados en *blockchain* pueden proporcionar transparencia en la gestión de los registros. Cada transacción se registra en la cadena de bloques y está disponible para su verificación por parte de los participantes de la red, lo que contribuye a la confiabilidad del sistema. Idealmente, un sistema perfecto debería tener toda la información sobre el catastro de un país o jurisdicción en su bloque génesis.¹⁵⁴

Tal como sucede en el caso de la votación basada en tecnología *blockchain*, al utilizar técnicas criptográficas avanzadas para proteger la seguridad de la información registrada, junto con la descentralización y la distribución de la información en la cadena de bloques, se reducen el riesgo de pérdida o alteración de los datos de propiedad. Sin embargo, la descentralización necesita, en ciertos casos dependiendo de la configuración de la *blockchain* o DLT en cuestión, de la colaboración de quienes poseen las claves para firmar la transacción en cuestión cuando se produce un efecto jurídico sin que el titular de las claves haya realizado un acto positivo, como, por ejemplo, ante la muerte de una persona, sus herederos deberían poner a disposición la clave para firmar y realizar los efectos de la sucesión.¹⁵⁵

El derecho a la propiedad consta bajo el Artículo 21. Los sistemas de registro de propiedad inmueble basados en *blockchain* pueden fortalecer el derecho a la propiedad al proporcionar un registro seguro, inmutable y transparente de los derechos de propiedad. En particular, y considerablemente relevante para los sistemas latinoamericanos, la premisa fundamental de *blockchain* y las DLT -la encadenación de eventos mediante bloques- guarda una relación directa con el principio de tracto sucesivo y, además, la prevención del doble gasto podría facilitar la anotación de dos actos contradictorios.¹⁵⁶ Sin embargo, es importante garantizar que el sistema sea accesible para todos los propietarios y evite la discriminación o exclusión de ciertos grupos en el acceso a la tecnología o la participación en el sistema.

Caso de estudio: LAC PropertyChain¹⁵⁷

El proyecto LAC PropertyChain propone la construcción de un sistema informático para el registro de propiedades que involucre a todas las partes como miembros y que garantice la confiabilidad de elementos clave como la producción de documentos y la identidad del usuario. Este sistema se basa en un modelo de confianza que no requiere

¹⁵⁴ Verhey, 127.

¹⁵⁵ Verhey, 127.

¹⁵⁶ Peiró y García, «Blockchain and Land Registration Systems», 301-2.

¹⁵⁷ Todd Miller et al., «Tecnología blockchain: una forma de aumentar la confianza, mejorar la eficiencia y reducir los costos en los procesos de registro de propiedades», Nota Técnica (Banco Interamericano de Desarrollo, 18 de julio de 2022), 12-14, <https://publications.iadb.org/es/tecnologia-blockchain-una-forma-de-aumentar-la-confianza-mejorar-la-eficiencia-y-reducir-los-costos>.



que los participantes se conozcan ni confíen entre sí. La solución propuesta busca proporcionar mayor certeza procesal y accesibilidad a los propietarios actuales y futuros, así como mayor seguridad para gobiernos, bancos e industria inmobiliaria a través de firmas criptográficas, validación de identidad y consenso en la validación de datos.

La implementación de LAC PropertyChain utiliza el sistema *blockchain* Chromia, el cual combina un *backend* de base de datos relacional con las garantías de transparencia y seguridad de *blockchain*. El proyecto se enfoca en hacer más accesible el proceso de transferencia de propiedad, aumentar la transparencia y mejorar la seguridad de los datos. LAC PropertyChain utiliza mecanismos de identidad respaldados por proveedores digitales confiables y un libro mayor distribuido para almacenar un registro inmutable de todos los datos y acciones relacionados con un proceso de propiedad. Chromia es una *blockchain* altamente personalizable y de alto rendimiento que aborda problemas de escala y complejidad lógica. Con el algoritmo de consenso PBFT, las transacciones pueden aprobarse en cuestión de segundos.

Respecto de los desafíos regulatorios identificados, la mayoría de los países de América Latina y el Caribe (ALC) tienen sistemas de registro de la propiedad que se basan en la normativa histórica española, donde los registros juegan un papel clave para la publicidad de los derechos de propiedad sobre bienes inmuebles junto con los notarios actuando en la arista constitutiva de derechos. El mayor problema radica en los procedimientos largos y complicados que no brindan suficiente seguridad y excluyen a los usuarios de bajos ingresos, así como la falta de integración de datos catastrales y registrales; junto a ello, la falta de representación gráfica de los objetos de derecho en los sistemas de registro de escrituras dificulta la definición precisa de las parcelas. Sobre la base del prototipo desplegado en jurisdicción peruana, no se identificaron barreras legales o regulatorias insuperables para implementar la solución basada en *blockchain*, al margen de la necesidad de ajustar ciertos instrumentos para dotar de plena validez jurídica a los actos desarrollados sobre la *blockchain*, cuestión que también es remarcada por la doctrina de forma general.¹⁵⁸

Aunque la publicidad es un principio rector de la actividad de toda dependencia pública, en el caso que nos ocupa puede comportar una afectación al derecho a la privacidad. Si bien la tecnología *blockchain* garantiza la integridad y la transparencia de la información registrada, también plantea desafíos en términos de privacidad. Los datos de propiedad almacenados en la cadena de bloques pueden ser accesibles para los participantes de la red, lo que requiere medidas de protección adecuadas para garantizar la confidencialidad de la información personal y evitar posibles abusos.

¹⁵⁸ Peiró y García, «Blockchain and Land Registration Systems», 314.



La vulnerabilidad es un vector común con otros casos bajo análisis. Existe el riesgo de que los sistemas de registro de propiedad basados en *blockchain* puedan exacerbar las desigualdades existentes o afectar a las minorías y grupos vulnerables. Por ejemplo, aquellos que no tienen acceso a la tecnología o a la educación digital podrían enfrentar barreras para participar en el sistema, lo que podría agravar la brecha digital y la exclusión de ciertos segmentos de la población. Asimismo, se debe garantizar que los sistemas de registro de propiedad basados en *blockchain* sean accesibles y estén disponibles para todos los propietarios, independientemente de su nivel de acceso a la tecnología o su ubicación geográfica. Esto implica proporcionar alternativas para aquellos que no tienen acceso a la tecnología, como opciones de registro físico o asistencia en la participación en el sistema.

La tecnología *blockchain* puede facilitar la resolución de disputas y el acceso a la justicia en casos de conflicto de propiedad. Al contar con registros inmutables y transparentes, se facilita la verificación de los derechos de propiedad y se agiliza el proceso de resolución de disputas. En este sentido, los sistemas de registro de propiedad basados en **blockchain** pueden proporcionar mayor seguridad y protección de los derechos de propiedad. Al garantizar la integridad y la transparencia de los registros, se reduce el riesgo de fraude, disputas y violaciones de los derechos de propiedad.

Los sistemas de registro de propiedad basados en *blockchain* pueden agilizar los procesos burocráticos asociados a la transferencia de propiedad. Al eliminar intermediarios y facilitar la verificación de la información, se reducen los costos y los tiempos involucrados en los trámites, lo que beneficia a los propietarios y promueve la eficiencia en la gestión de la propiedad. Sin embargo, la automatización irrestricta y la eliminación de intermediarios, como notarios, presenta ciertos problemas, particularmente para poblaciones vulnerables; la inclusión de estos actores, particularmente en los casos donde el registro opera como mecanismo de publicidad, como los notarios para hacer el control de legalidad de los actos y de asesoramiento jurídico, puede ser fundamental.¹⁵⁹

D. Dinero como instrumento de ejercicio de derechos humanos

Finalmente, es posible explorar las implicancias que tiene la aparición de un sistema monetario alternativo, particularmente en los supuestos contextos de inestabilidad latinoamericanos,¹⁶⁰ junto a problemas sobre la inclusión financiera.¹⁶¹ Como hemos reseñado previamente, los sistemas de dinero como Bitcoin han surgido como una alternativa descentralizada y digital al dinero tradicional, particularmente como reacción a los problemas de emisión monetario irrestricta, problema común en América Latina,¹⁶² y la falta de responsabilidad por parte de quienes tienen a cargo.

¹⁵⁹ Peiró y García, 307-9.

¹⁶⁰ «Informe de Economía Latinoamericana. Primer semestre de 2022», 2022; «Estudio Económico de América Latina y el Caribe 2022: dinámica y desafíos de la inversión para impulsar una recuperación sostenible e inclusiva», 2022.

¹⁶¹ Lisana Belén Martínez et al., «Instrumentos financieros clave para la inclusión financiera en América Latina», *Revista Finanzas y Política Económica* 14, n.o 1 (junio de 2022): 17-47, <https://doi.org/10.14718/revfinanzpolitecon.v14.n1.2022.2>.

¹⁶² Ramón Pineda Salazar y N. Alejandra Acevedo, «Financiamiento mediante emisión monetaria en América Latina, 1960-2016», 29 de julio de 2021, <https://repositorio.cepal.org/handle/11362/47137>.



Dentro del marco de una sociedad basada en el intercambio de bienes y servicios como motor económico, por un lado, y basada en la apertura social y de intercambio de ideas, del otro, contando el dinero el principal instrumento para facilitar dicha operación, los instrumentos monetarios pasan a cobrar un rol clave en el ejercicio de cualquier otro derecho.¹⁶³ En otras palabras, por ejemplo, ¿de qué sirve el derecho a la libertad de expresión si no se tienen los medios para comunicar las ideas? Este mismo criterio puede ser llevado a cualquier otro ámbito, como por ejemplo la libertad de culto y la posibilidad de contribuir con el proyecto espiritual que la persona considere relevante. El derecho a transaccionar, en este sentido, podría ser considerado como el punto de partida para el ejercicio de cualquier otro derecho en el marco de una economía de mercado, propia de los tiempos actuales.

A medida que progresa la digitalización del dinero,¹⁶⁴ las posibilidades de vigilancia crecen.¹⁶⁵ De allí que contar con instrumentos fuera del control estatal cobran una importancia fundamental. En una sociedad abierta, en la que la privacidad es primordial,¹⁶⁶ la posibilidad de realizar transacciones financieras sin vigilancia o seguimiento constantes fomenta un entorno propicio para el ejercicio de las libertades civiles.

Ahora bien, en el caso de las monedas basadas en tecnología *blockchain*, dado que las transacciones en la cadena de bloques son transparentes, es necesario asegurar que la identidad de los participantes no siempre este asociada directamente a las transacciones. De lo contrario, existe el riesgo de que la privacidad de los usuarios pueda verse comprometida si se vinculan sus identidades con las direcciones de las transacciones. Esto plantea desafíos en cuanto a la protección de la privacidad y los derechos de los usuarios, en particular cuando las operaciones pueden ser asociadas con datos personales sensibles.

Por otro lado, y en relación con problemáticas antes identificadas, estos sistemas demandan tanto acceso a la tecnología como la educación digital para usarla, lo cual puede toparse con barreras existentes en la población para participar en estos sistemas. Esto podría resultar en la exclusión financiera de ciertos grupos de la sociedad y acentuar las desigualdades existentes.

La separación entre Estado y moneda implica carecer de respaldo por una entidad pública central, lo cual puede derivar en riesgos adicionales para los consumidores en términos de seguridad, protección contra el fraude y mecanismos de resolución de disputas. En particular, algunos sistemas de dinero basados en *blockchain* están diseñados para ser resistentes a la inflación y la manipulación por parte de gobiernos o entidades centrales. Esto puede proteger a los individuos de la pérdida de valor de sus activos financieros y contribuir a la lucha contra la corrupción y la manipulación financiera.

¹⁶³ Jerry Brito, «The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society» (CoinCenter, 6 de febrero de 2019), 13, <https://coincenter.org/files/2019-02/the-case-for-electronic-cash-coin-center.pdf>.

¹⁶⁴ Bill Maurer, *How Would You Like to Pay? How Technology Is Changing the Future of Money* (Duke University Press, 2015).

¹⁶⁵ Josh Lauer, *Creditworthy: A History of Consumer Surveillance and Financial Identity in America* (New York: Columbia University Press, 2017).

¹⁶⁶ Brito, «The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society», 14.



Sin embargo, estos sistemas permiten a los usuarios tener un mayor control sobre sus activos financieros. Esto puede empoderar a los individuos y promover su autonomía económica, lo que se alinea con el derecho a la libertad económica y la propiedad privada. Buena parte de esta libertad radica en la posibilidad de facilitar las transferencias de dinero transfronterizas de manera más rápida y económica en comparación con los sistemas tradicionales, elemento clave para la sociedad digital e internacional. Esto puede contribuir al acceso a servicios financieros para personas en regiones con infraestructura financiera limitada, lo que puede tener un impacto positivo en los derechos económicos y sociales.

VI. Conclusiones

Como se ha explorado en este breve artículo, la tecnología *blockchain* necesita ser analizada en situaciones concretas, donde la potencial tensión entre los supuestos beneficios y los posibles riesgos sobre estos derechos pueda ser identificada. A modo de comparación, es posible traer las reflexiones de Lokke Moerel al estudiar la aplicabilidad del régimen de protección de datos personales a la tecnología *blockchain*, quien señalaba que se trataba de un ejercicio tan inútil como pretender aplicar la normativa a Internet en general, buscando quienes son los responsables del tratamiento de la red que conecta a todo el mundo.¹⁶⁷

Del estudio de los cuatro casos de uso (identidad digital, votación electrónica, registración de propiedad, y dinero digital) propuestos en este artículo, es posible identificar una particular preocupación por el derecho a la protección de datos personales y, en segunda instancia, sobre el derecho a la privacidad. En ese sentido, es fundamental recordar que *blockchain* no es más que una tecnología para la organización de información y su gestión en un ambiente donde estos procesos son realizados entre entidades que no, necesariamente, confían entre sí. Ahora bien, en estos casos concretos hemos podido identificar que una de las mayores inquietudes gira sobre dos características clave inherentes a estas tecnologías: la inmutabilidad y la transparencia de los datos almacenados.

La inmutabilidad hace referencia a la incapacidad de modificar o eliminar información una vez que ha sido registrada en ciertos sistemas, como la tecnología *blockchain*. La inmutabilidad puede ser beneficiosa en términos de seguridad y veracidad de los datos, particularmente en contextos como el latinoamericano donde instituciones débiles han dado lugar a la manipulación de información en diferentes situaciones, desde la alteración de cifras de inflación hasta violaciones del derecho a la identidad de niñas y niños de personas secuestradas durante dictaduras militares.

Sin embargo, esa inmutabilidad también conlleva desafíos significativos en lo que respecta a la autodeterminación informativa de las personas, elemento central del derecho a la protección de datos personales, que se estructura sobre la base de poder cambiar la información que lo con-

¹⁶⁷ Moerel, «Blockchain & Data Protection...and Why They Are Not on a Collision Course», 832-33.



figura a uno como persona. Si la información siempre se encontrará disponible sin posibilidad efectiva de eliminación, la persona se puede volver esclava de esa situación. Basta recordar la decisión del Tribunal de Justicia de la Unión Europea en el caso Costeja,¹⁶⁸ donde al mismo que se consagraba el llamado “derecho al olvido” también se “perpetuaba” el hecho que el Sr. Costeja fuera deudor de la seguridad social española en una sentencia judicial de acceso público irrestricto.

En relación con el segundo aspecto, la naturaleza pública de la información plantea un escenario propicio para el uso de herramientas de vigilancia facilitadas por estas tecnologías. La exposición masiva de datos puede tener consecuencias significativas, como el riesgo de manipulación, la segmentación de la publicidad invasiva y el potencial para crear perfiles detallados de individuos sin su conocimiento y/o su consentimiento.¹⁶⁹ Esto puede conducir a la creación de un entorno donde la vigilancia constante y generalizada se convierta en la norma, erosionando el derecho a la privacidad y la sensación de seguridad y libertad que deben acompañar la vida en sociedad.

Aunque la publicidad puede ser algo beneficioso en una *blockchain*, como por ejemplo en casos donde expertos independientes han podido recuperar criptomonedas apropiadas indebidamente siguiendo la información pública en la *blockchain* de Bitcoin, estos riesgos de identificación son reales. En este sentido, es relevante mencionar que, aunque este artículo no aborda detalladamente esta cuestión, existen ciertas configuraciones tecnológicas que buscan contrarrestar estos problemas. Entre ellas, destaca el uso de “*zero-knowledge proofs*” o pruebas de conocimiento cero, una técnica criptográfica que permite verificar la veracidad de una afirmación sin revelar la información real detrás de ella.¹⁷⁰ Estas herramientas pueden favorecer el anonimato y la protección de datos, al tiempo que brindan una mayor confianza en la validación de la información.

En conclusión, si bien *blockchain* y, de forma más amplia, las DLTs ofrecen múltiples beneficios y oportunidades para mejorar tanto el ejercicio como la protección de ciertos derechos humanos, incluyendo el derecho a la protección de datos y el derecho a la privacidad, es fundamental abordar de manera proactiva las cuestiones relacionadas con la inmutabilidad y la publicidad de la información almacenada en estas bases de datos. Esto implica equilibrar la innovación tecnológica con el respeto a los derechos humanos, tanto en la aplicación como en el desarrollo de marcos regulatorios sólidos en esta era digital en constante evolución.

¹⁶⁸ Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, No. C-131/12 (Tribunal de Justicia de la Unión Europea (Gran Sala) 13 de mayo de 2014).

¹⁶⁹ No es intención de este artículo ingresar en la discusión sobre que bases legales para el tratamiento de datos personales son aptas para la formación de perfiles, debate que se encuentra en plena discusión en la Unión Europea.

¹⁷⁰ Darko Čapko, Srđan Vukmirović, y Nemanja Nedić, «State of the Art of Zero-Knowledge Proofs in Blockchain», en 2022 30th Telecommunications Forum (TELFOR), 2022, 1-4, <https://doi.org/10.1109/TELFOR56187.2022.9983760>.





BIBLIOGRAFÍA

Al Tamimi, Yussef. «Human Rights and the Excess of Identity: A Legal and Theoretical Inquiry into the Notion of Identity in Strasbourg Case Law». *Social & Legal Studies* 27, n.o 3 (junio de 2018): 283- 98. <https://doi.org/10.1177/0964663917722598>.

Allen, Christopher. «The Path to Self-Sovereign Identity». Blog. *Life With Alacrity* (blog), 25 de abril de 2016. <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>.

Allende López, Marcos. *Identidad digital auto-gestionada: El futuro de la identidad digital: Autogestión, billeteras digitales y blockchain*. Inter-American Development Bank, 2020. <https://doi.org/10.18235/0002635>.

Antonopoulos, Andreas M. *Mastering Bitcoin: programming the open blockchain*. Second edition. Sebastopol, CA: O'Reilly, 2017.

———. *The Internet of Money: A collection of talks by Andreas M. Antonopoulos: Volume 1*. Vereinigte Staaten von America, 2016.

Baran, Paul. «I. Introduction to distributed communications networks». Memorandum. On Distributed Communications. Santa Monica, California: The RAND Corporation, agosto de 1964. https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf.

Barj, Sara, Aafaf Ouaddah, y Abdellatif Mezrioui. «A Review of Privacy-Preserving Cryptographic Techniques Used in Blockchain Platforms». En *Digital Technologies and Applications*, editado por Saad Motahhir y Badre Bossoufi, 230-40. *Lecture Notes in Networks and Systems*. Cham: Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-29857-8_23.

Belén Martínez, Lisana, María Belén Guercio, Sofía Orazi, Hernán Pedro Vígier, Lisana Belén Martínez, María Belén Guercio, Sofía Orazi, y Hernán Pedro Vígier. «Instrumentos financieros clave para la inclusión financiera en América Latina». *Revista Finanzas y Política Económica* 14, n.o 1 (junio de 2022): 17-47. <https://doi.org/10.14718/revfinanzpolitecon.v14.n1.2022.2>.

Bieker, Felix. *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law*. Vol. 34. *Information Technology and Law Series*. The Hague: T.M.C. Asser Press, 2022. <https://doi.org/10.1007/978-94-6265-503-4>.

Brito, Jerry. «The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society». *CoinCenter*, 6 de febrero de 2019. <https://coincenter.org/files/2019-02/the-case-for-electronic-cash-coin-center.pdf>.



Čapko, Darko, Srđan Vukmirović, y Nemanja Nedić. «State of the Art of Zero-Knowledge Proofs in Blockchain». En 2022 30th Telecommunications Forum (TEL FOR), 1-4, 2022. <https://doi.org/10.1109/TEL-FOR56187.2022.9983760>.

Chomczyk, Andrés. «Regulación de blockchain e identidad digital en América Latina: El futuro de la identidad digital». 2020.a ed. Banco interamericano de Desarrollo, 18 de diciembre de 2020. <https://doi.org/10.18235/0002935>.

Chomczyk Penedo, Andrés. «Self-Sovereign Identity Systems and European Data Protection Regulations: An Analysis of Roles and Responsibilities», P-312:95-106. Lecture Notes in Informatics (LNI) - Proceedings. Denmark: Gesellschaft für Informatik, 2021.

Crumpler, William, Marti Flacks, y Amith Mandavilli. «The Human Rights Risks and Opportunities in Blockchain», 2021.

De Filippi, Primavera, Morshed Mannan, y Wessel Reijers. «Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance». Technology in Society 62 (1 de agosto de 2020): 101284. <https://doi.org/10.1016/j.techsoc.2020.101284>.

«Estudio Económico de América Latina y el Caribe 2022: dinámica y desafíos de la inversión para impulsar una recuperación sostenible e inclusiva», 2022.

Farjat, Marcelo José García. «Nuevas tecnologías, promesas y alienación tecnológica: una mirada crítica del fenómeno del voto electrónico como dispositivo técnico moderno». ArtefaCToS. Revista de estudios sobre la ciencia y la tecnología 10, n.o 2 (29 de noviembre de 2021): 71-99. <https://doi.org/10.14201/art20211027199>.

Finck, Michèle, European Parliament, y Directorate-General for Parliamentary Research Services. «Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?». European Parliamentary Research Service, julio de 2019. http://publications.europa.eu/publication/manifestation_identifier/PUB_QA0219516ENN.

Giannopoulou, Alexandra. «Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity». Digital Society 2, n.o 2 (11 de mayo de 2023): 18. <https://doi.org/10.1007/s44206-023-00049-z>.

González Fuster, Gloria. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer Science & Business, 2014.

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, No. C-131/12 (Tribunal de Justicia de la Unión Europea (Gran Sala) 13 de mayo de 2014).



Harbitz, Mia Elisabeth, Juan Carlos Benitez Molina, y Iván Arcos Axt. «Inventario de los registros civiles e identificación de América Latina y el Caribe». Banco interamericano de Desarrollo, septiembre de 2010.

Herian, Robert. *Regulating Blockchain: Critical Perspectives in Law and Technology*. Routledge, 2018.

Hjálmarsson, Friðrik Þ., Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, y Gísli Hjálmtýsson. «Blockchain-Based E-Voting System». En 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), 983-86, 2018. <https://doi.org/10.1109/CLOUD.2018.00151>.

Huang, Jun, Debiao He, Mohammad S. Obaidat, Pandi Vijayakumar, Min Luo, y Kim-Kwang Raymond Choo. «The Application of the Blockchain Technology in Voting Systems: A Review». *ACM Computing Surveys* 54, n.o 3 (17 de abril de 2021): 60:1-60:28. <https://doi.org/10.1145/3439725>.

«Implementación del prototipo Blockchain para procesos electorales en colegios públicos segunda edición». Alcaldía Mayor de Bogotá D.C., 23 de abril de 2019. <https://tic.bogota.gov.co/documentos/blockchain-elecciones-estudiantiles>.

«Informe de Economía Latinoamericana. Primer semestre de 2022», 2022.

«Informe Final de Resultados Prototipo Blockchain». Alcaldía Mayor de Bogotá D.C. - Universidad Nacional de Colombia - ViveLab Bogotá, 31 de julio de 2018. <https://tic.bogota.gov.co/documentos/informe-final-resultados-prototipo-blockchain>.

John, Kose, Maureen O'Hara, y Fahad Saleh. «Bitcoin and Beyond». *Annual Review of Financial Economics* 14, n.o 1 (1 de noviembre de 2022): 95-115. <https://doi.org/10.1146/annurev-financial-111620-011240>.

Judmayer, Aljosha, Nicholas Stifter, Katharina Krombholz, y Edgar Weippl. «Nakamoto Consensus». En *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms*, editado por Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz, y Edgar Weippl, 61-86. *Synthesis Lectures on Information Security, Privacy, and Trust*. Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-031-02352-1_6.

Keathley, Elizabeth Ferguson. *Digital Asset Management*. Berkeley, CA: Apress, 2014. <https://doi.org/10.1007/978-1-4302-6377-7>.

Kostakis, Vasilis, y Chris Giotitsas. «The (A)Political Economy of Bitcoin». *TripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 12, n.o 2 (2014): 431-40. <https://doi.org/10.31269/triplec.v12i2.606>.

Lauer, Josh. *Creditworthy: A History of Consumer Surveillance and Financial Identity in America*. New York: Columbia University Press, 2017.



Liu, Xing, Bahar Farahani, y Farshad Firouzi. «Distributed Ledger Technology». En *Intelligent Internet of Things: From Device to Fog and Cloud*, editado por Farshad Firouzi, Krishnendu Chakrabarty, y Sani Nassif, 393-431. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-30367-9_8.

Madrid, Miguel González. «El voto electrónico en el mundo. Breve historia de experiencias acerca de un ascenso desigual». *Revista Mexicana de Estudios Electorales* 5, n.o 25 (25 de enero de 2021): 173-236.

Maurer, Bill. *How Would You Like to Pay? How Technology Is Changing the Future of Money*. Duke University Press, 2015.

Mayorga Jácome, Tannia C., Miguel García Jiménez, José F. Duret Gutiérrez, Joe Carrión Jumbo, y Pamela Valeria Yarad Jeada. «Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos». *Dominio de las Ciencias* 5, n.o 1 (2019): 518-37.

Maza, Marina Vega. «El auge de blockchain y sus posibilidades reales de aplicación en los registros de las administraciones públicas». *IDP. Revista de Internet, Derecho y Política*, n.o 28 (17 de febrero de 2019). <https://doi.org/10.7238/idp.v0i28.3154>.

Merkle, Ralph C. «A Digital Signature Based on a Conventional Encryption Function». En *Advances in Cryptology – CRYPTO '87*, editado por Carl Pomerance, 369-78. *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer, 1988. https://doi.org/10.1007/3-540-48184-2_32.

Miller, Todd, Víctor Endo, Gonzalo Muñoz, y Francisco Oliveira. «Tecnología blockchain: una forma de aumentar la confianza, mejorar la eficiencia y reducir los costos en los procesos de registro de propiedades». *Nota Técnica. Banco Interamericano de Desarrollo*, 18 de julio de 2022. <https://publications.iadb.org/es/tecnologia-blockchain-una-forma-de-aumentar-la-confianza-mejorar-la-eficiencia-y-reducir-los-costos>.

Moerel, Lokke. «Blockchain & Data Protection...and Why They Are Not on a Collision Course». *European Review of Private Law* 6 (2019): 825-52.

Nakamoto, Satoshi. «Bitcoin: A Peer-to-Peer Electronic Cash System», 31 de octubre de 2008. <https://bitcoin.org/bitcoin.pdf>.

Nasir, Muhammad Hassan, Junaid Arshad, Muhammad Mubashir Khan, Mahawish Fatima, Khaled Salah, y Raja Jayaraman. «Scalable Blockchains – A Systematic Review». *Future Generation Computer Systems* 126 (1 de enero de 2022): 136-62. <https://doi.org/10.1016/j.future.2021.07.035>.

Natarajan, Harish, Solvej Krause, y Helen Gradstein. «Distributed Ledger Technology and Blockchain». *Fintech Note. World Bank Group*, 2017. <http://hdl.handle.net/10986/29053>.



«OECD Blockchain Primer». OECD. Accedido 28 de junio de 2023. <https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf>.

Park, Sunoo, Michael Specter, Neha Narula, y Ronald L Rivest. «Going from Bad to Worse: From Internet Voting to Blockchain Voting». *Journal of Cybersecurity* 7, n.o 1 (16 de febrero de 2021): tyaa025. <https://doi.org/10.1093/cybsec/tyaa025>.

Peiró, Nicolás Nogueroles, y Eduardo J. Martínez García. «Blockchain and Land Registration Systems». *European Property Law Journal* 6, n.o 3 (20 de diciembre de 2017): 296-320. <https://doi.org/10.1515/eplj-2017-0017>.

Pérez Solà, Cristina, y Jordi Herrera Joancomartí. «Bitcoins y el problema de los generales bizantinos», 241-46. Alicante: Universidad de Alicante, 2014. <http://rua.ua.es/dspace/handle/10045/40444>.

Pineda Salazar, Ramón, y N. Alejandra Acevedo. «Financiamiento mediante emisión monetaria en América Latina, 1960-2016», 29 de julio de 2021. <https://repositorio.cepal.org/handle/11362/47137>.

Pöhn, Daniela, Michael Grabatin, y Wolfgang Hommel. «EID and Self-Sovereign Identity Usage: An Overview». *Electronics* 10, n.o 22 (enero de 2021): 2811. <https://doi.org/10.3390/electronics10222811>.

«Proyecto DIDI: Aprendizajes, resultados y desafíos de la identidad digital auto-gestionada para la inclusión». Banco Interamericano de Desarrollo, 10 de abril de 2023. <https://didi.org.ar/2023/04/10/proyecto-didi-aprendizajes-resultados-y-desafios-de-la-identidad-digital-auto-gestionada-para-la-inclusion/>.

Puthal, Deepak, Nisha Malik, Saraju P. Mohanty, Elias Kougianos, y Gautam Das. «Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems». *IEEE Consumer Electronics Magazine* 7, n.o 4 (julio de 2018): 6-14. <https://doi.org/10.1109/MCE.2018.2816299>.

Quintais, J. P., B. Bodó, A. Giannopoulou, y V. Ferrari. «Blockchain and the Law: A Critical Evaluation». *Stanford Journal of Blockchain Law & Policy* 2 (2019). <https://dare.uva.nl/search?identifier=38a8394a-ed48-46d5-b71c-9d42357074e7>.

Sherman, Alan T., Farid Javani, Haibin Zhang, y Enis Golaszewski. «On the Origins and Variations of Blockchain Technologies». *IEEE Security & Privacy* 17, n.o 1 (enero de 2019): 72-77. <https://doi.org/10.1109/MSEC.2019.2893730>.

Singh, Arshdeep, Gulshan Kumar, Rahul Saha, Mauro Conti, Mamoun Alazab, y Reji Thomas. «A Survey and Taxonomy of Consensus Protocols for Blockchains». *Journal of Systems Architecture* 127 (1 de junio de 2022): 102503. <https://doi.org/10.1016/j.sysarc.2022.102503>.



Szabo, Nick. «Smart Contracts». Nick Szabo's Essays, Papers, and Concise Tutorials (blog), 1994. <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>.

Tabatabaei, Mohammad Hossein, Roman Vitenberg, y Narasimha Raghavan Veeraragavan. «Understanding Blockchain: Definitions, Architecture, Design, and System Comparison». arXiv, 27 de noviembre de 2022. <http://arxiv.org/abs/2207.02264>.

Tapscott, Don, y Alex Tapscott. La revolución blockchain: Descubre cómo esta nueva tecnología transformará la economía global. Traducido por Juan Manuel Salmerón Arjona, 2017.

Upadhyay, Nitin. «Demystifying Blockchain: A Critical Analysis of Challenges, Applications and Opportunities». International Journal of Information Management 54 (1 de octubre de 2020): 102120. <https://doi.org/10.1016/j.ijinfomgt.2020.102120>.

Vacca, Anna, Andrea Di Sorbo, Corrado A. Visaggio, y Gerardo Canfora. «A Systematic Literature Review of Blockchain and Smart Contract Development: Techniques, Tools, and Open Challenges». Journal of Systems and Software 174 (1 de abril de 2021): 110891. <https://doi.org/10.1016/j.jss.2020.110891>.

Vargas, Luis, Jean Bacon, y Ken Moody. «Event-Driven Database Information Sharing». En Sharing Data, Information and Knowledge, editado por Alex Gray, Keith Jeffery, y Jianhua Shao, 5071:113-25. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008. https://doi.org/10.1007/978-3-540-70504-8_11.

Verheye, Benjamin. «Land Registration in the Twenty-First Century: Blockchain Land Registers from a Civil Law Perspective». En Disruptive Technology, Legal Innovation, and the Future of Real Estate, editado por Amnon Lehavi y Ronit Levine-Schnur, 123-35. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-52387-9_7.

Wangenheim, Georg von. «Blockchain-Based Land Registers: A Law-and-Economics Perspective». En Disruptive Technology, Legal Innovation, and the Future of Real Estate, editado por Amnon Lehavi y Ronit Levine-Schnur, 103-22. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-52387-9_6.

Yaga, Dylan, Peter Mell, Nik Roby, y Karen Scarfone. «Blockchain Technology Overview». Gaithersburg, MD: National Institute of Standards and Technology, octubre de 2018. <https://doi.org/10.6028/NIST.IR.8202>.

Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Profile Books, 2019.



ANEXO 3

INTERFACES ORDENADOR-CEREBRO: ¿ES NECESARIA LA PROTECCIÓN DE LOS “NEURODERECHOS” PARA RESPETAR LOS DERECHOS HUMANOS?



Verónica Hinestroza Arenas

Este artículo busca abonar al debate en torno a la necesidad o no de abordar, a nivel de marcos normativos internacionales existentes, el aún incipiente concepto de “neuro-derechos”, como requisito para garantizar el respeto a los derechos humanos en el desarrollo y utilización de neurotecnologías, así como de la información derivada de las mismas.

La neurociencia, establecida como una rama interdisciplinaria del conocimiento en la segunda mitad del siglo XX, se dedica al estudio del sistema nervioso¹⁷¹, el encargado de generar, modular y transmitir información entre las diferentes partes del cuerpo humano. El término neurotecnología se utiliza para describir procedimientos o dispositivos electrónicos tendientes a recabar información de la actividad neuronal para entender la actividad cerebral. Los dispositivos incluyen desde “tecnologías ponibles”, e interfaces cerebro-ordenador no invasivas como los miembros robóticos, hasta los implantes cerebrales que buscarán tratar discapacidades como la parálisis¹⁷². Mediante diversos métodos, tanto invasivos como no invasivos, la neurotecnología permite intervenir en el funcionamiento del sistema nervioso central (encéfalo y médula espinal) y periférico (nervios craneales y raquídeos)¹⁷³. Dichas intervenciones pueden estar dirigidas a estimular, alterar, reemplazar o reestablecer funciones sensoriales, motrices o cognitivas¹⁷⁴.

La neurotecnología con fines terapéuticos ha contribuido positivamente, por ejemplo, a la prevención, diagnóstico y tratamiento de afectaciones neurológicas¹⁷⁵. No obstante, su avance no

¹⁷¹ Herrera, Camarillo, L., “¿Qué es la neurociencia y cuál es su importancia?”, Universidad Iberoamericana, Ciudad de México, 27 de marzo de 2023. Disponible en: < <https://ibero.mx/prensa/que-es-la-neurociencia-y-cual-es-su-importancia>>.

¹⁷² Naciones Unidas, “Es urgente establecer un marco ético sobre neurotecnología a escala internacional”, en Noticias ONU, 6 de junio de 2023. Disponible en: < <https://news.un.org/es/story/2023/06/1521747>>.

¹⁷³ Eunice Kennedy Shriver National Institute of Child Health and Human Development, “Cuáles son las Partes del Sistema Nervioso?”. Disponible en < <https://espanol.nichd.nih.gov/salud/temas/neuro/informacion/partes>>

¹⁷⁴ Ver: IEEE Brain, “Neurotechnology: The Next Technology Frontier”. Disponible en: <<https://brain.ieee.org/topics/neurotechnologies-the-next-technology-frontier/>> -:~:text=“Neurotechnology” refers to any technology,mental illness or sleep patterns.>, y Costas Trascasas, M., “Evaluación de las implicaciones de la neurotecnología para los derechos humanos: hacia el reconocimiento de los neuroderechos” en Informe del Comité Asesor sobre su 28o período de sesiones ante el Consejo de Derechos Humanos de las Naciones Unidas, A/HRC/AC/28/2, 7 de septiembre de 2022

¹⁷⁵ Organisation for Economic Co-operation and Development, “Recommendation on Responsible Innovation in Neurotechnology”, OECD/LEGAL/0457, 11 de septiembre de 2019. Disponible en:< <https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm>>



se ha limitado a la salud pública, la neurotecnología también sigue evolucionando para entender el funcionamiento y desarrollo neurocognitivo de animales¹⁷⁶, como para responder a intereses privados tendientes a alterar la naturaleza humana, mediante, por ejemplo, el aumento y/o mejor funcionamiento cognitivo, incluyendo la memoria¹⁷⁷, la manipulación del cerebro de otras personas y/o la obtención de información sobre su identidad y emociones¹⁷⁸. Frente al último punto, vale la pena destacar que la obtención de información neurológica va de la mano con el avance tecnológico, de hecho una parte significativa de los datos neuronales es inconsciente, y por ende la neurotecnología puede recabar información que las personas no necesariamente revelarían de manera intencional¹⁷⁹.

A pesar, o como consecuencia, de incipientes, parciales y en ocasiones inapropiados marcos regulatorios, incluyendo en materia de patentes¹⁸⁰, diversas iniciativas estatales, de carácter académico y privado están invirtiendo capital financiero en investigación sobre neurotecnología¹⁸¹, 50% de las empresas privadas se encuentran en Estados Unidos, y el 35% están en Europa y en el Reino Unido¹⁸². De acuerdo con la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) desde 2013, “las inversiones públicas en este campo han superado los 6.000 millones de dólares y la financiación privada anual se ha multiplicado por 22 entre 2010 y 2020, alcanzando los 7.300 millones de dólares y un total de 33.200 millones”¹⁸³.

En 2019, la Organización para la Cooperación Económica y el Desarrollo, instancia de carácter global que trabaja para elaborar políticas que fomenten la prosperidad, la igualdad, las oportunidades y el bienestar, reconoció que las vías rápidas y a veces inciertas que navega la neurotecnología, al igual que otras tecnologías emergentes, pueden requerir formas ágiles de gobernanza. Este reconocimiento se enmarca en su “Recomendación sobre Innovación Responsable en la Neurotecnología”, instrumento que se constituyó en la primera guía en abarcar cada paso del proceso de innovación: investigación, transferencia de tecnología, inversión, comercialización y regulación. Sus nueve principios cubren: 1. Innovación responsable para abordar desafíos en materia de salud; 2. Priorización de estudios de seguridad; 3. Promoción inclusiva para el área de salud; 4. Incentivo a la colaboración científica entre países, sectores y disciplinas; 5. Deliberación social; 6. Facilitación del monitoreo y la asesoría para enfrentar nuevos desafíos; 7. Salvaguarda de la información; 8. Promoción de una cultura de confianza en los sistemas público y privado; y 9. Detección temprana y monitoreo del potencial no intencionado del uso o abuso de la neurotecnología¹⁸⁴.

¹⁷⁶ Frasnelli, E. Evolution and function of neurocognitive systems in non-human animals. Sci Rep 11, 23487 (2021). <https://doi.org/10.1038/s41598-021-02736-8>

¹⁷⁷ Costas Trascasas, M., “Evaluación de las implicaciones de la neurotecnología para los derechos humanos: hacia el reconocimiento de los neuroderechos”, en Informe del Comité Asesor sobre su 28o período de sesiones ante el Consejo de Derechos Humanos de las Naciones Unidas, A/HRC/AC/28/2, 7 de septiembre de 2022, párrafo 4

¹⁷⁸ Naciones Unidas, “Es urgente establecer un marco ético sobre neurotecnología a escala internacional”, en Noticias ONU, 6 de junio de 2023. Disponible en: <<https://news.un.org/es/story/2023/06/1521747>>.

¹⁷⁹ Ibid, página 28

¹⁸⁰ UNESCO, “Unveiling the neurotechnology landscape: scientific advancements, innovations and major trends”, 2023. Disponible en: <https://unesdoc.unesco.org/ark:/48223/pf0000386137>, página 81.

¹⁸¹ OpCit, Costas Trascasas, M., pie de página 9

¹⁸² OpCit, Naciones Unidas, junio de 2023

¹⁸³ OpCit, UNESCO, 2023

¹⁸⁴ OECD/LEGAL/0457, 11 de septiembre de 2019. Disponible en: <<https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm>>



Por su parte, El Comité Asesor del Consejo de Derechos Humanos de las Naciones Unidas, al igual que el Consejo de Europa¹⁸⁵, avanza en una evaluación de las implicaciones de la neurotecnología para los derechos humanos. En su informe de septiembre de 2022, sobre el 28 periodo de sesiones, el Comité destacó la posibilidad de que la neurotecnología llegue a reforzar dinámicas totalitarias o procesos autoritarios mediante, por ejemplo, la vigilancia intrusiva, la evaluación no consentida o la manipulación de los estados cerebrales o del comportamiento, así como a profundizar la brecha social entre grupos privilegiados que puedan acceder a la tecnología y quienes no tengan acceso a ella¹⁸⁶. Sin duda, el privilegio podría exacerbar la existente inequidad en oportunidades académicas, profesionales y de acceso al nivel más alto de salud posible; derivando incluso en un retroceso en los limitados avances globales en materia de justicia social. En la misma línea, pero considerando un escenario en que la gran mayoría de personas tengan acceso a la neurotecnología, existe el potencial de generar, nuevas asimetrías de poder, elevando a quienes naturalmente cuentan con un nivel cognitivo alto y segregando a quienes evidencien uno menor. En la actualidad “sólo seis países han presentado casi el 90% de las patentes de neurotecnología registradas en las principales oficinas de propiedad intelectual del mundo”¹⁸⁷.

La UNESCO, cuyo mandato incluye propiciar la reflexión y el debate sobre la ética de la ciencia y la tecnología¹⁸⁸, ha llamado desde 2021 a identificar los desafíos de la neurotecnología. El rápido avance del desarrollo de la neurotecnología genera múltiples preocupaciones en ético-legales, por ejemplo, la incertidumbre sobre la posibilidad de ofrecer toda la información necesaria para obtener un consentimiento plenamente informado, libre y revocable¹⁸⁹ de quienes se sometan a la tecnología, incluyendo el uso que se le dará a la información, la confidencialidad con que se tratará y la garantía de integridad de los datos recogidos. Previamente, la organización internacional ha impulsado procesos como la Declaración Universal sobre el Genoma Humano y los Derechos Humanos¹⁹⁰, y la Recomendación sobre la Ética de la Inteligencia Artificial¹⁹¹. En julio de 2023, en el marco de una conferencia internacional sobre ética y neurotecnología, la UNESCO obtuvo consenso entre académicos, políticos, y partes interesadas del sector, para establecer un instrumento normativo y un marco ético global para su regulación¹⁹².

El informe presentado en la conferencia destaca la capacidad tanto positiva como negativa, de la neurotecnología para impactar en el bienestar individual y social de la humanidad. El mismo

¹⁸⁵ Consejo de Europa, “Neurotechnologies and Human Rights Framework: Do We Need New Rights?”. Disponible en: < [https://www.coe.int/en/web/bioethics/round-table-on-the-human-rights-issues-raised-by-the-applications-of-neurotechnologies#\(%22106485310%22:\[1\]\)>](https://www.coe.int/en/web/bioethics/round-table-on-the-human-rights-issues-raised-by-the-applications-of-neurotechnologies#(%22106485310%22:[1])>)

¹⁸⁶ Ibid, pie de página 13

¹⁸⁷ OpCit., UNESCO, julio de 2023

¹⁸⁸ Ver: UNESCO, “Ética de la Neurología”. Disponible en: < https://www.unesco.org/es/ethics-neurotech?TSPD_101_R0=080713870fab200019afaf220fdab3784ab14191e287e79c8b5b0381a519630f084625f7716f35700805459b991430007ec39a4ceacb13ab79c621ecc-8295d418bbfe625a48adeddc208c0c4a33cfc409e832e2464810ff3c3738c888b38ffd7>

¹⁸⁹ Ver: UNESCO, “Declaración Universal sobre Bioética y Derechos Humanos”, 19 de octubre de 2005. Disponible en: < https://unesdoc.unesco.org/ark:/48223/pf0000146180_sp&

¹⁹⁰ Naciones Unidas, “Declaración Universal sobre el Genoma Humano y los Derechos Humanos. Disponible en: <https://www.ohchr.org/es/instruments-mechanisms/instruments/universal-declaration-human-genome-and-human-rights>

¹⁹¹ UNESCO, “Recomendación sobre la Ética de la Inteligencia Artificial”, 2021. Disponible en: < https://unesdoc.unesco.org/ark:/48223/pf0000380455_sp&

¹⁹² UNESCO, “Ethics of Neurotechnology: UNESCO, leaders and top experts call for solid governance”, julio de 2023. Disponible en: < <https://www.unesco.org/en/articles/ethics-neurotechnology-unesco-leaders-and-top-experts-call-solid-governance>>



revela que el crecimiento del sector de la neurotecnología, desigual por el dominio de pocos países, significa un cambio en la trayectoria tradicional de la tecnología. La tendencia previa fue el avance principalmente en la biotecnología y la farmacéutica, y hoy se privilegian la informática y la medicina. El informe llama a las autoridades a seguir estos avances y en especial su interacción con la Inteligencia Artificial.

Este documento de la UNESCO menciona además un debate que caracteriza como emergente: el debate en torno a los neuroderechos. El informe recoge que en los últimos años algunos científicos y especialistas en neuroética han formulado el concepto de “neuroderechos” para abordar los desafíos éticos y jurídicos asociados al desarrollo de la neurotecnología. Su propuesta llama a trabajar un nuevo marco jurídico internacional y de derechos humanos¹⁹³, desde posiciones que el neurólogo Philipp Kellmeyer clasifica en la innovación y el reformismo legal respectivamente¹⁹⁴: 1. El desarrollo de los neuroderechos humanos; y 2. La inclusión de los neuroderechos en instrumentos internacionales existentes, en particular en la Declaración Universal de los Derechos Humanos.

El argumento que sostiene el primer elemento de la propuesta, es decir la definición de un marco normativo neuroespecífico¹⁹⁵ denominado “neuroderechos humanos” es proteger de manera diferenciada la actividad y los datos del cerebro, ante avances tecnológicos que tienen el potencial de impactar la existencia humana. La propuesta de inclusión de esta normativa en la Declaración Universal se basa en la idea de que la misma es insuficiente para hacer frente a los desafíos de la neurotecnología, y requiere ser actualizada¹⁹⁶.

Iniciativas para crear y/o revisar marcos normativos para responder a nuevos desafíos no son ajenas al derecho internacional de los derechos humanos, por el contrario, son un lugar común para quienes no están familiarizados con el contenido y alcance evolutivo de la interpretación de cada derecho contenido en su pilar, la Declaración Universal de los Derechos Humanos. Limitarse al vocabulario utilizado en la redacción del enunciado de los derechos ignora el andamiaje normativo que de deriva de estos, y facilita asumir que al no contar con el vocabulario propio del nuevo dilema de que se trate o no especificar el riesgo que busca limitarse, el derecho internacional es obsoleto. Por el contrario, el derecho internacional de los derechos humanos ha demostrado, tanto al nivel de las Naciones Unidas como de sistemas regionales, ser un instrumento vivo que se adapta a las circunstancias modernas mediante las diferentes herramientas con que cuenta, incluyendo informes, recomendaciones, observaciones generales, protocolos de actuación y jurisprudencia.

¹⁹³ OpCit, UNESCO, 2023

¹⁹⁴ Kellmeyer, P., “A Human Rights–Based Approach for Governing Neurotechnologies” from Part VII - Responsible AI Healthcare and Neurotechnology Governance, en The Cambridge Handbook of Responsible Artificial Intelligence Interdisciplinary Perspectives, Cambridge University Press, 2022

¹⁹⁵ Ver: Ienca, M., “Neuroderechos: Por qué debemos actuar antes de que sea demasiado tarde?”, en Anuario Internacional CIDOB 2021. Disponible en: < https://www.cidob.org/articulos/anuario_internacional_cidob/2021/neuroderechos_por_que_debemos_actuar_antes_de_que_sea_demasiado_tarde>

¹⁹⁶ “Es necesario poner al día la Declaración Universal de Derechos Humanos debido al acceso a la información cerebral”, incide Yuste.” Garvi, Carvajal, A., “Neuroderechos, una garantía para evitar ‘hackear’ el cerebro”, 14 de marzo de 2022, en Cinco Días 45. Disponible en: https://cincodias.elpais.com/cincodias/2022/03/11/legal/1646988690_719731.html.



Vale la pena destacar en este punto que desde 1948, la Declaración ha inspirado más de 80 declaraciones y tratados internacionales, un gran número de convenciones regionales, proyectos de ley nacionales de derechos humanos y disposiciones constitucionales¹⁹⁷, y que si bien la Declaración Universal en un inicio no representaba un conjunto de normas vinculantes, tras más de 60 años de implementación, varios de los derechos que consigna se han constituido en derecho consuetudinario¹⁹⁸.

En su trayectoria evolutiva, lejos de buscar contraponerse a la ciencia, el derecho internacional de los derechos humanos ha establecido diálogos propositivos con diversas áreas de la misma, facilitando el abordaje multidisciplinario de las autoridades de los sistemas de justicia a nivel doméstico, de la promoción de los derechos humanos y la sanción de graves violaciones. Ejemplos de estos diálogos son el Protocolo de Minnesota para la Investigación de Muertes Potencialmente Ilícitas¹⁹⁹ y mutatis mutandis de casos de desaparición forzada, en el que interactúan el derecho internacional de los derechos humanos, la ética y las ciencias forenses, y el Protocolo de Estambul para la Investigación y Documentación Eficaces de la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes²⁰⁰, en el que los derechos humanos y la ética se complementan con la medicina y la psicología. En esta misma línea se cuenta el Protocolo de Berkeley para la Investigación de Código Abierto de Archivos Digitales²⁰¹ que integra el derecho internacional de los derechos humanos, la ética y la tecnología para orientar el uso de información digital pública como prueba ante instancias judiciales. Finalmente, los Principios Méndez sobre Entrevistas Efectivas para Investigación y Recopilación de Información²⁰², establecen un diálogo entre los derechos humanos, la ética y la ciencia, incluyendo la neurociencia y medicina, para orientar el desarrollo de entrevistas no coercitivas, fortaleciendo la implementación de la prohibición absoluta de la tortura y la garantías del debido proceso.

La idea de los neuroderechos como especialidad legal²⁰³ comenzó a desarrollarse en la década de los 90's, y solo hasta 2017, en un artículo escrito por Marcello Lenca y Roberto Andorro, se abordó la idea de los neuroderechos humanos. El artículo propuso entonces el desarrollo de cuatro neuroderechos: 1. Libertad cognitiva, que abarca la toma de decisiones libres y competentes frente a

¹⁹⁷ Ver :Naciones Unidas " Declaración Universal de los Derechos Humanos". Disponible en: < <https://www.un.org/es/about-us/udhr/foundation-of-international-human-rights-law> >

¹⁹⁸ Tomuschat, C., "United Nations General Assembly", 2002, en Max Planck Encyclopedia of Public International Law, párrafo 22

¹⁹⁹ Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "Protocolo de Minnesota para la Investigación de Muertes Potencialmente Ilícitas", Nueva York y Ginebra, 1991, 2017. Disponible en: < https://www.ohchr.org/sites/default/files/Documents/Publications/MinnesotaProtocol_SP.pdf >

²⁰⁰ Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, " Protocolo de Estambul; Manual para la Investigación y Documentación Eficaces de la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes", Nueva York, 2001, 2004, 2022. Disponible en: < https://www.ohchr.org/sites/default/files/documents/publications/2022-06-29/Istanbul-Protocol_Rev2_EN.pdf >

²⁰¹ Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos y The Human Rights Center at the University of California, Berkeley, School of Law, "Protocolo de Berkeley para la Investigación de Código Abierto de Archivos Digitales", Nueva York, 2022. Disponible en: < https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf >

²⁰² Iniciativa contra la Tortura, la Asociación para la Prevención de la Tortura y el Centro Noruego de Derechos Humanos, "Principios sobre Entrevistas Efectivas para Investigación y Recopilación de Información", 2021. Disponible en: < https://www.apt.ch/sites/default/files/publications/apt_PoEI_SPA_04.pdf >

²⁰³ Para antecedentes sobre el desarrollo del concepto neuroderecho, ver: Borbón Rodríguez, D. A., Borbón Rodríguez, L. F., & León Bustamante, M. A., "Neuroderecho al acceso equitativo a tecnologías de mejora: Análisis desde el posthumanismo, el derecho y la bioética", 2021, en Revista Iberoamericana De Bioética, (16), 01–15. Disponible en: <<https://doi.org/10.14422/rib.i16.y2021.006> >



la neurotecnología y la prohibición de su uso coercitivo y no consentido; **2.** Privacidad mental que aborda la protección frente a la intrusión y uso no consentido en los datos cerebrales; **3.** Integridad mental, dirigido a salvaguardar la salud mental de quienes hacen posible la neurotecnología; y **4.** Continuidad psicológica que pretende preservar la identidad de las personas y la continuidad de su vida mental.²⁰⁴

Años más tarde, en 2021, lenca trabajó el informe del Consejo de Europa, comisionado por el Comité de Bioética, sobre los retos para los derechos humanos que plantean las distintas aplicaciones de las neurotecnologías en el ámbito biomédico. En este informe el autor reitera sus planteamientos de 2017, argumentando que si bien algunos de los derechos y libertades contenidos en la Declaración Universal se refieren implícitamente a la protección del cerebro y la esfera mental, su alcance es insuficiente por no detallar explícitamente los escenarios de riesgo específicos de la neurotecnología ni, en su concepto, proporcionan un marco articulado directamente para proteger el cerebro y la mente humanos. En el mismo texto, lenca elabora una vez más sobre los cuatro neuroderechos incluidos en su artículo original²⁰⁵.

En 2017, mismo año en que lenca publicó su artículo original, el neurobiólogo Rafael Yuste y otros autores²⁰⁶, recomendaron, desde la ética, añadir cláusulas de protección a los neuroderechos en los tratados internacionales, como la Declaración Universal de los Derechos Humanos de 1948, no obstante sostuvieron que esto podría ser insuficiente, ya que en su concepto las declaraciones y leyes internacionales no son más que acuerdos entre Estados, e incluso la Declaración Universal no es jurídicamente vinculante²⁰⁷.

En 2019, bajo la “NeuroRights Initiative” en la Universidad de Columbia, Yuste pasó a promover el desarrollo de cinco neuroderechos: **1.** Identidad personal, que busca establecer límites para impedir que la tecnología altere el sentido del yo; **2.** Libre albedrío, que pretende que los individuos tengan el control último sobre su propia toma de decisiones, sin manipulaciones desconocidas de neurotecnologías externas; **3.** Privacidad mental que aboga por que cualquier dato obtenido de la medición de la actividad neuronal se mantenga en privado, y a la vez porque la venta, la transferencia comercial y el uso de los datos neuronales sea estrictamente regulada; **4.** Acceso equitativo a las tecnologías de mejora, que implica el establecimiento de directrices, tanto a nivel internacional como nacional, que regulen el desarrollo y las aplicaciones de las neurotecnologías de mejora mental; directrices basadas en el principio de justicia y garantizar la igualdad de acceso a todos los ciudadanos; y **5.** Protección contra sesgos en los algoritmos mediante la adopción de medidas²⁰⁸.

²⁰⁴ lenca, M., Andorno, R., “Towards new human rights in the age of neuroscience and neurotechnology.” En Life Sci Soc Policy 13, 5, 2017. Disponible en: < <https://doi.org/10.1186/s40504-017-0050-3> >

²⁰⁵ lenca, M., “Common human rights challenges raised by different applications of neurotechnologies in the biomedical fields” Consejo de Europa, 2021. Disponible en: < <https://rm.coe.int/report-final-en/1680a429f3> >.

²⁰⁶ Yuste, R., Goering, S., Arcas, B. et al., “Four ethical priorities for neurotechnologies and AI” en Nature 551, 159–163, 2017. Disponible en: <<https://doi.org/10.1038/551159a>>

²⁰⁷ Ibid

²⁰⁸ Neurorights Initiative, “The five neurorights”. Disponible en: https://neurorights-initiative.site.drupaldisttest.cc.columbia.edu/sites/default/files/content/The%20Five%20Ethical%20NeuroRights%20Updated%20pdf_0.pdf



El contenido de las dos propuestas de neuroderechos evidencian que no hay consenso en el comprensión de conceptos clave, y que la profundidad de su abordaje, incluyendo por su desconexión con la normativa internacional, es insuficiente. En materia de privacidad mental e integridad mental, Kellmeyer destaca la ausencia de transdisciplinariedad para traducir las exigencias éticas que se enmarcan como neuroderechos en marcos de acción para una gobernanza responsable y eficaz de las neurotecnologías²⁰⁹. El autor llama además la atención sobre que tanto en filosofía moral como en filosofía jurídica se ha demostrado que los bienes morales y jurídicos, especialmente si no son conceptualmente dependientes entre sí terminan co-existiendo en conflicto²¹⁰.

En materia de integridad mental, como destaca la UNESCO, el concepto abarca el reconocimiento de la dignidad humana, incluida la integridad del cuerpo y el respeto del principio de igualdad. La Declaración Universal de los Derechos Humanos establece que los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia²¹¹. Tanto la Declaración como el Pacto de Derechos Civiles y Políticos y el Pacto de Derechos Económicos y Culturales, que con esta conforman la Carta Internacional de Derechos Humanos, destacan las obligaciones del Estado frente a la garantía positiva y de derechos humanos íntimamente ligados preocupaciones derivadas de la neurotecnología, incluyendo el derecho al nivel más alto de salud posible, a la identidad personal, la libertad de pensamiento, la libertad de conciencia, la libertad de religión, la libertad de opinión y expresión, la privacidad incluyendo la protección de la ley injerencias o ataques, la igualdad ante la ley, la no discriminación, y el derecho a participar del progreso científico y de los beneficios que de él resulten.

Más aún la normativa internacional, ofrece protección frente a derechos que aún no se han abordado suficientemente en el marco de las preocupaciones en torno al uso de la neurotecnología, como son el derecho a la presunción de inocencia y en su conjunto el derecho a un juicio justo con la garantía de todas las salvaguardas que este implica. Amenazas a estos derechos, íntimamente ligados a la justicia penal a nivel doméstico, ya comienzan a abordarse en marcos regulatorios relativos a la inteligencia artificial, sin que al hacerlo se pretenda reformar los tratados internacionales. En este sentido, el 16 de junio de 2023, el Parlamento Europeo aprobó una ley que prohíbe el uso de sistemas de predicción policial y criminal utilizados por las autoridades policiales y judiciales de la Unión Europea con el fin de evaluar el riesgo de zonas o de personas física de delinquir o reincidir. La ley prohíbe además la identificación biométrica a distancia, como son los sistemas de reconocimiento facial en espacios de acceso público, así como los sistemas de reconocimiento de emociones y el rastreo masivo de bases de datos biométricas²¹².

Adicional a las obligaciones positivas de los Estados, los instrumentos de derechos mencionados, así como posteriores tratados vinculantes, abordan obligaciones negativas de los Estados también relevantes frente al avance de la neurociencia, como son la detención arbitraria y la pro-

²⁰⁹ OpCit, Kellmeyer, P., página 422

²¹⁰ Ibid, página 421

²¹¹ OpCit, UNESCO, 2023

²¹² Ver: Fair Trials, "El Parlamento Europeo aprueba una ley histórica sobre Inteligencia Artificial". Disponible en: < <https://www.fairtrials.org/articulos/news/el-parlamento-europeo-aprueba-una-ley-historica-sobre-inteligencia-artificial/> >



hibición absoluta de someter a alguien a tortura o a otros tratos o penas crueles, inhumanas o degradantes, es decir que nadie será sometido intencionalmente a dolores o sufrimientos graves, ya sean físicos o mentales con fines que incluyen la obtención de información o una confesión²¹³. Es más, el texto del Pacto de Derechos Civiles y políticos incluye explícitamente en la prohibición de la tortura, que nadie será sometido sin su libre consentimiento a experimentos médicos o científicos²¹⁴. Las obligaciones negativas de los Estados entrañan las obligaciones positivas de proteger, prevenir, investigar, procesar y castigar.

Reconocer el contenido, desarrollo y alcance del derecho internacional de los derechos humanos para continuar abordando problemáticas emergentes, no implica sin embargo caer en una lógica conservadora, que como plantea Kellmeyer implique una postura estática que asuma que se cuenta con suficiente cobertura para proteger los bienes antropológicos de la intimidad mental y la integridad mental²¹⁵. Como concluye el más reciente informe de la UNESCO, se puede y se debe avanzar en identificar vacíos para el establecimiento de marcos regulatorios éticos que amplíen y refuercen el alcance de las responsabilidades internacionales de los estados en materia de derechos humanos²¹⁶. Una postura que encuentra coincidencia en el planteamiento del mismo Kellmeyer, quién sin limitarse a la ética y reconociendo que el derecho internacional de los derechos humanos y las normas domésticas que de él derivan, proporcionan suficientes fundamentos normativos, propone avanzar en un enfoque de gobernanza multinivel que proporcione soluciones normativas, jurídicas y políticas adaptables y sensibles al contexto, incluyendo instrumentos ascendentes, como la autorregulación ética, pero también leyes constitucionales de protección de los consumidores y otras leyes civiles, y reglamentos de protección de datos y del consumidor, así como instrumentos de derecho indicativo a nivel supranacional²¹⁷.

En materia de leyes, en 2021 Chile aprobó la Ley 21383 que modifica el artículo 19 de la Constitución que protege los derechos humanos a la vida y a la integridad física y psíquica de la persona, para incluir que el desarrollo científico y tecnológico estará al servicio de las personas, como la establece ya la Declaración Universal, y que se llevará acabo respetando los derechos protegidos. La modificación incluye también que la ley regulará los requisitos, condiciones y restricciones para la utilización del desarrollo científico y tecnológico en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella²¹⁸. En agosto de 2023, la Corte Suprema de Chile se refirió al artículo 19 de la Constitución en un fallo referente a la comercialización y uso en el país del dispositivo Insight, que permite recoger y almacenar información neuronal. La Corte se refirió al artículo constitucional para destacar que el dispositivo no

²¹³ Naciones Unidas, "Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes", 10 de diciembre de 1984, artículo 1. Disponible en: < <https://www.ohchr.org/es/instruments-mechanisms/instruments/convention-against-torture-and-other-cruel-inhuman-or-degrading> >

²¹⁴ Naciones Unidas, "Pacto Internacional de Derechos Civiles y Políticos", 23 de marzo de 1976, artículo 7. Disponible en: < <https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> >

²¹⁵ OpCit, Kellmeyer, página 421

²¹⁶ OpCit, Unesco, 2023, página 33

²¹⁷ OpCit, Kellmeyer, página 42e

²¹⁸ Congreso de Chile, Ley 21383 de 202. Disponible en: < <https://www.bcn.cl/leychile/navegar?idNorma=1166983&idParte=10278855&idVersion=2021-10-25> >



cuenta con todas las autorizaciones pertinentes, y no ha sido evaluado y estudiado por la autoridad sanitaria ²¹⁹.

Por su parte, un esfuerzo supranacional que parte de reconocer la normativa existente en materia de derechos humanos y destaca la importancia de garantizar su protección y respeto integral es la Declaración de Principios Interamericanos en Materia de Neurociencia, Neurotecnología y Derechos Humanos²²⁰, adoptada en marzo de 2023 en el seno del Comité Jurídico Interamericano de la Organización de los Estados Americanos, encargado de promover el desarrollo progresivo y la codificación del derecho internacional y de estudiar la posibilidad de uniformar las legislaciones de los países del Continente. La Declaración promueve un enfoque basado en Derechos Humanos en el desarrollo de las neurotecnologías, sus modos de investigación, como en su implementación, comercialización, evaluación y uso.

La Declaración, además de referirse a los derechos a la dignidad, la no discriminación, la identidad, el derecho a la privacidad e intimidad, la salud física y mental, innova al abordar por primera vez, en el marco del debate sobre los neuroderechos, la prevención de la tortura y los tratos o penas crueles, inhumanos o degradantes, y reconocer la vulnerabilidad especial ante los efectos nocivos de la neurotecnología, de niñas, niños y adolescentes, personas con discapacidad y personas privadas de libertad²²¹. La Declaración llama a los Estados a ejercer una función contralora de supervisión y fiscalización, para garantizar que el uso y la aplicación de las neurotecnologías se desarrolle conforme a los estándares internacionales en materia de derechos humanos²²².

A manera de conclusión, considerando el ritmo cada vez más acelerado en que el mundo cambia, en gran medida como consecuencia de avances tecnológicos, y los desafíos que esto implica para distintas áreas del conocimiento, en contextos heterogéneos en materia económica, social y política, se destaca la importancia de privilegiar enfoques colaborativos, que hagan contrapeso a la tentación de alterar innecesariamente los limitados consensos universales con que se cuenta en la actualidad.

El marco internacional de los derechos humanos, en particular los instrumentos de la Carta Universal, son el resultado de múltiples encuentros y desencuentros, incluyendo guerras mundiales, por codificar los derechos y libertades mínimos para el goce de una vida digna, atribuyendo la responsabilidad al Estado por su promoción, respeto y garantía. La neurotecnología, con todas sus posibles implicaciones positivas y negativas, no es ni será el único desafío al que ha tenido que responder el derecho internacional de los derechos humanos. La posibilidad de informar su interpretación y de fortalecer su protección mediante normativas domésticas y el desarrollo de

²¹⁹ Corte Suprema de Chile, “Escrito folio N° 217225-2023”. Disponible en: < https://drive.google.com/file/d/1wX2fUrBDTI3B1W_IK_DUOCC-7neQS6Hhu/view >

²²⁰ Comité Jurídico Interamericano de la Organización de Estados Americanos, “Declaración de Principios Interamericanos en Materia de Neurociencia, Neurotecnología y Derechos Humanos”, marzo de 2023. Disponible en: < https://www.oas.org/es/sla/cji/docs/CJI-RES_281_CII-O-23_corr1_ESP.pdf >

²²¹ Ibid, principios 2 y 9

²²² Ibid, principio 9



instrumentos internacionales complementarios es invaluable, y debe protegerse de los peligros de someterlo a nuevas deliberaciones entre gobiernos con agendas e intereses diversos que no siempre convergen con valores democráticos. El camino está dado para seguir avanzando de manera interdisciplinaria en la identificación de los riesgos del avance de la neurotecnología para el conjunto de los derechos humanos, y dada la premura en que todos los actores acá mencionados coinciden, es fundamental avanzar en lugar de estancarse en debates sesgados.





BIBLIOGRAFÍA

Borbón Rodríguez, D. A., Borbón Rodríguez, L. F. ., & León Bustamante, M. A., “Neuroderecho al acceso equitativo a tecnologías de mejora: Análisis desde el posthumanismo, el derecho y la bioética”, 2021, en Revista Iberoamericana De Bioética, (16), 01–15. Disponible en;< <https://doi.org/10.14422/rib.i16.y2021.006> >

Consejo de Europa, “Neurotechnologies and Human Rights Framework: Do We Need New Rights?”. Disponible en: < [https://www.coe.int/en/web/bioethics/round-table-on-the-human-rights-issues-raised-by-the-applications-of-neurotechnologies#{%22106485310%22:\[1\]}>](https://www.coe.int/en/web/bioethics/round-table-on-the-human-rights-issues-raised-by-the-applications-of-neurotechnologies#{%22106485310%22:[1]}>)

Congreso de Chile, Ley 21383 de 202. Disponible en:< <https://www.bcn.cl/leychile/navegar?idNorma=1166983&idParte=10278855&idVersion=2021-10-25>

Costas Trascasas, M., “Evaluación de las implicaciones de la neurotecnología para los derechos humanos: hacia el reconocimiento de los neuroderechos” en Informe del Comité Asesor sobre su 28 período de sesiones ante el Consejo de Derechos Humanos de las Naciones Unidas, A/HRC/AC/28/2, 7 de septiembre de 2022

Comité Jurídico Interamericano de la Organización de Estados Americanos, “Declaración de Principios Interamericanos en Materia de Neurociencia, Neurotecnología y Derechos Humanos”, marzo de 2023. Disponible en: < https://www.oas.org/es/sla/cji/docs/CJI-RES_281_CII-O-23_corr1_ESP.pdf

Corte Suprema de Chile, “Escrito folio N° 217225-2023”. Disponible en: < https://drive.google.com/file/d/1wX2fUrBDTI3B1W_IK_DUOCC7neQS6Hhu/view

Eunice Kennedy Shriver National Institute of Child Health and Human Development, “Cuáles son las Partes del Sistema Nervioso?”. Disponible en < <https://espanol.nichd.nih.gov/salud/temas/neuro/informacion/partes>>.

Fair Trials, “El Parlamento Europeo aprueba una ley histórica sobre Inteligencia Artificial”. Disponible en: < <https://www.fairtrials.org/articles/news/el-parlamento-europeo-aprueba-una-ley-historica-sobre-inteligencia-artificial/>>

Frasnelli, E., “Evolution and function of neurocognitive systems in non-human animals”. Sci Rep 11, 23487 (2021).

Garvi, Carvajal, A., “Neuroderechos, una garantía para evitar ‘hackear’ el cerebro”, 14 de marzo de 2022, en Cinco Días 45. Disponible en: <https://cincodias.elpais.com/cincodias/2022/03/11/legal/1646988690_719731.html>



Herrera, Camarillo, L., “¿Qué es la neurociencia y cuál es su importancia?”, Universidad Iberoamericana, Ciudad de México, 27 de marzo de 2023. Disponible en: < <https://ibero.mx/prensa/que-es-la-neurociencia-y-cual-es-su-importancia>>.

IEEE Brain, “Neurotechnology: The Next Technology Frontier”. Disponible en <<https://brain.ieee.org/topics/neurotechnologies-the-next-technology-frontier/#:~:text=“Neurotechnology”%20refers%20to%20any%20technology,mental%20illness%20or%20sleep%20patterns>>.

Ilenca, M., “Neuroderechos: Por qué debemos actuar antes de que sea demasiado tarde”, en Anuario Internacional CIDOB 2021. Disponible en: < https://www.cidob.org/articulos/anuario_internacional_cidob/2021/neuroderechos_por_que_debemos_actuar_antes_de_que_sea_demasiado_tarde>

Ilenca, M., “Common human rights challenges realised by different applications of neurotechnologies in the biomedical fields” Consejo de Europa, 2021. Disponible en: < <https://rm.coe.int/report-fil-nal-en/1680a429f3>>.

Ilenca, M., Andorno, R., “Towards new human rights in the age of neuroscience and neurotechnology.” En Life Sci Soc Policy 13, 5, 2017. Disponible en: < <https://doi.org/10.1186/s40504-017-0050-1>>

Iniciativa contra la Tortura, la Asociación para la Prevención de la Tortura y el Centro Noruego de Derechos Humanos, “Principios sobre Entrevistas Efectivas para Investigación y Recopilación de Información”, 2021. Disponible en: < https://www.apt.ch/sites/default/files/publications/apt_PoEI_SPA_04.pdf>

Kellmeyer, P., “A Human Rights–Based Approach for Governing Neurotechnologies” from Part VII - Responsible AI Healthcare and Neurotechnology Governance, en The Cambridge Handbook of Responsible Artificial Intelligence Interdisciplinary Perspectives, Cambridge University Press, 2022

Naciones Unidas “Declaración Universal de los Derechos Humanos”. Disponible en: < <https://www.un.org/es/about-us/udhr/foundation-of-international-human-rights-law>>

Naciones Unidas, “Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes”, 10 de diciembre de 1984, artículo 1. Disponible en: < <https://www.ohchr.org/es/instruments-mechanisms/instruments/convention-against-torture-and-other-cruel-inhuman-or-degrading>>

Naciones Unidas, “Pacto Internacional de Derechos Civiles y Políticos”, 23 de marzo de 1976, artículo 7. Disponible en: < <https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>>

Naciones Unidas, “Es urgente establecer un marco ético sobre neurotecnología a escala internacional”, en Noticias ONU, 6 de junio de 2023. Disponible en: < <https://news.un.org/es/story/2023/06/1521747>>.



Neurorights Initiative, "The five neurorights". Disponible en: https://neurorights-initiative.site.drupal-disttest.cc.columbia.edu/sites/default/files/content/The%20Five%20Ethical%20NeuroRights%20updated%20pdf_0.pdf

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "Protocolo de Minnesota para la Investigación de Muertes Potencialmente Ilícitas", Nueva York y Ginebra, 1991, 2017. Disponible en: https://www.ohchr.org/sites/default/files/Documents/Publications/MinnesotaProtocol_SP.pdf

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "Protocolo de Estambul; Manual para la Investigación y Documentación Eficaces de la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes", Nueva York, 2001, 2004, 2022. Disponible en: https://www.ohchr.org/sites/default/files/documents/publications/2022-06-29/Istanbul-Protocol_Rev2_EN.pdf

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos y The Human Rights Center at the University of California, Berkeley, School of Law, "Protocolo de Berkeley para la Investigación de Código Abierto de Archivos Digitales", Nueva York, 2022. Disponible en: https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf

Organization for Economic Co-operation and Development, "Recommendation on Responsible Innovation in Neurotechnology", OECD/LEGAL/0457, 11 de septiembre de 2019. Disponible en: <https://www.oecd.org/science/recommendation-on-responsible-innovation-in-neurotechnology.htm>

UNESCO, "Ethics of Neurotechnology: UNESCO, leaders and top experts call for solid governance", julio de 2023. Disponible en: <https://www.unesco.org/en/articles/ethics-neurotechnology-unesco-leaders-and-top-experts-call-solid-governance>.

UNESCO, "Unveiling the neurotechnology landscape: scientific advancements, innovations and major trends", 2023. Disponible en: <https://unesdoc.unesco.org/ark:/48223/pf0000386137>.

UNESCO, "Declaración Universal sobre Bioética y Derechos Humanos", 19 de octubre de 2005. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000146180_spa

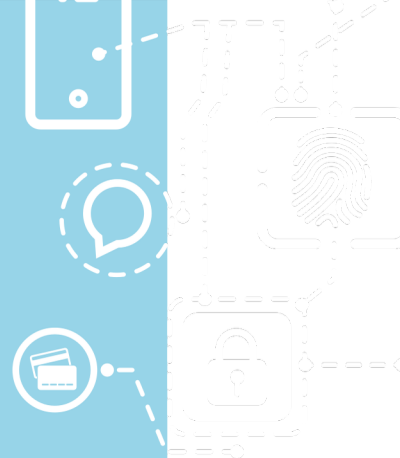
UNESCO, "Recomendación sobre la Ética de la Inteligencia Artificial", 2021. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa

Yuste, R., Goering, S., Arcas, B. et al., "Four ethical priorities for neurotechnologies and AI" en *Nature* 551, 159–163, 2017. Disponible en: <https://doi.org/10.1038/551159a>



ANEXO 4

SONRÍA, USTED ESTÁ SIENDO VIGILADO. LOS LÍMITES Y RIESGOS DEL RECONOCIMIENTO FACIAL COMO HERRAMIENTA DE SEGURIDAD.



Por: Carolina Botero ²²³ y Juan de Brigard ²²⁴

Introducción

“El hombre criminal” es el título del libro, publicado por primera vez en 1876, en que el médico psiquiatra y criminólogo Cesare Lombroso compiló sus teorías sobre el origen fisiológico de la conducta criminal.²²⁵ A lo largo del texto Lombroso defiende, apoyándose en los mejores argumentos que la ciencia y la tecnología del momento podían ofrecer, la idea de que la fisiología de las personas –el tamaño de su cráneo, la forma de los huesos de su rostro y sus expresiones faciales– permitía inferir, con la certeza determinista del positivismo científico, su propensión a conductas antijurídicas. La pretensión de Lombroso se extendía mucho más allá de una simple descripción etnográfica: como científico que era, su trabajo tenía una intención predictiva. Si es posible distinguir al criminal del no-criminal por su fisonomía, es también posible intervenir antes de que el crimen tenga lugar. La antropología criminal de fines del siglo XIX era la promesa de que el crimen puede predecirse en el rostro²²⁶ incluso antes de que sea cometido.

Las teorías de Lombroso, a las que se suman otros como Francis Galton, eugenista inglés, y Alphonse Bertillon, criminólogo francés,²²⁷ tuvieron una amplia resonancia entre los nacientes cuerpos de policía de occidente que, en el marco de la modernidad, estaban ávidos de desarrollos técnicos que permitieran dar legitimidad científica a sus prácticas y prejuicios. Así empezaron

²²³ Es directora de la Fundación Karisma. Columnista de El Espectador y La Silla Vacía. Abogada, Máster en Derecho internacional y de la cooperación, y Máster en Derecho del Comercio y la Contratación. Desde hace más de una década trabaja en la promoción y defensa de los derechos humanos en Internet. Forma parte de la Junta Directiva de Creative Commons y de CSISAC, el grupo observador de la sociedad civil ante la OCDE.

²²⁴ Es coordinador del área de Autonomía y Dignidad en la Fundación Karisma. Estudió filosofía en la Universidad de los Andes, e hizo la maestría en bioética en la Universidad Javeriana. Está particularmente interesado en los límites éticos de los usos de la tecnología en ámbitos como la seguridad y la salud, así como en la interacción entre desigualdad y tecnología.

²²⁵ Cesare Lombroso, Mary Gibson, y Nicole Hahn Rafter, *Criminal Man* (Durham, NC: Duke University Press, 2006).

²²⁶ Cesar Lombroso, English: *Picture of criminals, according to Lombroso. Dates back to ca. 1880. Author: Cesar Lombroso (died in 1909). Français: L'homme criminel. Étude anthropologique et psychiatrique. Traduit sur la quatrième édition italienne par MM. Régnier et Bournet et précédé d'une préface du Dr Ch. Létourneau. Paris: Ancienne Librairie Germer Baillière et Cie, Félix Alcan, Éditeur, 1887.*, Cesar Lombroso, accedido 18 de julio de 2023, https://commons.wikimedia.org/wiki/File:Lombroso_1.jpg#/media/File:Lombroso_1.jpg.

²²⁷ Kelly Gates, *Our biometric future: facial recognition technology and the culture of surveillance*, Critical cultural communication (New York: New York University Press, 2011).



a llegar a las comisarías del mundo cámaras para tomar fotografías de rostros –tanto de frente como de perfil– orejas, narices, ojos y cicatrices,²²⁸ y se desarrollaron fichas técnicas en que se consignaba “el nombre, lugar de nacimiento, procedencia familiar, edad, estatura, color y forma del cabello, tamaño de la frente, las cejas, los ojos, la nariz, la boca, el color de la barba, el rostro y las señales particulares”.²²⁹ Las fotos y las fichas servían un propósito doble: permitían fijar la identidad de los criminales para poder identificarlos y someterlos si reincidían, y –para los suscriptores de la teoría de Lombroso– permitían también anticiparse a esa reincidencia calculando su probabilidad.

Hoy en día la herencia de Lombroso se ha erosionado bastante: en general hemos dejado atrás las formas más extremadamente explícitas y racistas de la antropología criminal europea: ya no asociamos las formas y tamaños del cráneo a comportamientos ilegales y –aunque aún ocurra–²³⁰ ya no consideramos legítimo ni científicamente justificable asociar el color de piel de una persona con el carácter criminal.

En todo caso, la labor policial ha seguido tecnificándose progresivamente. Nuevas herramientas como softwares de predicción del delito,²³¹ cámaras corporales,²³² softwares de inteligencia de fuentes abiertas (OSINT) o tecnologías de inteligencia de señales (SIGINT),²³³ entre otros, han entrado al arsenal de las fuerzas del orden. Y por más que ya no confiemos en la promesa de poder anticipar el crimen en el rostro, la identificación facial como pieza clave del discurso de seguridad sigue presente y se apoya en cámaras cada vez más capaces y métodos más complejos y sofisticados. Además, muchas de estas tecnologías fomentan –a la vez que dependen de– la creciente datificación que avanza en todo el mundo. Sin duda, la identificación mediante registros biométricos es un ejemplo de ello.

Para comprender el alcance del problema empecemos por su definición: la biometría es una técnica que permite medir características corporales o comportamentales individuales, que se presumen inalterables y únicas, y que deben permitir identificar a una persona a lo largo de su vida y

²²⁸ «Deviance, disorder and the self Criminality», accedido 18 de julio de 2023, <http://www7.bbk.ac.uk/deviance/criminality/french/36-20%20larcassagne%20ears%20page1.htm>.

²²⁹ Max-Sebastián Hering Torres, 1892: un año insignificante: orden policial y desorden social en la Bogotá de fin de siglo (Bogotá: Crítica Universidad Nacional de Colombia, 2018).

²³⁰ «Report to the United Nations on Racial Disparities in the U.S. Criminal Justice System», The Sentencing Project, 19 de abril de 2018, <https://www.sentencingproject.org/reports/report-to-the-united-nations-on-racial-disparities-in-the-u-s-criminal-justice-system/>; Drew Desilver, Michael Lipka, y Dalia Fahmy, «10 Things We Know about Race and Policing in the U.S.», *Pew Research Center* (blog), accedido 31 de julio de 2023, <https://www.pewresearch.org/short-reads/2020/06/03/10-things-we-know-about-race-and-policing-in-the-u-s/>; Radley Balko, «There's Overwhelming Evidence That the Criminal Justice System Is Racist. Here's the Proof.», *Washington Post*, accedido 31 de julio de 2023, <https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/>.

²³¹ Egbert, S. *About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany*. 2018. <https://doi.org/10.1007/s41125-017-0027-3>

²³² Barak Ariel, «Police Body Cameras in Large Police Departments», *The Journal of Criminal Law and Criminology* (1973-) 106, n.o 4 (2016): 729-68. Ver también el número 14(1) de la revista *Surveillance & Society* dedicado a la discusión sobre cámaras corporales que puede accederse aquí: https://ojs.library.queensu.ca/index.php/surveillance-and-society/issue/view/Open_2016

²³³ «Cuando el estado vigila. Ciberpatrullaje y OSINT en Colombia Fundación Karisma», accedido 26 de julio de 2023, <https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia/>.



distinguirla de otras.²³⁴ Diversos métodos y características biométricas son usadas en todo tipo de procesos que requieren verificar la identidad de las personas, como trámites financieros, el ejercicio del derecho al voto en ciertos países e incluso el acceso a servicios sociales del Estado. Pero más allá de eso, tanto su origen histórico como su tecnificación y sofisticación han implicado que perviva sobre todo como una herramienta para combatir el crimen, ya no sobre la base de la predicción frenológica del delito y la antropología criminal del siglo diecinueve, sino como un elemento del aparato securitario de vigilancia, en el cual los sistemas de reconocimiento facial basados en biometría son cada vez más ubicuos.²³⁵

Los desarrollos recientes que automatizan el reconocimiento biométrico –además de heredar algunas de las taras anteriores, como veremos más adelante– han traído consigo su propio conjunto de dificultades y riesgos y tensiones frente a derechos. En este artículo nos ocuparemos del uso actual de tecnología de reconocimiento facial como herramienta para combatir el crimen. El texto se divide en tres secciones: la primera explora los mecanismos tecnológicos, el dato biométrico como tal y las bases necesarias para su operación, revisando brevemente la protección de datos personales como un mecanismo de garantía de derechos frente al reconocimiento facial; la segunda explora los límites técnicos, los fallos propios de la tecnología y los sesgos que pueden estar implícitos; la tercera explora las concepciones de justicia y seguridad que subyacen al uso de esta tecnología, así como las consecuencias sociales que puede implicar su uso. Por último, el texto ofrece una serie de recomendaciones al respecto de las regulaciones que deberían implementarse para reducir los impactos negativos de su uso sobre los derechos de la población.

Sección primera - Cuerpos hechos datos

La forma más rudimentaria de reconocimiento facial es la contrastación simple de la foto de un rostro con la persona presente: es el tipo de control al que estamos acostumbrados cuando un agente de policía nos exige el documento de identidad o cuando, durante el procedimiento migratorio, controlan nuestra visa en el pasaporte, por ejemplo. Se trata, evidentemente, de verificar que la persona que presenta el documento que lo identifica como ciudadano ante el Estado o como titular de la visa, respectivamente, sí es quien dice ser. Este proceso, al que llamamos *verificación*, es el primero que la tecnología automatizada de reconocimiento facial pretende replicar.

Para conseguirlo, la tecnología opera de la siguiente manera: partiendo de una imagen del rostro –que puede ser de dos o tres dimensiones– un primer algoritmo la procesa, ubicando zonas o puntos clave del rostro y midiendo las distancias y ángulos entre ellos, para abstraer la información

²³⁴ Aunque nuestra definición se apoya en la norma técnica («ISO/IEC 2382-37:2022 Information technology –Vocabulary –Part 37: Biometrics», 2022, <https://www.iso.org/standard/73514.html>.) diverge en la medida en que no considera que la biometría se refiere únicamente a los procesos automatizados de reconocimiento o identificación.

²³⁵ «Facial Recognition Is Everywhere. Here's What We Can Do About It.», Wirecutter: Reviews for the Real World (blog), 15 de julio de 2020, <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/>.



geométrica de cada cara.²³⁶ Mediante este proceso se construye una plantilla, que es una representación numérica –ya no gráfica– de ese rostro individual. En el reconocimiento facial esta plantilla es comparada por un segundo algoritmo²³⁷ con otra u otras plantillas de rostros. Tras la comparación el sistema arroja un valor numérico que indica, en términos probabilísticos, la posibilidad de que dos plantillas corresponden al mismo rostro, es decir, la probabilidad de que efectivamente se trate de la misma persona en ambas imágenes.

El segundo proceso que la tecnología busca automatizar se parece más bien a una rueda de identificación policial o una línea de sospechosos, lo que en inglés se conoce como un *police lineup*. En ese contexto, la víctima de un crimen conoce –en principio– el rostro de su agresor, pero ninguna otra información. Para dar con su identidad la policía presenta ante la víctima un grupo de sospechosos y esta debe indicar quién, dentro de ese grupo, coincide con su recuerdo del agresor. La *identificación biométrica* es similar: se parte del dato biométrico de un (presunto) criminal, obtenido a partir de una foto, un video o una huella dactilar recogida de una escena del crimen o capturada previamente, para luego contrastar esa plantilla contra todos los registros de una base de datos dada hasta que se encuentre una coincidencia –que nuevamente se expresa en términos probabilísticos– entre el dato recogido y un registro específico dentro de la base. Dado que la base de datos biométricos asocia cada plantilla con datos adicionales de la persona como su nombre o su número de identificación, por ejemplo, esto debería conducir a su identificación.

En todos los procesos de reconocimiento facial –es decir, tanto para los procesos de verificación como para los de identificación– es necesario tener dos imágenes: la primera corresponderá a la foto o fotos original(es) con que se construye la plantilla almacenada en una base de datos –por ejemplo, la foto en la base de datos de registro público, como es el caso de la Registraduría Nacional del Estado Civil en Colombia, la foto de rostros de sospechosos de la INTERPOL²³⁸ o las fotos que se toman para generar la plantilla guardada en nuestro teléfono al momento de configurar el reconocimiento facial para desbloquearlo– y una segunda imagen que usualmente se obtiene en el momento de realizar el reconocimiento y se contrasta con dicho registro previo. También es posible que la imagen a contrastar se capture mediante, por ejemplo, una cámara de vigilancia en el espacio público.

Así, en el proceso de *verificación* biométrica se lleva a cabo una comparación de una plantilla contra otra específica buscando coincidencia o divergencia entre las dos (comparación 1:1), mientras que en el proceso de *identificación* biométrica la plantilla se compara con una base entera para ver si coincide con alguno de los registros almacenados (1:N). Esta breve explicación ya nos permite abordar un primer conjunto de retos propios del uso de biometría facial en contextos securitarios, a saber, las implicaciones de concebir el rostro como un dato y las bases de datos biométricas y su manejo.

²³⁶ Relly Victoria Petrescu, «Face Recognition as a Biometric Application», SSRN Electronic Journal, 2019, <https://doi.org/10.2139/ssrn.3417325>.

²³⁷ Para una revisión de los tipos de algoritmos específicos que se utilizan en este paso clave de comparar los rostros revisar: Paramjit Kaur et al., «Facial-Recognition Algorithms: A Literature Review», *Medicine, Science and the Law* 60, n.o 2 (abril de 2020): 131-39, <https://doi.org/10.1177/0025802419893168>.

²³⁸ INTERPOL, «Our 19 Databases», accedido 31 de julio de 2023, <https://www.interpol.int/How-we-work/Databases/Our-19-databases>.



¿Es el rostro un dato?

Las bases de datos que almacenan información biométrica son colecciones diferentes de las que almacenan otras informaciones personales. Empecemos por lo evidente: los datos biométricos son, en los países con leyes de protección de datos, al menos, datos sensibles y están sujetos a garantías particulares, por lo que deben ser tratados con especial cuidado. En Colombia, por ejemplo, la ley 1581 de 2012 prohíbe, en general el tratamiento de datos sensibles, permitiéndolo sólo en cinco casos excepcionales. Dicha ley considera sensibles aquellos datos que “afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación”.²³⁹ En el caso de los datos biométricos faciales esto es central puesto que, por su naturaleza, siempre se recogen para identificar o verificar la identidad del titular.

Por otra parte, el hecho de que pueden generar discriminación no es menor: los demás datos que permiten identificar a las personas en el marco de procesos judiciales –como el nombre o incluso otras formas de biometría como las huellas dactilares, las huellas palmares o el iris– no cargan con una cantidad tan grande de información implícita como el rostro, y por lo mismo es menos probable que sean utilizadas de manera discriminatoria. Si bien el nombre permite hacer inferencias –acertadas o erradas– sobre la identidad de género de una persona o sobre su procedencia regional, por ejemplo, el rostro releva de manera mucho más decisiva el perfil racial de la persona, elementos sobre su expresión de género y su edad aparente. Cada una de estas características es susceptible de leerse de manera discriminatoria y su revelación dentro de un proceso judicial puede redundar en un trato desigual para la persona sospechosa. En este sentido, siempre que sea posible elegir, deberían preferirse otros datos biométricos menos invasivos.

Aunque podría sostenerse que la plantilla matemática que se utiliza para el reconocimiento facial, en la medida en que es una abstracción matemática, no permite conocer de manera evidente la información implícita sobre edad, expresión de género o raza, en la práctica los softwares de procesamiento rara vez separan esta plantilla matemática de la imagen del rostro. En este sentido, aunque esta forma de anonimización de los datos sería en teoría posible y es ofrecida por algunas compañías,²⁴⁰ no necesariamente es irreversible, no es una práctica estándar en este tipo de tecnología, ni mucho menos es una exigencia legal. Sin mencionar que el anonimato evidentemente sólo es aplicable al proceso de autenticación, más no al de identificación.

Más aún, a diferencia de otros datos personales individualizantes (el nombre o los números únicos de identificación, en los países en que estos se utilizan, por ejemplo), los datos biométricos no están arbitraria ni convencionalmente asociados con la persona, sino que están atados a ella por el hecho de tener ese cuerpo. El nombre y el número de cédula nos son asignados a través de procesos culturales y administrativos, y en casos excepcionales son susceptibles de cambiar (por

²³⁹ «Ley 1581 de 2012 - Por la cual se dictan disposiciones generales para la protección de datos personales.», revisado el 25 de julio de 2023, <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

²⁴⁰ «Solutions, United Biometrics», *United Biometrics* (blog), 2 de diciembre de 2020, <https://unitedbiometrics.com/solutions/>.



ejemplo, en el caso colombiano, con el cambio legal de sexo)²⁴¹. Por su parte, nuestros rostros y nuestras huellas no pueden ser reasignados, no podemos renunciar a ellos y cuando cambian sustancialmente lo hacen –en general– por procesos ajenos a nuestro control, como el envejecimiento o los accidentes que deforman el rostro. Si nuestros datos biométricos son robados no podemos simplemente renovarlos, como sí podemos hacer con una contraseña o una tarjeta de crédito.

Ciertos ejemplos límite nos muestran las implicaciones de la relación de absoluta indisociabilidad entre la persona y sus datos biométricos: los casos de automutilación de huellas dactilares en criminales o migrantes que quieren evitar ser identificados por medio de sistemas biométricos²⁴² y célebres ejemplos de narcotraficantes colombianos que –como alias “Chupeta”²⁴³– se someten a cirugías plásticas para alterar su rostro²⁴⁴ y evadir el control policial. Las compañías que desarrollan tecnologías de reconocimiento biométrico, por supuesto, ven en esta indisociabilidad un estándar de seguridad mayor y están buscando constantemente mejorar sus sistemas²⁴⁵ para garantizar que puedan seguir identificando a las personas aún cuando han intervenido su rostro o sus huellas, pero este sigue siendo un reto importante y no del todo resuelto.

La concepción del rostro como dato implica otra dificultad adicional y es el hecho de que el rostro está, en las condiciones normales de las sociedades occidentales, públicamente expuesto. Contrario a otros datos personales que elegimos cuándo entregar o cuándo retener (¿le damos nuestros nombres a los extraños por el teléfono? ¿publicamos nuestra dirección de residencia en internet?) el rostro, usualmente descubierto, hace parte de todas nuestras interacciones presenciales y muchas de nuestras interacciones virtuales sin que consideremos siquiera que estamos entregando información personal. En este sentido, el reconocimiento facial como mecanismo de identificación aprovecha el carácter público –en términos prácticos, no necesariamente legales– de un dato que por su naturaleza es sensible.

²⁴¹ En las cédulas de ciudadanía colombianas anteriores a 2003, había rangos numéricos que correspondían a hombres y mujeres respectivamente. Por esta razón al solicitar el cambio de sexo en el registro de nacimiento, a la persona se le asignaba un nuevo número de identidad correspondiente con el sexo hacia el que transitaba. Desde 2003 en Colombia se utiliza un Número Único de Identificación Personal (NUIP) que no tiene información implícita, más allá de asignarse consecutivamente, lo que permite hacer estimaciones al respecto de la edad de la persona a partir del número. Por esta razón este número no cambia si la persona solicita el cambio de sexo ante la Dirección Nacional de Identificación de la RNEC. Ver <https://www.registraduria.gov.co/Asignacion-de-un-nuevo-numero-de-cedula-por-cambio-de-sexo.html>

²⁴² K Wertheim, «Extreme Case of Fingerprint Mutilation», *Journal of Forensic Identification* 48, n.o 4 (agosto de 1998): 466-77; «Calais migrants mutilate fingertips to hide true identity | Daily Mail Online», accedido 26 de julio de 2023, <https://www.dailymail.co.uk/news/article-1201126/Calais-migrants-mutilate-fingertips-hide-true-identity.html>.

²⁴³ «Drug Lord Who Changed His Face Testifies against “El Chapo”», NBC News, 30 de noviembre de 2018, <https://www.nbcnews.com/news/us-news/el-chapo-trial-drug-lord-who-changed-his-face-testifies-n942116>.

²⁴⁴ Redacción Justicia, «Las cirugías con las que “narcos” han buscado evadir su captura», *El Tiempo*, 19 de noviembre de 2020, sec. justicia, <https://www.eltiempo.com/justicia/conflicto-y-narcotrafico/narcos-que-se-han-operado-para-cambiar-su-apariencia-y-evadir-captura-549891>.

²⁴⁵ Christian Rathgeb et al., «Plastic Surgery: An Obstacle for Deep Face Recognition?», en 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) (2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Seattle, WA, USA: IEEE, 2020), 3510-17, <https://doi.org/10.1109/CVPRW50498.2020.00411>; Kevin J. Zuo, Tomas J. Saun, y Christopher R. Forrest, «Facial Recognition Technology: A Primer for Plastic Surgeons», *Plastic and Reconstructive Surgery* 143, n.o 6 (junio de 2019): 1298e-1306e, <https://doi.org/10.1097/PRS.0000000000005673>.



Para el caso colombiano, por ejemplo, la Corte Constitucional ha dicho que “el anonimato es un elemento esencial del derecho a la libertad de expresión”,²⁴⁶ pero la utilización de biometría facial para la identificación por parte de la fuerza pública implica que este derecho se hace efectivamente imposible de ejercer en el espacio público, salvo que se oculte el rostro. Y por supuesto que es posible salir a la calle con el rostro cubierto o maquillado hasta ser irreconocible, pero en un sentido práctico esto sólo reduplica las sospechas sobre los individuos. Obligar a las personas, por ejemplo en una manifestación, a ocultar su rostro por temor a poder ser identificados mediante biometría facial y posteriormente perfilados es una manera de deslegitimar el derecho a protestar y de convertir automáticamente en sospechoso a todo aquel que decida no mostrar su cara.

Al mismo tiempo, para un delincuente común es fácil ocultar el rostro, pero de cierta manera está con ello invirtiendo la carga que queda sobre todas las demás personas, pues deben transitar el espacio público con su rostro descubierto y disponible ante la autoridad para que sea posible garantizar que no son sospechosas.²⁴⁷ ¿Qué ocurre aquí con la presunción de inocencia? En un sentido parece que la sola inclusión de nuestros datos biométricos en una base, a la que la autoridad policial o judicial de un país puede acceder, implica que se nos trate permanentemente como sospechosos. Tal base de datos opera –si se nos permite utilizar nuevamente la analogía– como una inmensa fila de identificación policial en que todos los individuos estamos constantemente formados, esperando a que en algún momento se nos identifique como delincuentes. Es decir, el reconocimiento facial, si se utiliza en el espacio público, es un mecanismo de vigilancia masiva.

Del hecho de que el rostro esté públicamente expuesto se desprende una última consecuencia problemática: el reconocimiento facial puede hacerse sin el consentimiento y sin el conocimiento de quien está siendo reconocido. Contrario a lo que ocurre con las huellas digitales, cuya contrastación en la gran mayoría de los casos depende de que la persona presione su dedo contra un lector digital o del iris que obliga a la persona a abrir los ojos frente a un lector ubicado cerca del rostro, la posibilidad de identificar personas a partir de fotografías o videos de su cara abre la puerta a que quien está siendo identificado ni siquiera sepa que eso está ocurriendo y no pueda rehusarse a ello. Nuestros datos biométricos son una réplica de nuestro cuerpo que espera en las estaciones de policía sin que nosotros estemos presentes y sin necesidad de que se nos informe cuándo estamos siendo, *in absentia*, interrogados sobre nuestra identidad.

Y hasta aquí hemos asumido que quien lleva a cabo la identificación está actuando dentro de su legítima competencia, pero ¿qué sucede cuando este no es el caso? En todas las demás circunstancias en que nuestra identidad se verifica a partir de algo que sabemos (por ejemplo una contraseña o incluso nuestro nombre) nos es posible simplemente mentir para evitar ser identifi-

²⁴⁶ Corte Constitucional de Colombia, «Sentencia SU420-19», accedido 26 de julio de 2023, <https://www.corteconstitucional.gov.co/relatoria/2019/SU420-19.htm>.

²⁴⁷ Esto se evidencia, por ejemplo, en el artículo 353 A del código penal Colombiano, que se refiere a la “Obstrucción a vías públicas que afecten el orden público”. Con frecuencia este es uno de los cargos que se le imputa a las personas que han participado en protestas sociales y, desde 2022, contempla la siguiente circunstancia de agravación punitiva: “1. Cuando se empleen máscaras o elementos similares que sirvan para ocultar la identidad o la dificulten.” (Ley 599 de 2000 Por la cual se expide el Código Penal y Ley 2197 de 2022 Por medio de la cual se dictan normas tendientes al fortalecimiento de la seguridad ciudadana y se dictan otras disposiciones).



cados. Esta es, sin duda, una salvaguardia importante para nuestra seguridad. La biometría cierra esta posibilidad de plano y hace que nos sea imposible resistir a la autenticación o identificación cuando, por ejemplo, alguien desbloquea nuestro celular sosteniéndolo frente a nuestro rostro o fuerza nuestra mano contra el lector de huellas digitales.

Esto no es sólo importante como defensa frente a un asaltante, un chantajista o incluso una pareja abusiva, sino que incluso puede ser determinante como mecanismo de resistencia frente a la violencia Estatal: en el marco del estallido social del 2021 en Colombia varias organizaciones reportaron que los agentes de policía, actuando por fuera de sus atribuciones, obligaron a manifestantes a desbloquear sus teléfonos para borrar videos e imágenes en que se registraba la violencia policial.²⁴⁸ De ser así, esto habría sido posible, en algunos casos, obligando a las personas a presionar sus dedos contra los lectores de huella de los dispositivos o desbloqueando sus teléfonos con reconocimiento facial.

Con lo que hemos mostrado hasta aquí podemos ver que en los datos biométricos faciales hay una tensión particular y una estructura paradójica. La tensión es la siguiente: como con cualquier dato, buscamos que las plantillas sean una abstracción de la realidad que la simplifique y haga más manejable; pero simultáneamente buscamos que capten todas las características de ese rostro, para poder identificarlo en cualquier contexto y distinguirlo del de cualquier otra persona. La tensión surge entre la necesidad de abstraer y simplificar, por un lado, y la necesidad de conservar toda la información, por el otro. La estructura paradójica es la siguiente: los datos biométricos captan una característica indisociable e inalienable a la persona –a su cuerpo, específicamente– pero permiten que dicha característica circule por fuera del dominio de la persona y aún cuando el cuerpo está ausente. Esto ocurre, por ejemplo, en los casos citados arriba de identificación *in absentia*.

Esta concepción del rostro como un dato y, por extensión, de los datos biométricos como idénticos a otros datos sensibles, no solo deshumaniza nuestro rasgo identitario por excelencia convirtiéndolo en una moneda transable y disociándolo de la persona dueña de ese rostro, sino que circunscribe la cuestión sobre los límites que deberían imponerse a esta tecnología al dominio de la protección de datos personales. En este caso, como en muchos otros en que las implicaciones sociales de la datificación son particularmente apremiantes, la concepción legalista es insuficiente para comprender el fenómeno y para protegernos efectivamente de sus consecuencias negativas, pues las categorías de la ley no son capaces de captar la realidad con todos sus matices e implicaciones.

²⁴⁸ Temblores ONG, «Bolillo, Dios y Patria», 2021, <https://www.temblores.org/bolillo-dios-y-patria>; Carlos Alfonso Negret Mosquera, «Informe Final Para el esclarecimiento de los hechos ocurridos los días 9 y 10 de septiembre de 2020» (Colectivo de abogados José Alvear Restrepo CAJAR, 2021), <https://www.colectivodeabogados.org/wp-content/uploads/2021/12/Informe-Final-Relatori%CC%81a-Esclarecimiento-9S-VF.pdf>.



¿Quién custodia los datos?

Al margen de la discusión al respecto de si el rostro es un dato, podemos afirmar con claridad que las plantillas biométricas sí lo son: son datos personales que se almacenan en bases y se procesan y analizan utilizando computadores. Pero por la compleja naturaleza de estos datos, las implicaciones que existen con respecto al manejo de las bases son amplias.

Al considerar la relación entre reconocimiento facial y bases de datos, las primeras preguntas que surgen tienen que ver con cómo estas se construyen. En lo que respecta a la persecución de criminales estas bases suelen ser las de las fuerzas de policía o las autoridades judiciales de cada país y, especialmente, la base consolidada de reconocimiento facial de la INTERPOL que recoge información de más de 160 países y, de acuerdo con su propia información, ha conducido a la captura de más de 1500 personas desde 2016 cuando empezó a funcionar.²⁴⁹

Las imágenes que conforman las bases nacionales, que a su vez informan la de INTERPOL, suelen provenir de sistemas de identidad nacionales. En ciertos casos, como el de Estados Unidos, se apoyan en otras bases de datos como registros de conductores levantados al momento de expedir la licencia²⁵⁰, mientras que en otros casos, como el de Colombia, se trata de los sistemas de identidad centralizados nacionales. El caso colombiano no es único: en más países cada vez la identidad legal tiende a digitalizarse y la expedición de los documentos que acreditan a las personas como ciudadanas –es decir, que materializa el derecho humano a la identidad legal– implica inevitablemente un registro biométrico y la inserción de las características individuales en una base de datos.

Para comprender las implicaciones de lo anterior revisemos más profundamente el caso colombiano:

“La Corte [Constitucional] ha manifestado que la cédula de ciudadanía constituye un documento cuyos alcances y virtualidades trascienden al ámbito constitucional, pues versa sobre asuntos de la vida personal de los individuos que inciden de modo especial en el propio acontecer de la organización y funcionamiento de la sociedad. De esta manera, la cédula de ciudadanía cumple con tres funciones particulares: i) identificar a las personas; ii) permitir el ejercicio de sus derechos civiles; y iii) asegurar la participación de los ciudadanos en la actividad política dentro de un escenario democrático”.²⁵¹

La expedición del documento nacional de identidad, que desde 2018 incluye, más allá de la foto simple, información biométrica facial, es la manera de garantizar la identidad legal de las personas. Por lo mismo en su expedición no media consentimiento alguno, ni habría cabida a rehusarlo,

²⁴⁹ «INTERPOL - Facial Recognition», accedido 27 de julio de 2023, <https://www.interpol.int/How-we-work/Forensics/Facial-Recognition>.

²⁵⁰ Olivia Solon, «Facial Recognition Database Used by FBI Is out of Control, House Committee Hears», *The Guardian*, 27 de marzo de 2017, sec. Technology, <https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports>.

²⁵¹ Corte Constitucional, 2016. Sentencia T-622 de 2016



en la medida en que este documento es necesario para todas las formas de relacionamiento con el Estado y no tener una cédula resulta imposible en términos prácticos. En Colombia, la garantía del derecho humano a la identidad legal está ineludiblemente atada a la entrega de dos datos biométricos –faciales y dactilares– al Estado.

Sin embargo, la inclusión de estos datos en las bases de la Registraduría Nacional del Estado Civil (RNEC) no está acompañada –ni de cara al titular, ni en términos legales claros– de límites al respecto de lo que esta entidad tiene permitido y lo que no tiene permitido hacer con ellos. Es decir, el principio de finalidad, claramente establecido en la ley de protección de datos (1581 de 2012), queda supeditado al mandato de registro civil propio de la entidad. Esta base de datos no solo se ha construido de manera masiva e indiscriminada con los registros de –progresivamente– todas las personas de Colombia, sino que esto ocurrió sin claridad sobre los usos posibles de dicha información. Por la misma razón, los titulares de los datos no suelen tener conciencia de quién puede acceder a ellos, en qué condiciones y con qué fines.

La RNEC usa estas bases de datos²⁵² para ofrecer servicios de autenticación biométrica a privados y a otras entidades del sector público promocionándolo como un mecanismo eficiente y confiable contra el fraude. Hoy en día la Registraduría tiene acuerdos interadministrativos con la fuerza pública en Colombia, que permiten a la policía y el ejército utilizar estas bases de datos biométricas para hacer autenticación e identificación sin que la ciudadanía se entere o pueda rehusar su consentimiento.²⁵³ Estas prácticas limitan el ejercicio del derecho a la privacidad consagrado en la Constitución política. Esto, además, obliga a preguntarse qué ventaja representa para la autoridad de registro el levantar datos biométricos faciales en el marco de su función constitucional de garantizar la identidad legal. Esta respuesta es imposible de responder sin comprender 1) la lucrativa posibilidad de ofrecer servicios de autenticación biométrica a terceros y 2) el proceso subyacente de securitización que establece una relación directa entre la identificación facial y la seguridad. El segundo aspecto será más ampliamente explorado en la tercera sección del presente artículo.

Sección segunda - La tecnología no es perfecta

En la medida en que la identificación con reconocimiento facial para el uso securitario sigue siendo un terreno en disputa, existe una discusión amplia al respecto de la legitimidad e idoneidad de su uso. En este nicho el nombre de Robert Williams se ha hecho célebre como “el primer caso de un arresto equivocado basado en reconocimiento facial”²⁵⁴. Se trata de un hombre afroamericano

²⁵² Ya existen acuerdos contractuales con entidades financieras que permiten utilizar biometría dactilar y en junio de 2023 se hizo público un piloto para permitir que Rappi, una popular aplicación de envíos y domicilios, utilice reconocimiento facial apoyándose en la base de la RNEC para su área de servicios financieros (Rappipay). al área de servicios financieros (Rappipay). Ver: <https://www.xataka.com.co/empresas-y-economia/rappi-registraduria-anuncian-piloto-para-implementar-biometria-facial-rappipay-colombia>

²⁵³ «El sistema de identidad administrado por la Registraduría Nacional del Estado Civil», accedido 31 de julio de 2023, <https://digitalid.karisma.org.co/2022/11/27/el-sistema-de-identidad-administrado-por-la-Registraduri-a-Nacional-del-Estado-Civil/>.

²⁵⁴ Johana Bhuiyan, «First Man Wrongfully Arrested Because of Facial Recognition Testifies as California Weighs New Bills», *The Guardian*, 27 de abril de 2023, sec. US news, <https://www.theguardian.com/us-news/2023/apr/27/california-police-facial-recognition-software>.



que en 2020 fue acusado de robar relojes en Detroit, Estados Unidos, gracias a que un sistema de reconocimiento facial arrojó una coincidencia entre una imagen captada con una cámara de videovigilancia y la foto de la licencia de conducción del señor Williams.²⁵⁵ Aunque en este caso pudo establecerse que la identificación fue un falso positivo del sistema, el arresto sí tuvo lugar y alguien que no tenía nada que ver con los hechos delictivos tuvo que acudir a la corte a defenderse.²⁵⁶ Casos como este, que sin duda aumentarán si el uso de esta tecnología se expande desreguladamente, señalan hacia los riesgos asociados al funcionamiento –o mejor, la disfunción– de la tecnología.

Nos ocuparemos de tres aspectos de estos riesgos, enfocándonos en la identificación por medio del reconocimiento facial, más que en la autenticación: 1) los casos de falso positivo y falso negativo, 2) la carga de componentes étnico-raciales y de género –así como los determinantes socioeconómicos– en la confiabilidad de la identificación, y 3) la tendencia a la retroalimentación negativa en estos sistemas.

Falsos positivos y falsos negativos

Aunque las tecnologías que utilizamos cotidianamente fallan una y otra vez –el computador en que trabajamos se congela, las llamadas de zoom se entrecortan o el bluetooth se desconecta–, cuando pensamos en la implementación pública de soluciones tecnológicas, con frecuencia olvidamos su falibilidad y, como cualquier otro sistema, las tecnologías de reconocimiento facial también fallan. Podemos clasificar sus errores de reconocimiento en dos grandes grupos: los falsos positivos (FP) y los falsos negativos (FN). En el FP el sistema arroja una coincidencia entre dos fotos que en la realidad no corresponden a la misma persona, como en el caso de Williams citado arriba, mientras que en el FN, una cámara que captó la imagen de una persona y debió haber encontrado una coincidencia, no dispara ninguna alarma. Tanto en los casos en que se busca ubicar a un criminal determinado, como en los casos en que se busca identificar al responsable desconocido de una conducta criminal, la existencia de FP es problemática, pues ambos conducen a que, por una falla en el algoritmo de comparación, un transeúnte desprevenido quede equivocadamente envuelto en una investigación criminal. Los casos de FN son problemáticos en otro sentido: ya no se trata aquí de involucrar a alguien erróneamente en un proceso, sino en confiar en la tecnología para que contribuya a la solución de una necesidad pública, en este caso la judicialización de delincuentes, y encontrar que no es adecuada para este fin y que los recursos dispuestos para ello no conducen a la solución.

²⁵⁵ Stephan Cléménçon y Winston Maxwell, «Why Facial Recognition Algorithms Can't Be Perfectly Fair», The Conversation, 20 de julio de 2020, <http://theconversation.com/why-facial-recognition-algorithms-cant-be-perfectly-fair-142608>.

²⁵⁶ Sidney Fussell, «A Flawed Facial-Recognition System Sent This Man to Jail», Wired, accedido 29 de julio de 2023, <https://www.wired.com/story/flawed-facial-recognition-system-sent-man-jail/>.

²⁵⁷ Patrick Grother, Mei Ngan, y Kayee Hanaoka, «Face Recognition Vendor Test (FRVT) Part 2: Identification» (Gaithersburg, MD: National Institute of Standards and Technology, septiembre de 2019), <https://doi.org/10.6028/NIST.IR.8271>.



Medir cuál es la tasa de FP o FN de un algoritmo particular como una cifra fija no es posible, porque depende de cómo se configure el umbral de éxito (i.e. la probabilidad que se requiere para que el sistema considere que dos caras coinciden). Sin embargo, un estudio comparativo hecho en 2019 por el Instituto nacional de estándares y tecnología de los Estados Unidos (NIST) en que se evaluaron cerca de 200 algoritmos de identificación facial de más de 50 desarrolladores utilizando 4 bases de datos (cerca de 33 millones de imágenes correspondientes a más de 12 millones de personas), muestra que “con fotos de retrato de buena calidad los algoritmos más acertados encuentran coincidencias, en caso de que las haya, en bases de datos de 12 millones de individuos, con tasas de error menores al 0,2%”.²⁵⁷ Esta métrica, que se refiere a los casos en que se buscan coincidencias únicas²⁵⁸ y puede parecer alta, implica que, en las mejores condiciones –es decir con bases de datos de fotos frontales, de retrato y de buena calidad, los algoritmos más acertados– se equivocan, si somos generosos, en una de cada mil búsquedas. Obviamente estas condiciones ideales rara vez se presentan en la realidad: con mucha frecuencia la foto que se tiene para identificar a la persona está lejos de ser una foto frontal de retrato, de buena calidad y en que la persona sale sin gafas, tapabocas o gorra, lo que implica que dicha tasa de una equivocación en cada mil crecerá rápidamente.

Como dijimos más atrás, la cantidad de FP y FN varía en función de qué tan exigentes somos con el algoritmo, sin embargo, lo que sí podemos comparar son las tasas de fallo por FP y por FN entre distintos algoritmos. La precisión de los algoritmos varía mucho más si se miden los FP que arroja, frente a cuando se miden los FN. En general, de acuerdo con otro estudio posterior realizado por la misma entidad estadounidense, entre diferentes algoritmos la tasa de FN no varía por un factor de más de 3, mientras que la tasa de FP puede ser entre 10 y 100 veces mayor en unos algoritmos que otros (en particular cuando se revisan sesgos raciales, como discutiremos más adelante).²⁵⁹ Esto tiene una explicación clara: los algoritmos están diseñados, frecuentemente, para sistemas de enrolamiento en que trata de evitar que una persona ya enrolada en la base no logre acreditarse ante el sistema. Es decir, se diseñan buscando reducir los casos de FN y sobre todo para usos de autenticación, pues este es el uso comercial más frecuente.

Pero a más de eso, el reporte citado –a pesar de su tono optimista por el avance en la precisión de los sistemas de identificación facial– muestra una característica muy preocupante de los algoritmos: “en la medida en que el umbral para reducir falsos positivos se aumenta, los FN aumentan rápidamente. Esto implica que una tasa baja de falsos positivos es inaccesible para estos algoritmos”.²⁶⁰ Y es lógico, son dos caras de la misma moneda: cuando se le pide a un algoritmo que sea más exigente en sus comparaciones para evitar que dos personas diferentes, aunque sean similares en apariencia, den un resultado de coincidencia positiva, es más probable que una misma persona, en dos fotos ligeramente diferentes, sea clasificada por el algoritmo como dos

²⁵⁸ Los *softwares* de identificación suelen ofrecer como resultado, en lugar de una única coincidencia, una lista de entre 1 y 50 rostros que posiblemente coinciden con la búsqueda para luego ser evaluados por una persona. En vez de considerar que 49 de los cincuenta rostros listados son FP, esta tasa de error se calcula para cuando esta lista se limita a una única coincidencia, como si se le exigiera al algoritmo encontrar sólo al más probable de los candidatos, allí los algoritmos más precisos del mercado yeran en el 0,12% y 0,24% de las búsquedas respectivamente.

²⁵⁹ Patrick Grother, Mei Ngan, y Kayee Hanaoka, «Face Recognition Vendor Test Part 3: Demographic Effects» (Gaithersburg, MD: National Institute of Standards and Technology, diciembre de 2019), <https://doi.org/10.6028/NIST.IR.8280>.

²⁶⁰ Grother, Ngan, y Hanaoka, «Face Recognition Vendor Test (FRVT) Part 2».



individuos distintos. Entre más exigentes somos con la similitud de los rostros, más se reducen las posibilidades de que el sistema encuentre coincidencias o, en otras palabras, entre menos tolerantes somos con los FP más probable es que ocurran FN.

Este filo de cuchilla en la que camina todo el reconocimiento biométrico –que le exige ser suficientemente flexible como para poder reconocer el mismo rasgo como idéntico en instancias diferentes, pero suficientemente riguroso para asegurarse de que no son, de hecho, los rasgos de otra persona– implica una precisión que muy difícilmente alcanzará los estándares de confiabilidad que requiere la justicia. Si, con los mejores algoritmos en condiciones muy controladas, sigue existiendo la posibilidad de que uno de cada mil casos sea errado, será muy difícil confiar en la coincidencia que arroje este sistema cuando se le presente una imagen tomada por una cámara de vigilancia de baja resolución, con poca luz y con un rostro ladeado y cubierto por gafas o una gorra.

En este sentido, y por razones técnicas que no pueden superarse, para los delincuentes se vuelve prácticamente trivial evadir el reconocimiento facial o argumentar la posibilidad de que la coincidencia sea un FP. Para ello basta con utilizar tapabocas o bufandas junto con gafas oscuras o gorras. Aunque la tecnología avance rápidamente para poder identificar a las personas utilizando sólo secciones del rostro²⁶¹ y las compañías están trabajando arduamente por conseguir buenos resultados de identificación con rostros parcialmente cubiertos, según un tercer estudio del NIST realizado en 2020²⁶², los algoritmos testeados tienen una tasa de FN de entre el 20 y el 50% cuando el rostro está cubierto por un tapabocas. Si esta tasa de confiabilidad mejora, es muy probable que lo haga a costa de incrementar la probabilidad de que ocurran FP.

Factores raciales, de género y socioeconómicos

Una de las críticas más usuales a los sistemas de reconocimiento facial en su dimensión técnica, tiene que ver con la aserción de que tienen tasas de FP y FN más altas con personas racializadas y mujeres, que con hombres blancos europeos. Esta afirmación, aunque bien documentada,²⁶³ está en constante disputa por parte de los desarrolladores de software y proponentes del uso de tecnología de reconocimiento facial con fines securitarios. A pesar de que el debate sigue abierto, las razones históricas, sociales y culturales subyacentes que explican por qué la tecnología difícilmente puede estar libre de sesgos, no han sido disputadas. Se trata principalmente de fenómenos

²⁶¹ Stephanie Glen, «Sunglasses and Face Mask Won't Fool Facial Recognition Systems Any More - DataScienceCentral.Com», Data Science Central, 11 de octubre de 2021, <https://www.datasciencecentral.com/sunglasses-and-face-mask-wont-fool-facial-recognition/>.

²⁶² Mei Ngan, Patrick Grother, y Kayee Hanaoka, «Ongoing Face Recognition Vendor Test (FRVT) Part 6A:: Face Recognition Accuracy with Masks Using Pre-COVID-19 Algorithms» (Gaithersburg, MD: National Institute of Standards and Technology, julio de 2020), <https://doi.org/10.6028/NIST.IR.8311>.

²⁶³ Clare Garvie Frankle Jonathan, «Facial-Recognition Software Might Have a Racial Bias Problem», The Atlantic, 7 de abril de 2016, <https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/>; David Leslie, «Understanding bias in facial recognition technologies» (Zenodo, 26 de septiembre de 2020), <https://doi.org/10.5281/ZENODO.4050457>; Sidney Perkowitz, «The Bias in the Machine: Facial Recognition Technology and Racial Disparities», MIT Case Studies in Social and Ethical Responsibilities of Computing, n.o Winter 2021 (5 de febrero de 2021), <https://doi.org/10.21428/2c646de5.62272586>.



sociales que preceden a la tecnología, pero que se amplifican por la misma. En aras de no repetir lo ya publicado en suficientes estudios²⁶⁴, veamos sólo cuatro aspectos particularmente relevantes para nuestro contexto latinoamericano.

La principal explicación para que los sistemas de reconocimiento facial funcionen de manera desigual en poblaciones diversas es que los conjuntos de datos utilizados para entrenar los algoritmos encargados del reconocimiento y la comparación no suelen estar balanceados en términos de género o raza. Con frecuencia, en las muestras, los hombres blancos de fenotipo europeo están sobrerrepresentados tanto en términos de la cantidad de las imágenes, como de su calidad. La desproporción de cantidad se explica sencillamente porque el lugar y los recursos con que el software se desarrolla influyen en el tipo de bases de datos a las que es más fácil acceder, por lo que un programa creado, por ejemplo, en España, puede más fácilmente utilizar bases de datos de personas españolas que de otra procedencia, y así se entrena más eficientemente para distinguir a personas cuyo fenotipo es más cercano al español. Si pensamos por ejemplo, en la posibilidad de entrenar algoritmos con las fotografías tomadas para expedir la licencia de conducción, la disparidad entre el número de hombres y mujeres que poseen una licencia²⁶⁵ puede contribuir a explicar por qué los algoritmos son más precisos al reconocer rostros de hombres. Dependiendo del tipo de datos que se utilicen, pueden hallarse ejemplos similares con disparidades propias de las bases.

En términos de la diferencia en calidad, la explicación requiere ir un poco más profundo y referirse, por ejemplo, a la optimización técnica de las películas fotosensibles diseñadas por las compañías de fotos para captar los tonos de piel “blanca” mejor que los de pieles oscuras.²⁶⁶ Esta disparidad, que se reprodujo en los sistemas de fotografía digital,²⁶⁷ implica que los softwares de reconocimiento facial tienen información de peor calidad (por ejemplo, fotografías con menos contraste) tanto para entrenar, como para realizar las comparaciones.

La segunda razón, fuertemente vinculada con la primera, tiene que ver con el hecho de que el *software* usualmente ha sido desarrollado en el norte global. Si bien estudios técnicos citados más arriba sostienen que los algoritmos más precisos son prácticamente igual de precisos con distintos tonos de piel y fenotipos, dicen con claridad que “ciertos algoritmos desarrollados en China mostraron tasas de FP menores en rostros [de personas] del este de Asia, y en algunos casos estas fueron menores que las de rostros caucásicos.”²⁶⁸ Lo anterior lleva a pensar que, en la medida en que ciertos países o regiones del mundo con poblaciones fenotípicamente diversas, como latinoamérica, sigan utilizando algoritmos desarrollados en otros contextos, la tasa de error.

²⁶⁴ Ver nota anterior.

²⁶⁵ «Las mujeres son más seguras al volante que los hombres | Motor», accedido 29 de julio de 2023, <https://www.elmundo.es/motor/2022/03/08/62267f3dfdddf8b8e8b45ce.html>.

²⁶⁶ Sarah Lewis, «The Racial Bias Built Into Photography», *The New York Times*, 25 de abril de 2019, sec. Lens, <https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html>.

²⁶⁷ Wired UK, «How to Make a Genuinely Inclusive Phone Camera», *Wired UK*, accedido 29 de julio de 2023, <https://www.wired.co.uk/article/inclusive-cameras-apple-google>.

²⁶⁸ Grother, Ngan, y Hanaoka, «Face Recognition Vendor Test Part 3». Traducción propia.



en sus procesos de identificación será mayor que el óptimo ofrecido por el desarrollador y difícilmente mejorará sin reentrenamientos específicos, que pueden ser costosos.

En tercer lugar vale la pena considerar los efectos de esta tecnología sobre las minorías. Es natural que las personas que pertenecen a estos grupos humanos, por el hecho mismo de que son minoritarios, estén subrepresentadas en las bases de datos. Piénsese por ejemplo en los distintos pueblos indígenas de Colombia, no sólo sería más difícil conseguir los datos necesarios –garantizando la calidad– para entrenar los algoritmos con su información facial, sino que la muestra probablemente siempre será proporcionalmente menor en la medida en que representan una minoría. Esto implica que las minorías con fenotipos particulares tenderán a estar subrepresentadas y siempre será más probable que los algoritmos procesen su información con menos fiabilidad.

No cabe duda de que las tecnologías biométricas han heredado las perspectivas racistas desde las cuales han surgido. Esto lo ha señalado la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, al indicar que el uso de tecnologías biométricas puede generar estructuras discriminatorias que “de manera holística o sistemática socavaban el disfrute de los derechos humanos de determinados grupos por motivos de raza u origen étnico o nacional, en combinación con otras características”.²⁶⁹

Por último, en la medida en que la identificación de criminales normalmente tendría que hacerse sobre imágenes captadas en espacios públicos, la calidad de las mismas puede ser enormemente variada. Existe una correlación estrecha entre la calidad de las imágenes, dada por la infraestructura tecnológica, y la fiabilidad de los resultados. Esto puede significar más invasividad y menos cuidado por la privacidad en los espacios públicos. Por ejemplo, “en China, las fuerzas del orden tratan de evadir este problema instando intrusivas cámaras de alta definición con luces brillantes a la altura del rostro, y asociando los sistemas de reconocimiento facial a otras tecnologías que rastrean celulares en un área.”²⁷⁰ Y más allá de incentivar la hipervigilancia, en países con menos recursos esto puede traducirse en que los sistemas desplegados resultan inútiles porque utilizan cámaras anticuadas o en incentivos para invertir en infraestructura de vigilancia más moderna, justificados –de nuevo– sobre la base de solucionar tecnológicamente los problemas de seguridad. En este sentido, la desigualdad económica, que se manifiesta en la muy distinta calidad de los equipos, puede producir desigualdades en la justicia, castigando nuevamente a las regiones más empobrecidas.

²⁶⁹ E. Tendayi Achiume, «Informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia» (Naciones Unidas, 10 de noviembre de 2020), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/304/57/PDF/N2030457.pdf?OpenElement>.

²⁷⁰ «How the Police Use Facial Recognition, and Where It Falls Short - The New York Times», accedido 28 de julio de 2023, <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html>. <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html> «How the Police Use Facial Recognition, and Where It Falls Short - The New York Times». Traducción propia.



Ciclos de retroalimentación negativa

En nuestro imaginario moldeado por Hollywood y por el discurso de seguridad en medios y campañas políticas, la promesa de cómo el reconocimiento facial debe ayudar a atrapar criminales puede funcionar de dos maneras: en la primera, una cámara –instalada en el sistema de transporte masivo de una ciudad, en la entrada de un estadio o al frente de una patrulla de policía– capta la imagen de una persona cualquiera y un sistema automatizado contrasta dicha imagen contra una base de datos de personas contra las que pesa una orden de captura, como la de la INTERPOL, y encuentra una coincidencia que idealmente le permite a la policía concretar el arresto. En este caso el sistema está contribuyendo a ubicar criminales conocidos respondiendo a la pregunta ¿dónde está o por dónde se mueve esta persona? En la segunda, la imagen de una persona es captada mientras comete un delito y su rostro es contrastado contra una la base de datos de la población en general para así identificarlo y poder avanzar en la investigación y judicialización. En este caso el sistema está ayudando a identificar a presuntos criminales cuya identidad no se conoce respondiendo a la pregunta: ¿quién es esta persona? Ambas son formas de identificación a través de vigilancia masiva.

El despliegue de estos tipos de tecnología que menos resistencia despierta es la ubicación de criminales conocidos, pues no necesariamente implica la utilización de bases de datos de la población general. Sin embargo, esta utilización produce un sesgo de retroalimentación negativa que vale la pena revisar. Pensemos en la siguiente comparación: por un lado un criminal de quien únicamente se tiene la foto, por ejemplo, de la licencia de conducción, que puede ser una foto con años de antigüedad, tomada en condiciones regulares de iluminación y con poca resolución, y por otro, un criminal reincidente que pasó hace poco por el sistema penal –cualquier haya sido su infracción– y del que, por lo mismo, se tienen más fotos, más recientes y de mejor calidad. Si ambos están siendo activamente buscados por un sistema de reconocimiento facial ¿cuál será más probable identificar en el espacio público?

Por supuesto, la respuesta es que el criminal reincidente está más expuesto a ser identificado, pues la mayor información que se tiene sobre su rostro permitirá hallar una coincidencia con más facilidad. Esto implica que entre mayor haya sido la vigilancia y la ratificación previa de los sujetos antes de que surja la necesidad de identificarlos, más fácil será hacerlo. Por lo mismo, la implementación de estas tecnologías depende de robustecer sistemas de identidad digitalizados cada vez más invasivos, con la promesa abstracta de que conducirán a una sociedad más segura.²⁷¹

Ahora busquemos comprender las consecuencias de esto en un contexto concreto del presente: la utilización de biometría para el ingreso a estadios de fútbol en varios países de latinoamérica

²⁷¹ Casi a manera de anécdota risible, el informe de la Fundación Karisma titulado *Cámaras Indiscretas* (<https://web.karisma.org.co/camaras-indiscretas/>) documenta cómo el sistema de reconocimiento facial que se propuso implementar en el sistema integrado de transporte público de Bogotá fracasó por el hecho de que no había una base de datos robusta para contrastar las imágenes recogidas por las cámaras. Visto en retrospectiva es fácil comprender que esta haya sido una de las motivaciones de la RNEC para ampliar su base de datos e incorporar biometría en la cédula a partir de 2018.



incluidos Colombia²⁷², Brasil²⁷³, Argentina²⁷⁴ y México²⁷⁵, entre otros. Este contexto específico de utilización implica una vigilancia desproporcionada –fundada ya en datos históricos de comisión de delitos en escenarios deportivos, ya en (pre)juicios al respecto de su probabilidad de ocurrir– sobre una población particular. Si este experimento social de la implementación empieza a mostrar éxitos y conduce a la persecución penal de personas, tendrá la consecuencia de cimentar más el prejuicio que pesa sobre los hinchas, pues contribuirá a construir un sesgo de confirmación sobre la correlación que se presupone entre fanáticos del fútbol y criminales. Esto, a su vez, legitima la vigilancia exacerbada y sirve como argumento para la instalación de cámaras en la entrada de otros estadios o escenarios. Además de confirmar el sesgo negativo contra una población específica, esta práctica tiene el efecto paradójico de que todos los criminales que no son fanáticos de fútbol ni acuden al estadio resultan –por este hecho arbitrario– menos expuestos a ser capturados, mientras que los hinchas, aún los pacíficos, son vigilados con más rigor.

Similarmente, el sistema multibiométrico aplicado a personas que se acogen al estatuto temporal de migrantes venezolanos en Colombia²⁷⁶ los convierte en una población –en tanto que hipervigilada– más susceptible de ser identificada. Más adelante esto puede redundar en que la frecuencia de captura de personas venezolanas sea mayor, no por que su criminalidad sea mayor, sino simplemente porque es más fácil identificarlos y capturarlos. ¿En qué medida esto infringe el principio de igualdad ante la ley? Esto es análogo a lo que sucede con sistemas de predicción del delito:²⁷⁷ aunque datos históricos estadísticos muestren una desigualdad en la distribución geográfica del crimen, la hipervigilancia de los espacios más delictivamente densos conduce a agravar estas diferencias, pues al producir más arrestos refuerza la carga de datos de delitos en la zona y legitima su vigilancia creando un círculo de retroalimentación negativa. Adicionalmente espacios más libres de crimen tienen el privilegio de que su privacidad no se vea tan fuertemente vulnerada.

²⁷² El Colombiano, «Así opera la tecnología biométrica en seguridad de estadios y centros de espectáculos», www.elcolombiano.com, 12 de junio de 2023, <https://www.elcolombiano.com/colombia/asi-opera-la-tecnologia-biometrica-en-seguridad-de-estadios-y-centros-de-espectaculos-MG21721739>.

²⁷³ Casa Editorial El Tiempo, «Los estadios de Brasil tendrán reconocimiento facial en Copa América», futbolred.com, accedido 29 de julio de 2023, <https://www.futbolred.com/copa-america-brasil-2019/los-estadios-de-brasil-tendran-reconocimiento-facial-en-copa-america-2019-97841>.

²⁷⁴ Por Diego Schurman, «Seguridad en los estadios: el Gobierno activará un sistema de reconocimiento facial en la Superliga», [infobae](http://infobae.com), accedido 29 de julio de 2023, <https://www.infobae.com/deportes-2/2018/03/25/seguridad-en-los-estadios-el-gobierno-quiere-instalar-un-sistema-de-reconocimiento-facial-en-la-superliga/>.

²⁷⁵ WIRED, «Hinchas, familias y reconocimiento facial: ¿el Fan ID vulnera tus datos biométricos?», [WIRED](http://wired.com), 23 de julio de 2023, <https://es.wired.com/articulos/hinchas-familias-y-reconocimiento-facial-el-fan-id-vulnera-tus-datos-biometricos>.

²⁷⁶ «Biometría para entrar al país: el Estatuto Temporal de Protección a Migrantes Venezolanos», accedido 29 de julio de 2023, <https://digitalid.karisma.org.co/2021/07/01/sistema-multibiotrico-etpmv/>.

²⁷⁷ Jamie Grierson y Home affairs correspondent, «Predictive Policing Poses Discrimination Risk, Thinktank Warns», *The Guardian*, 15 de septiembre de 2019, sec. UK news, <https://www.theguardian.com/uk-news/2019/sep/16/predictive-policing-poses-discrimination-risk-think-tank-warns>; Griff Ferris, Bruno Min, y Misha Nayak-Oliver, «Automating injustice: The use of artificial intelligence & automated decision-making systems in criminal justice in Europe», 2021, https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf.



Sección tercera - El tecnopositivismo y la seguridad automática

En los lugares en que la violencia y la criminalidad son todavía un grave problema social por resolver, la tecnología con frecuencia se presenta como una solución cuasi-mágica. Los ejemplos en campañas electorales y propuestas de política pública de seguridad abundan en nuestro continente²⁷⁸, abarcando desde cámaras con tecnología de reconocimiento facial hasta drones, globos aerostáticos apodados “el ojo de Dios”, sistemas de georeferenciación de disparos, identificadores morfológicos que prometen individualizar a los criminales por su forma de caminar y “big data” para alimentar sistemas de inteligencia artificial capaces de anticiparse a los delitos.

Las promesas suelen ser vagas: hablan de “tecnología de punta”, se apoyan en gráficas espectaculares y hacen laxas asociaciones entre las herramientas y la reducción de tasas de criminalidad. En ellas parece persistir la idea de que un desarrollo técnico va a poder sustituir, casi por completo, el trabajo investigativo de los policías.²⁷⁹ Si para el policía victoriano bastaba con medir el rostro de una persona para saber si su comportamiento era criminal, a la policía contemporánea parece que le basta con instalar cámaras de reconocimiento facial para identificar a los criminales y proceder a aprehenderlos.²⁸⁰ En ambos casos, las causas profundas del delito, los contextos socio-culturales en que se produce y las propuestas estructurales que apuntan a sus raíces pasan a un segundo plano, pues la administración de justicia se presenta como una tarea que puede delegarse a las máquinas y solucionarse técnicamente.

Pero más allá de evaluar el realismo de estas ciber-utopías libres de crimen, quizá lo que resulta más interesante es pensar en tipo de sociedad o el modelo de justicia que subyace a la implementación de este tipo de tecnología. ¿Qué entrañan estas fantasías en que el complejo problema social de la seguridad está solucionado por máquinas? En esta sección del artículo discutiremos tres presuposiciones sin las cuales es imposible considerar al reconocimiento facial como una herramienta útil para la seguridad: 1) el paradigma punitivo, 2) el efecto inhibitorio y 3) la neutralidad de la tecnología.

²⁷⁸ «¿Qué es el Plan ÁNGEL? Marcelo Ebrard presenta plan de seguridad con reconocimiento facial», Marca México, 11 de julio de 2023, <https://www.marca.com/mx/actualidad/2023/07/11/64acb977ca4741270c8b45bb.html>; Jorge Alzate, «Con drones y globos aerostáticos: así es la propuesta de seguridad de Rodrigo Lara para Bogotá», infobae, accedido 30 de julio de 2023, <https://www.infobae.com/colombia/2023/07/18/con-drones-y-globos-aerostaticos-asi-es-la-propuesta-de-seguridad-de-rodrigo-lara-para-bogota/>; Robert Muggah y Pedro Augusto Pereira, «La riesgosa apuesta tecnológica de Brasil para combatir el crimen», InSight Crime (blog), 19 de febrero de 2020, <https://es.insightcrime.org/noticias/analisis/la-riesgosa-apuesta-tecnologica-de-brasil-para-combatir-el-crimen/>; Verónica Arroyo, «Cámaras Con Reconocimiento Facial En Lima», Access Now (blog), 15 de noviembre de 2019, <https://www.accessnow.org/camaras-con-reconocimiento-facial-en-lima/>; Revista Defensa InfoDefensa, «S2T de Chile presenta el software de reconocimiento facial de Oosto en la Conferencia Regional de Interpol», Infodefensa - Noticias de defensa, industria, seguridad, armamento, ejércitos y tecnología de la defensa, accedido 30 de julio de 2023, <https://www.infodefensa.com/texto-diario/mostrar/4230062/s2t-chile-presenta-software-reconocimiento-facial-oosto-conferencia-regional-interpol>.

²⁷⁹ Simon Egbert, «About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany», *European Journal for Security Research* 3, n.o 2 (1 de octubre de 2018): 95-114, <https://doi.org/10.1007/s41125-017-0027-3>.

²⁸⁰ Luke Stark y Jevan Hutson, «Physiognomic Artificial Intelligence», *SSRN Electronic Journal*, 2021, <https://doi.org/10.2139/ssrn.3927300>.



La seguridad como respuesta

Como hemos establecido, cuando en una ciudad se instalan cámaras de seguridad y se declara ante los medios que tendrán capacidades de reconocimiento facial, la promesa implícita es que será posible ubicar a los criminales identificados o será posible identificar a los criminales desconocidos. En ambos casos lo que se está proponiendo es actuar reaccionando tras el crimen. La tecnología de reconocimiento facial únicamente asiste a la justicia en su dimensión punitiva: promete que permitirá identificar al criminal para capturarlo, pero no puede asistir en la tarea de prevenir el delito.

Esto revela una visión de la justicia y la seguridad que otorga un lugar central al castigo y necesariamente pone en segundo lugar la prevención. Tanto en el imaginario social como en los presupuestos de seguridad, la tecnología como herramienta punitiva desplaza otras soluciones enfocadas en atender los problemas subyacentes y las causas de las conductas ilegales; desestima completamente las propuestas enfocadas en evitar las conductas delictivas. Así, para que el público considere pertinente esta solución, sus proponentes se enfocan en promover una visión –usualmente populista y acompañada de incrementos en las penas o mayor rigor en los juicios– según la cual el incremento en la vigilancia se traduce invariablemente en un incremento en la seguridad, lo que permite justificar la invasión a la privacidad y el gran gasto público que implica implementar estos sistemas.

Sin embargo, demostrar que la hipervigilancia disminuye el crimen no es sencillo. Un caso interesante es el de la ciudad de Medellín, donde hay un fuerte énfasis en el despliegue de tecnologías securitarias incluidas las cámaras de vigilancia.²⁸¹ Según una investigación del Instituto Edgelands, en esta ciudad el principal problema de seguridad se deriva del control territorial que grupos delincuenciales (los llamados “combos”) ejercen sobre ciertas zonas. A la par de los delitos más violentos, la extorsión y el narcotráfico son muy comunes. Sin embargo, las cámaras por sí solas son prácticamente obsoletas para hacer frente a estos delitos (pues una extorsión y el narcotráfico no son visibles en una grabación), pero además, según el reporte, “a medida que aumentan las intervenciones del Estado en los barrios donde viven y operan los combos, también aumenta la autoridad de éstos para mantener el control de su territorio.”²⁸² Lo anterior indica con claridad que la aproximación punitiva, además de no estar cumpliendo su objetivo de garantizar la seguridad y promover la justicia, puede incluso estar causando el efecto contrario. Este problema de seguridad,

²⁸¹ Según múltiples declaraciones públicas de oficiales de gobierno de la ciudad, las cámaras cuentan con capacidad de hacer reconocimiento facial, sin embargo, a pesar de nuestros mejores esfuerzos, ha sido imposible verificar estas aseveraciones. Como se verá más adelante, esta podría ser una estrategia para reforzar el efecto inhibitorio.

²⁸² Adriana Lasso-Harrier et al., «Medellín: Un reporte diagnóstico sobre seguridad, vigilancia digital y retos para el contrato social de la ciudad» (Instituto Edgelands, 2021), <https://es.edgelands.institute/reports/medellin-report>.



como muchos otros en la región, es claramente estructural y demanda una solución que excede por mucho a la tecnología. La ilusión de control a través de la hipervigilancia que está a la base de estas narrativas securitarias es poco más que eso: una ilusión.²⁸³

Finalmente, otra promesa propia de este enfoque punitivo es la posibilidad de aumentar la eficiencia de la policía reduciendo su tiempo de reacción a casi cero: si la tecnología de reconocimiento facial consigue que una cámara, en tiempo real, identifique a un sospechoso contra quien pesa una orden de captura, podría funcionar como un mecanismo de atención urgente que permita la intervención inmediata de la policía. Aquí la cámara operaría como una suerte de llamado automático de auxilio. Sin embargo, además de que este uso implica un monitoreo masivo persistente (automatizado o no) del espacio público -que por sí mismo es considerado un ejercicio violatorio de derechos por cuanto es una forma de vigilancia masiva-, actuar sobre ese improbable resultado algorítmico solo es posible si de antemano hay una fuerza pública capaz de llevar a cabo el despliegue. En ese sentido es claro que lo prioritario es trabajar en los tiempos de reacción de las unidades de policía a la par que en el despliegue tecnológico. Y eso no anula la posibilidad, evaluada en la sección anterior, de que haya un error de FP y una violación de la presunción de inocencia. En este caso, como otros abordados más atrás, tomar acciones con base en el resultado de un proceso automatizado implica vulnerar las garantías judiciales que se supone cobijan al sospechoso.

Te estamos observando: el efecto inhibitorio

Si bien es claro que la concepción de justicia que acompaña al reconocimiento facial es sobre todo punitiva, existe una aproximación que podría considerarse “preventiva” o, cuanto menos, disuasoria. Se trata de el efecto inhibitorio [chilling effect], que hace que al sabernos vigilados actuemos distinto de como lo haríamos sin vigilancia. Esta expresión, que surgió alrededor de 1960 en Estados Unidos, en el contexto jurídico de la libertad de expresión²⁸⁴, se refiere al “impacto que la vigilancia de la audiencia [en este caso la policía, o quien quiera que esté “al otro lado” de la cámara] tiene en la restricción del comportamiento”.²⁸⁵ En un sentido, esto es sólo una extensión del principio punitivo, pues la motivación que modifica el comportamiento es el temor al castigo o la represalia en el delincuente potencial.

²⁸³ Un ejemplo irónico y triste del alcance de esta ilusión del control a través de la tecnología quedó ilustrado en un incidente ocurrido en Bogotá durante la campaña a la alcaldía: en el mes de junio de 2023 un violento atraco tuvo lugar en una avenida principal de la ciudad y todo el robo, que duró varios minutos y dejó a un taxista herido de muerte, fue captado por una cámara de seguridad en un poste de luz a pocos metros de allí. Al día siguiente un candidato a la alcaldía publicó el video en twitter agregando: “Eso no pasará en mi Alcaldía. Con drones, responderemos en forma inmediata.” Es difícil saber qué imaginaba el candidato. Si todo el incidente fue grabado y la policía no acudió ¿qué ventaja podría suponer tener drones de policía en esa situación?

²⁸⁴ Frederick Schauer, «Fear, Risk and the First Amendment: Unraveling the Chilling Effect», *BOSTON UNIVERSITY LAW REVIEW* 58 (s. f.).

²⁸⁵ Moritz Büchi et al., «Chilling Effects of Profiling Activities: Mapping the Issues», *SSRN Electronic Journal*, 2019, <https://doi.org/10.2139/ssrn.3379275>.



En primer lugar, al considerar la efectividad del efecto inhibitorio habría que partir del hecho de que, si se lo valora como mecanismo de prevención del delito, lo verdaderamente disuasor sería la pena efectiva, es decir, la aplicación real de la justicia. No hay efecto inhibitorio si el delincuente potencial sabe que, aunque identificada, la conducta no será castigada. Si el reconocimiento facial es únicamente una herramienta –técnicamente insuficiente– de un sistema inoperante, no conseguirá disuadir al criminal en potencia. En ese sentido, el despliegue de herramientas tecnológicas para combatir el crimen debe ir siempre acompañado de garantías de acceso y eficiencia de la justicia, y de una preocupación por reducir de las tasas de impunidad, que en nuestra región está más vinculada con la ineficacia del sistema judicial que con las falencias técnicas de la policía.²⁸⁶ Lo anterior nuevamente nos obliga a cuestionar el lugar de la tecnología dentro de la política pública securitaria, pues más allá de cuál sea nuestra postura al respecto de la legitimidad del efecto inhibitorio y del miedo como mecanismos de prevención, sin un sistema judicial efectivo es imposible pensar que la tecnología como herramienta del sistema punitivo sea un disuasor eficiente.

Sin embargo, hay con respecto al efecto inhibitorio una consideración más profunda que merece atención. La literatura muestra que al saberse vigilada una persona no sólo inhibe su conducta ilegal, sino que “los efectos inhibitorios también son productivos. No sólo conducen al silenciamiento de discursos, sino también a la expresión de discursos y conductas socialmente conformes.”²⁸⁷ En este sentido no basta preguntarse con qué dejamos de hacer cuando se está bajo vigilancia de una cámara capaz de identificar nuestro rostro, sino qué también hay que reflexionar sobre el tipo de conducta positiva que se asume. Cuando nuestra conducta cambia por este motivo, el Estado ya no está regulando nuestro hacer desde la restricción legal sino desde el encauzamiento moral dado por lo socialmente permitido o sancionado, de manera que efectivamente limita nuestras libertades más allá de las prohibiciones legales.

Un ejemplo muy explícito de este tipo de encauzamiento de la conducta se da, en China, a través de la humillación pública: cuando el sistema de reconocimiento facial identifica a una persona cometiendo una infracción de tránsito como, por ejemplo, cruzar una calle por donde no hay paso peatonal, proyecta su rostro en pantallas LED gigantes. En un famoso caso de 2018, el rostro de la presidenta de una gran compañía de aires acondicionados fue proyectado en una pantalla; el problema es que ella nunca cruzó la calle fuera de la cebsa, su rostro había sido tomado de una publicidad en el costado del bus y el sistema asumió que era un peatón que no seguía las reglas.²⁸⁸

²⁸⁶ «¿Cómo combatir la impunidad? La modernización del sistema de justicia criminal en América Latina», *Seguridad Ciudadana* (blog), 19 de noviembre de 2019, <https://blogs.iadb.org/seguridad-ciudadana/es/como-combatir-la-impunidad-la-modernizacion-del-sistema-de-justicia-criminal-en-america-latina/>.

²⁸⁷ Jon Penney, «Understanding Chilling Effects», *SSRN Scholarly Paper* (Rochester, NY, 28 de mayo de 2021), <https://doi.org/10.2139/ssrn.3855619>.

²⁸⁸ Billie Thomson, «China's facial-recognition cameras put jaywalkers' faces on billboards», *Mail Online*, 8 de noviembre de 2019, <https://www.dailymail.co.uk/news/article-7664797/Chinas-facial-recognition-punishes-jaywalkers-putting-pictures-big-screens.html>; «Facial Recognition Flags Woman on Bus Ad for “Jaywalking” in China», *Gizmodo*, 26 de noviembre de 2018, <https://gizmodo.com/facial-recognition-flags-woman-on-bus-ad-for-jaywalking-1830654750>. Alto Comisionado de las Naciones Unidas para los Derechos Humanos, «Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas», Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (Naciones Unidas, 24 de junio de 2020), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/38/PDF/G2015438.pdf?OpenElement>.



El efecto inhibitorio afecta el derecho de las personas a reunirse, manifestarse y expresarse pues temen que pueden ser identificados, estigmatizados, perseguidos e incriminados. El Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha alertado sobre este efecto al indicar que “el uso de la tecnología de reconocimiento facial para identificar a las personas en el contexto de las manifestaciones tiene efectos adversos considerables sobre los derechos a la privacidad, la libertad de expresión y la reunión pacífica”²⁸⁹

Vale la pena entonces hacernos unas preguntas frente a la vigilancia con reconocimiento facial: ¿Qué tipo de conductas resultan socialmente desincentivadas? ¿Qué tipo de conductas, más allá de las conductas ilegales, interesa al Estado desincentivar? Un elemento que puede ser interesante para avanzar hacia sus respuestas es el hecho de que, con frecuencia, se publicitan herramientas de reconocimiento facial en medios de comunicación antes de que la tecnología haya sido de hecho instalada,²⁹⁰ tratando de conseguir el efecto social inhibitorio sin un sistema que lo secunde.

Tal como en el ejemplo de la línea de identificación policial, servirse del efecto inhibitorio implica tratar a todas las personas que ocupan el espacio público como potenciales sospechosos y considerar que sus rostros deben ser escrutados. No sólo somos criminales potenciales ante el Estado, que –si emplea reconocimiento facial masivo– verifica constantemente este estatus, sino que estamos rodeados de potenciales criminales también. El despliegue de esta tecnología nos empuja hacia un espacio social en que el Estado ha declarado a todos como sujetos potencialmente peligrosos; así como las cámaras son un recuerdo persistente de que cada uno de nosotros debe comportarse dentro de los límites morales, cada uno de nuestros conciudadanos es una amenaza potencial.

La utopía de la tecnología infalible

El último punto de esta exploración de la automatización de la seguridad y la justicia que nos proponemos explorar es la asunción de que la tecnología es neutra y la promesa de que, a pesar de sus imperfecciones, el advenimiento de máquinas perfectas es sólo cuestión de tiempo.

La idea de que la tecnología, en tanto que libre de emociones, sesgos y prejuicios humanos, es neutra en sus consecuencias está muy difundida. Sin embargo, las posiciones que cuestionan esta neutralidad son también cada vez más frecuentes: de manera casi simultánea con la escalada de popularidad de ChatGPT, por ejemplo, las personas usuarias empezaron a develar sus límites mostrando cómo el modelo de lenguaje reproducía estereotipos y sesgos presentes en los datos con que fue entrenado.²⁹¹ Este sano escepticismo choca con la visión acrítica que parece dominar

²⁹⁰ Esta es una tendencia que hemos notado desde hace varios años: los medios de comunicación anuncian la instalación de cámaras de reconocimiento facial y, al ser indagadas de manera específica, las entidades reconocen que no tienen (aún, al menos) estas capacidades.

²⁹¹ «ChatGPT and Large Language Model Bias - CBS News», 5 de marzo de 2023, <https://www.cbsnews.com/news/chatgpt-large-language-model-bias-60-minutes-2023-03-05/>; Zachary B. Wolf, «AI Can Be Racist, Sexist and Creepy. What Should We Do about It? | CNN Politics», CNN, 18 de marzo de 2023, <https://www.cnn.com/2023/03/18/politics/ai-chatgpt-racist-what-matters/index.html>.



una buena parte de las aplicaciones de seguridad. En el reconocimiento facial, como en otras tecnologías, el sesgo no sólo está dado por las características de las bases de datos con que se entrena, sino sobre todo por el uso que hacemos de esta herramienta.

Por supuesto, la idea de la neutralidad de la tecnología no es espontánea, es lo que permite desplazar la responsabilidad de las decisiones difíciles hacia las máquinas. Tal como Lombroso se ocultaba detrás de rigurosas mediciones del cráneo y la cara para demostrar su ‘superioridad racial’ y justificar las más racistas políticas judiciales, el complejo andamiaje técnico y la automaticidad del reconocimiento facial sirven como criterios ‘objetivos’ a los que señalar en el momento de tomar decisiones que pueden cambiar las vidas de las personas. En este proceso, el reconocimiento facial permite decir: “aquí hay un culpable” con el respaldo de la infalibilidad científica y técnica, desplazando así la responsabilidad de quien señala y adjudicándosela a la máquina.

Sin embargo, la explicabilidad de esa decisión es secundaria. A las máquinas que se perciben neutrales y justas, ¿quién puede cuestionarlas? Confiar en esta tecnología implica invertir la carga de la prueba, exigiendo demostrar la inocencia, como en el caso de Williams, para quien fue necesario probar que, aunque la máquina lo dijera, no se trataba de él. Esta carga, en la medida en que confiemos más en los veredictos de estos sistemas, recaerá con más fuerza sobre los sospechosos, para quienes revertir este juicio puede ser un ejercicio humillante, costoso y agotador.

A estos reclamos, los desarrolladores de tecnología con frecuencia responden mostrando los grandes avances tecnológicos que se han conseguido en los últimos años y prometiendo que la tecnología mejora día a día, ofreciendo la ilusión de que en el futuro será infalible. Sin embargo, el hecho de que esta herramienta tiene límites técnicos y sociales es claro. No se trata aspirar al estándar imposible de tener sistemas de reconocimiento facial técnicamente perfectos –el problema de la antropología criminal nunca fue no tener mediciones suficientemente precisas del rostro– sino de asegurarnos de que sus capacidades y sus instancias de uso se alinean con nuestros intereses sociales y nuestra visión de la justicia como bien público. Insistir en el uso de esta tecnología para fines de seguridad consigue poco más que reforzar una concepción de la seguridad y la justicia como un juego de suma cero, en que la privacidad tiene que ser ofrecida como tributo. Pero ¿es esa una visión de la seguridad que nos interese promover?

Mientras el despliegue de sistemas de reconocimiento facial ocurre, no se desarrollan en paralelo marcos regulatorios que garanticen los derechos de las personas, evitando perfilamientos, mal uso y discriminación. Por todo esto las Naciones Unidas²⁹² y organizaciones de la sociedad civil alrededor del mundo²⁹³ han solicitado una moratoria de estas tecnologías para reflexionar y desarrollar la

²⁹² «UN Expert Calls for Immediate Moratorium on the Sale, Transfer and Use of Surveillance Tools», OHCHR, accedido 9 de agosto de 2023, <https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance>; Sammy Westfall, «U.N. Official Calls for Moratorium on Artificial Intelligence Tools That Breach Human Rights», Washington Post, 17 de septiembre de 2021, <https://www.washingtonpost.com/world/2021/09/15/un-ai-moratorium/>. <https://www.washingtonpost.com/world/2021/09/15/un-ai-moratorium/> «UN Expert Calls for Immediate Moratorium on the Sale, Transfer and Use of Surveillance Tools»; Westfall, «U.N. Official Calls for Moratorium on Artificial Intelligence Tools That Breach Human Rights».

²⁹³ «La tecnología biométrica en espacios públicos permite la vigilancia discriminatoria Fundación Karisma», accedido 9 de agosto de 2023, <https://web.karisma.org.co/la-tecnologia-biometrica-en-espacios-publicos-permite-la-vigilancia-discriminatoria/>.



reglamentación necesaria que permita aplicar los estándares de derechos humanos de legalidad, necesidad y proporcionalidad, de modo que se puedan aprovechar los efectos positivos sin comprometer nuestros derechos.

Conclusiones y recomendaciones

Estamos todavía lejos, como sociedad, de tener un consenso claro al respecto del uso de las tecnologías de reconocimiento facial con fines securitarios. Por lo mismo, su legitimidad sigue en disputa y su adecuada regulación sigue pendiente en las sociedades democráticas. Para establecer garantías adecuadas al respecto del uso de tecnologías de reconocimiento facial es necesario empezar por cuestionar qué problemas resuelven y qué necesidades sociales atienden, es decir, debe incluir un análisis de necesidad. El sentido de su implementación debe estar siempre dictado por la relevancia de la herramienta en el contexto específico de su uso y, sobre todo, por sus posibles impactos en materia de derechos y garantías, es decir, debe incluir un análisis de proporcionalidad y de legalidad. Además de lo anterior debe llevarse a cabo también un análisis previo de riesgos que cubra al menos los derechos a: la intimidad, la no discriminación, la libertad de expresión, la libre asociación, la reunión pacífica, la igualdad ante la ley, la presunción de inocencia y el debido proceso.²⁹⁴

Siempre que sea posible optar por tecnologías menos invasivas y menos propensas al abuso – como el reconocimiento palmar o de iris, antes que reconocimiento facial– debe hacerse. Sin embargo, cuando las tecnologías se implementan en contextos de uso público o mediante datos administrados por el Estado es necesario que esto ocurra de manera transparente y que sea posible auditarlas técnicamente antes, durante y después de su uso y de manera recurrente, aún cuando tocan temas de seguridad nacional. Vale decir que estas garantías son necesarias, pero tienen un alcance limitado, pues no necesariamente toda la información puede hacerse pública, sólo son relevantes en la medida en que los contextos, las prácticas y los estándares de uso de la tecnología son públicos y verificables también. Como mínimo deberían ser de conocimiento público los estándares, las certificaciones y las tasas de confiabilidad de la tecnología implementada.

Por último, los sistemas de identidad subyacentes que permiten realizar reconocimiento facial deben, a su vez, cumplir con una serie de principios básicos. Desde Karisma proponemos seis fundamentales: 1) inclusión, los Estados tienen la obligación de promover condiciones para el acceso igualitario e inclusivo a la identidad legal para todas las personas; 2) no discriminación, los sistemas deben tratar a todas las personas en condiciones de igualdad y sin discriminación por razón de su origen o nacionalidad; 3) seguridad digital, los sistemas de identidad deben proteger los datos de las personas de injerencias ilegítimas; 4) privacidad, los sistemas de identidad deben estar diseñados con un enfoque de privacidad por diseño; 5) sostenibilidad, los sistemas de identidad deben ser sostenibles financiera y operacionalmente; y 6) Estado de derecho, los sistemas

²⁹⁴ Naciones Unidas, «La Declaración Universal de los Derechos Humanos | Naciones Unidas», United Nations (United Nations), accedido 11 de agosto de 2023, <https://www.un.org/es/about-us/universal-declaration-of-human-rights>.



de identidad deben estar estructurados integralmente en los marcos regulatorios con responsabilidades y procedimientos claramente definidos.²⁹⁵

Finalmente ofrecemos una serie de recomendaciones concretas para antes, durante y después de la implementación de sistemas de reconocimiento facial en contextos securitarios:

Sistemas de identidad con datos biométricos faciales y su uso para identificación:

Siempre que el Estado recoja datos biométricos faciales es indispensable que exista un marco normativo que lo permita y estipule claramente los usos posibles. Se debe excluir la vigilancia masiva. Deben existir estándares claros para definir la validez de estas herramientas en los contextos de individualización e identificación, siempre mediada por autorización judicial.

Es indispensable que cuando el Estado recoge datos biométricos faciales justifique la captación de estos datos más allá de la mera necesidad de identificación individual para el ejercicio de la identidad legal y, en cada caso, justifique por qué razón se sirve específicamente de datos biométricos faciales por oposición a otras formas de biometría.

Los sistemas cuyas bases de datos no estén centralizadas son, por regla general, preferibles. Esto disminuye su vulnerabilidad ante ciberataques y reduce el interés por abusar de ellos así como el daño potencial. Esto es especialmente relevante cuando se trata de datos biométricos, en la medida en que estos son especialmente sensibles.

Los sistemas de identidad centralizados no deben incluir información biométrica que permita la *identificación*, pues es imposible garantizar que no serán abusados. En dichos sistemas basta con que permitan la *verificación* de identidad.

La probabilidad de que los sistemas arrojen FP aumenta en la medida en que aumenta el tamaño de las bases de datos. Por lo mismo, no es deseable tener grandes bases de datos centralizadas. Por el contrario, la especificidad de las bases de datos contribuye a que la justicia pueda operar de manera más eficiente y certera.

En los contextos en que es posible utilizar identificación facial debe establecerse la obligación legal de informar a las personas cuando han sido identificadas. Siempre deben entregarse los datos del caso a la persona identificada (lugar, hora, fecha, motivo, la imagen contrastada junto con la explicación de su procedencia, etc.) y los detalles técnicos (tasa de confiabilidad del resultado, etc.).

²⁹⁵ «Principios para un sistema de identidad que proteja los derechos humanos», accedido 11 de agosto de 2023, <https://digitalid.karisma.org.co/2021/12/07/principios-id/>.



Verificación de identidad con reconocimiento facial:

Para fines de verificación de la identidad con sistemas de reconocimiento facial, es deseable separar la imagen que permitió construir la plantilla. Las imágenes deben estar más y mejor protegidas, en la medida en que cargan toda la información implícita, mientras que en la plantilla esta información no es legible a simple vista.

Aquellos sistemas de verificación en que el titular lleva consigo su propia plantilla biométrica en un dispositivo intransferible (por ejemplo, un token o una memoria USB) y esta únicamente se utiliza como un segundo factor, sin necesidad de contrastarla contra una base centralizada, son los que mejores estándares tienen. Aún en este caso, es preferible que el dato biométrico utilizado no sea facial.

Si bien hay que aceptar que la anonimización nunca es irreversible, es deseable garantizar estándares de anonimización y encriptación para las plantillas en todos los contextos en que esto sea posible, es decir, en las instancias de verificación de identidad. La función de desanonimización debe ser posible para verificar posibles fallos de la tecnología, pero debe estar adecuadamente regulada y limitada, y debe ser trazable.

El borrado de las imágenes que se utilizan para construir las plantillas no es deseable como principio general, pues estas permiten hacer una verificación humana siempre que se sospeche un FP. Esta debe hacerse de manera regulada, limitada y trazable.

Especificaciones técnicas y auditabilidad:

Las especificaciones técnicas de los algoritmos de reconocimiento facial son importantes y deben ser públicas y auditables, pero sólo pueden leerse en conjunto con las instancias reales de uso de la tecnología. Por esta razón su publicación debe ir acompañada de principios de transparencia general sobre los sistemas y sus usos. Es decir, la tecnología debe ser auditable en términos técnicos, pero también en términos de su utilización.

Como mínimo debe haber estándares públicos que permitan construir confianza sobre los sistemas, revelando, por ejemplo, su tasa de confiabilidad, sus capacidades, sus instancias de uso, las actualizaciones, las versiones, las fallas previas, las vulnerabilidades resueltas, etc. Así mismo debe haber estándares de transparencia al rededor de los procesos de contratación de las tecnologías. Entre otras cosas, dichos estándares deben garantizar la posibilidad de que múltiples oferentes compitan para proveer los servicios.





BIBLIOGRAFÍA

Alto Comisionado de las Naciones Unidas para los Derechos Humanos. «Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas». Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Naciones Unidas, 24 de junio de 2020. [https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/38/PDF/G2015438.pdf](https://documents-dds-ny.un.org/doc/UNDOC/GEN/G20/154/38/PDF/G2015438.pdf?OpenElement) OpenElement.

Alzate, Jorge. «Con drones y globos aerostáticos: así es la propuesta de seguridad de Rodrigo Lara para Bogotá». infobae. Accedido 30 de julio de 2023. <https://www.infobae.com/colombia/2023/07/18/con-drones-y-globos-aerostaticos-asi-es-la-propuesta-de-seguridad-de-rodrigo-lara-para-bogota/>.

Ariel, Barak. «Police Body Cameras in Large Police Departments». The Journal of Criminal Law and Criminology (1973-) 106, n.o 4 (2016): 729-68.

Arroyo, Verónica. «Cámaras Con Reconocimiento Facial En Lima». Access Now (blog), 15 de noviembre de 2019. <https://www.accessnow.org/camaras-con-reconocimiento-facial-en-lima/>.

Balko, Radley. «There's Overwhelming Evidence That the Criminal Justice System Is Racist. Here's the Proof.» Washington Post. Accedido 31 de julio de 2023. <https://www.washingtonpost.com/graphics/2020/opinions/systemic-racism-police-evidence-criminal-justice-system/>.

Bhuiyan, Johana. «First Man Wrongfully Arrested Because of Facial Recognition Testifies as California Weighs New Bills». The Guardian, 27 de abril de 2023, sec. US news. <https://www.theguardian.com/us-news/2023/apr/27/california-police-facial-recognition-software>.

«Biometría para entrar al país: el Estatuto Temporal de Protección a Migrantes Venezolanos». Accedido 29 de julio de 2023. <https://digitalid.karisma.org.co/2021/07/01/sistema-multibiometria-co-etpmv/>.

Büchi, Moritz, Eduard Fosch Villaronga, Christoph Lutz, Aurelia Tamò-Larrieux, Shruthi Velidi, y Salome Viljoen. «Chilling Effects of Profiling Activities: Mapping the Issues». SSRN Electronic Journal, 2019. <https://doi.org/10.2139/ssrn.3379275>.

«Calais migrants mutilate fingertips to hide true identity | Daily Mail Online». Accedido 26 de julio de 2023. <https://www.dailymail.co.uk/news/article-1201126/Calais-migrants-mutilate-fingertips-hide-true-identity.html>.



«ChatGPT and Large Language Model Bias - CBS News», 5 de marzo de 2023. <https://www.cbsnews.com/news/chatgpt-large-language-model-bias-60-minutes-2023-03-05/>.

Cléménçon, Stephan, y Winston Maxwell. «Why Facial Recognition Algorithms Can't Be Perfectly Fair». The Conversation, 20 de julio de 2020. <http://theconversation.com/why-facial-recognition-algorithms-cant-be-perfectly-fair-142608>.

Colombiano, El. «Así opera la tecnología biométrica en seguridad de estadios y centros de espectáculos». www.elcolombiano.com, 12 de junio de 2023. <https://www.elcolombiano.com/colombia/asi-opera-la-tecnologia-biometrica-en-seguridad-de-estadios-y-centros-de-espectaculos-MG21721739>.

Corte Constitucional de Colombia. Sentencia SU420-19. Accedido 26 de julio de 2023. <https://www.corteconstitucional.gov.co/relatoria/2019/SU420-19.htm>.

«Cuando el estado vigila. Ciberpatrullaje y OSINT en Colombia: Fundación Karisma». Accedido 26 de julio de 2023. <https://web.karisma.org.co/cuando-el-estado-vigila-ciberpatrullaje-y-osint-en-colombia/>.

Desilver, Drew, Michael Lipka, y Dalia Fahmy. «10 Things We Know about Race and Policing in the U.S.» Pew Research Center (blog). Accedido 31 de julio de 2023. <https://www.pewresearch.org/short-reads/2020/06/03/10-things-we-know-about-race-and-policing-in-the-u-s/>.

«Deviance, disorder and the self: Criminality». Accedido 18 de julio de 2023. <http://www7.bbk.ac.uk/deviance/criminality/french/36-20%20larcassagne%20ears%20page1.htm>.

Egbert, Simon. «About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany». European Journal for Security Research 3, n.o 2 (1 de octubre de 2018): 95-114. <https://doi.org/10.1007/s41125-017-0027-3>.

«El sistema de identidad administrado por la Registraduría Nacional del Estado Civil». Accedido 31 de julio de 2023. <https://digitalid.karisma.org.co/2022/11/27/el-sistema-de-identidad-administrado-por-la-Registraduri-a-Nacional-del-Estado-Civil/>.

Ferris, Griff, Bruno Min, y Misha Nayak-Oliver. «Automating injustice: The use of artificial intelligence & automated decision-making systems in criminal justice in Europe», 2021. https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf.

Frankle, Clare Garvie, Jonathan. «Facial-Recognition Software Might Have a Racial Bias Problem». The Atlantic, 7 de abril de 2016. <https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/>.

Fussell, Sidney. «A Flawed Facial-Recognition System Sent This Man to Jail». Wired. Accedido 29 de julio de 2023. <https://www.wired.com/story/flawed-facial-recognition-system-sent-man-jail/>.

Gates, Kelly. Our biometric future: facial recognition technology and the culture of surveillance. Critical cultural communication. New York: New York University Press, 2011.

Gizmodo. «Facial Recognition Flags Woman on Bus Ad for “Jaywalking” in China», 26 de noviembre de 2018. <https://gizmodo.com/facial-recognition-flags-woman-on-bus-ad-for-jaywalking-1830654750>.

Glen, Stephanie. «Sunglasses and Face Mask Won’t Fool Facial Recognition Systems Any More - DataScienceCentral.Com». Data Science Central, 11 de octubre de 2021. <https://www.datasciencecentral.com/sunglasses-and-face-mask-wont-fool-facial-recognition/>.

Grierson, Jamie y Home affairs correspondent. «Predictive Policing Poses Discrimination Risk, Thinktank Warns». The Guardian, 15 de septiembre de 2019, sec. UK news. <https://www.theguardian.com/uk-news/2019/sep/16/predictive-policing-poses-discrimination-risk-thinktank-warns>.

Grother, Patrick, Mei Ngan, y Kayee Hanaoka. «Face Recognition Vendor Test (FRVT) Part 2:: Identification». Gaithersburg, MD: National Institute of Standards and Technology, septiembre de 2019. <https://doi.org/10.6028/NIST.IR.8271>.

—. «Face Recognition Vendor Test Part 3: Demographic Effects». Gaithersburg, MD: National Institute of Standards and Technology, diciembre de 2019. <https://doi.org/10.6028/NIST.IR.8280>.

Hering Torres, Max-Sebastián. 1892: un año insignificante: orden policial y desorden social en la Bogotá de fin de siglo. Bogotá: Crítica: Universidad Nacional de Colombia, 2018.

«How the Police Use Facial Recognition, and Where It Falls Short - The New York Times». Accedido 28 de julio de 2023. <https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html>.

InfoDefensa, Revista Defensa. «S2T de Chile presenta el software de reconocimiento facial de Oos- to en la Conferencia Regional de Interpol». Infodefensa - Noticias de defensa, industria, seguridad, armamento, ejércitos y tecnología de la defensa. Accedido 30 de julio de 2023. <https://www.infodefensa.com/texto-diario/mostrar/4230062/s2t-chile-presenta-software-reconocimiento-facial-oos-to-conferencia-regional-interpol>.

INTERPOL. «Our 19 Databases». Accedido 31 de julio de 2023. <https://www.interpol.int/How-we-work/Databases/Our-19-databases>.

«INTERPOL - Facial Recognition». Accedido 27 de julio de 2023. <https://www.interpol.int/How-we-work/Forensics/Facial-Recognition>.

«ISO/IEC 2382-37:2022 Information technology – Vocabulary – Part 37: Biometrics», 2022. <https://www.iso.org/standard/73514.html>.

Kaur, Paramjit, Kewal Krishan, Suresh K. Sharma, y Tanuj Kanchan. «Facial-Recognition Algorithms: A Literature Review». *Medicine, Science and the Law* 60, n.o 2 (abril de 2020): 131-39. <https://doi.org/10.1177/0025802419893168>.

«La tecnología biométrica en espacios públicos permite la vigilancia discriminatoria: Fundación Karisma». Accedido 9 de agosto de 2023. <https://web.karisma.org.co/la-tecnologia-biometrica-en-espacios-publicos-permite-la-vigilancia-discriminatoria/>.

«Las mujeres son más seguras al volante que los hombres | Motor». Accedido 29 de julio de 2023. <https://www.elmundo.es/motor/2022/03/08/62267f3dfdddf8b8e8b45ce.html>.

Lasso-Harrier, Adriana, Beatriz Botero Arcila, Laura García Vargas, y Santiago Uribe-Sáenz. «Medellín: Un reporte diagnóstico sobre seguridad, vigilancia digital y retos para el contrato social de la ciudad». Instituto Edgelands, 2021. <https://es.edgelands.institute/reports/medellin-report>.

Leslie, David. «Understanding bias in facial recognition technologies». Zenodo, 26 de septiembre de 2020. <https://doi.org/10.5281/ZENODO.4050457>.

Lewis, Sarah. «The Racial Bias Built Into Photography». *The New York Times*, 25 de abril de 2019, sec. Lens. <https://www.nytimes.com/2019/04/25/lens/sarah-lewis-racial-bias-photography.html>.

Ley 1581 de 2012 - Por la cual se dictan disposiciones generales para la protección de datos personales. Accedido 25 de julio de 2023. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>.

Lombroso, Cesar. English: Picture of criminals, according to Lombroso. Dates back to ca. 1880. Author: Cesar Lombroso (died in 1909). Français : L'homme criminel. Étude anthropologique et psychiatrique. Traduit sur la quatrième édition italienne par MM. Régnier et Bournet et précédé d'une préface du Dr Ch. Létourneau. Paris: Ancienne Librairie Germer Baillière et Cie, Félix Alcan, Éditeur, 1887. Cesar Lombroso. Accedido 18 de julio de 2023. https://commons.wikimedia.org/wiki/File:Lombroso_1.jpg#/media/File:Lombroso_1.jpg.

Lombroso, Cesare, Mary Gibson, y Nicole Hahn Rafter. *Criminal Man*. Durham, NC: Duke University Press, 2006.

Marca México. «¿Qué es el Plan ÁNGEL? Marcelo Ebrard presenta plan de seguridad con reconocimiento facial», 11 de julio de 2023. <https://www.marca.com/mx/actualidad/2023/07/11/64acb-977ca4741270c8b45bb.html>.

Muggah, Robert, y Pedro Augusto Pereira. «La riesgosa apuesta tecnológica de Brasil para combatir

el crimen». InSight Crime (blog), 19 de febrero de 2020. <https://es.insightcrime.org/noticias/analisis/la-riesgosa-apuesta-tecnologica-de-brasil-para-combatir-el-crimen/>.

Naciones Unidas. «La Declaración Universal de los Derechos Humanos | Naciones Unidas». United Nations. United Nations. Accedido 11 de agosto de 2023. <https://www.un.org/es/about-us/universal-declaration-of-human-rights>.

NBC News. «Drug Lord Who Changed His Face Testifies against “El Chapo”», 30 de noviembre de 2018. <https://www.nbcnews.com/news/us-news/el-chapo-trial-drug-lord-who-changed-his-face-testifies-n942116>.

Negret Mosquera, Carlos Alfonso. «Informe Final Para el esclarecimiento de los hechos ocurridos los días 9 y 10 de septiembre de 2020». Colectivo de abogados José Alvear Restrepo CAJAR, 2021. <https://www.colectivodeabogados.org/wp-content/uploads/2021/12/Informe-Final-Relatori%C3%81a-Esclarecimiento-9S-VF.pdf>.

Ngan, Mei, Patrick Grother, y Kayee Hanaoka. «Ongoing Face Recognition Vendor Test (FRVT) Part 6A:: Face Recognition Accuracy with Masks Using Pre-COVID-19 Algorithms». Gaithersburg, MD: National Institute of Standards and Technology, julio de 2020. <https://doi.org/10.6028/NIST.IR.8311>.

OHCHR. «UN Expert Calls for Immediate Moratorium on the Sale, Transfer and Use of Surveillance Tools». Accedido 9 de agosto de 2023. <https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance>.

Penney, Jon. «Understanding Chilling Effects». SSRN Scholarly Paper. Rochester, NY, 28 de mayo de 2021. <https://doi.org/10.2139/ssrn.3855619>.

Perkowitz, Sidney. «The Bias in the Machine: Facial Recognition Technology and Racial Disparities». MIT Case Studies in Social and Ethical Responsibilities of Computing, n.o Winter 2021 (5 de febrero de 2021). <https://doi.org/10.21428/2c646de5.62272586>.

Petrescu, Rely Victoria. «Face Recognition as a Biometric Application». SSRN Electronic Journal, 2019. <https://doi.org/10.2139/ssrn.3417325>.

«Principios para un sistema de identidad que proteja los derechos humanos». Accedido 11 de agosto de 2023. <https://digitalid.karisma.org.co/2021/12/07/principios-id/>.

Rathgeb, Christian, Didem Dogan, Fabian Stockhardt, Maria De Marsico, y Christoph Busch. «Plastic Surgery: An Obstacle for Deep Face Recognition?» En 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 3510-17. Seattle, WA, USA: IEEE, 2020. <https://doi.org/10.1109/CVPRW50498.2020.00411>.

Redacción Justicia. «Las cirugías con las que “narcos” han buscado evadir su captura». El Tiempo,

19 de noviembre de 2020, sec. justicia. <https://www.eltiempo.com/justicia/conflicto-y-narcotrafico/narcos-que-se-han-operado-para-cambiar-su-apariencia-y-evadir-captura-549891>.

Schauer, Frederick. «Fear, Risk and the First Amendment: Unraveling the Chilling Effect». BOSTON UNIVERSITY LAW REVIEW 58 (s. f.).

Schurman, Por Diego. «Seguridad en los estadios: el Gobierno activará un sistema de reconocimiento facial en la Superliga». infobae. Accedido 29 de julio de 2023. <https://www.infobae.com/deportes-2/2018/03/25/seguridad-en-los-estadios-el-gobierno-quiere-instalar-un-sistema-de-reco-nocimiento-facial-en-la-superliga/>.

Seguridad Ciudadana. «¿Cómo combatir la impunidad? La modernización del sistema de justicia criminal en América Latina», 19 de noviembre de 2019. <https://blogs.iadb.org/seguridad-ciudadana/es/como-combatir-la-impunidad-la-modernizacion-del-sistema-de-justicia-criminal-en-america-latina/>.

Solon, Olivia. «Facial Recognition Database Used by FBI Is out of Control, House Committee Hears». The Guardian, 27 de marzo de 2017, sec. Technology. <https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports>.

Stark, Luke, y Jevan Hutson. «Physiognomic Artificial Intelligence». SSRN Electronic Journal, 2021. <https://doi.org/10.2139/ssrn.3927300>.

Temblores ONG. «Bolillo, Dios y Patria», 2021. <https://www.temblores.org/bolillo-dios-y-patria>.

Tendayi Achiume, E. «Informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia». Naciones Unidas, 10 de noviembre de 2020. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/304/57/PDF/N2030457.pdf?OpenElement>.

The Sentencing Project. «Report to the United Nations on Racial Disparities in the U.S. Criminal Justice System», 19 de abril de 2018. <https://www.sentencingproject.org/reports/report-to-the-united-nations-on-racial-disparities-in-the-u-s-criminal-justice-system/>.

Thomson, Billie. «China's facial-recognition cameras put jaywalkers' faces on billboards». Mail Online, 8 de noviembre de 2019. <https://www.dailymail.co.uk/news/article-7664797/Chinas-facial-recognition-punishes-jaywalkers-putting-pictures-big-screens.html>.

Tiempo, Casa Editorial El. «Los estadios de Brasil tendrán reconocimiento facial en Copa América». futbolred.com. Accedido 29 de julio de 2023. <https://www.futbolred.com/copa-america-brasil-2019/los-estadios-de-brasil-tendran-reconocimiento-facial-en-copa-america-2019-97841>.

United Biometrics. «Solutions, United Biometrics», 2 de diciembre de 2020. <https://unitedbiometrics.com/solutions/>.



Wertheim, K. «Extreme Case of Fingerprint Mutilation». *Journal of Forensic Identification* 48, n.o 4 (agosto de 1998): 466-77.

Westfall, Sammy. «U.N. Official Calls for Moratorium on Artificial Intelligence Tools That Breach Human Rights». *Washington Post*, 17 de septiembre de 2021. <https://www.washingtonpost.com/world/2021/09/15/un-ai-moratorium/>.

Wirecutter: Reviews for the Real World. «Facial Recognition Is Everywhere. Here's What We Can Do About It.», 15 de julio de 2020. <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/>.

WIRED. «Hinchas, familias y reconocimiento facial: ¿el Fan ID vulnera tus datos biométricos?» WIRED, 23 de julio de 2023. <https://es.wired.com/articulos/hinchas-familias-y-reconocimiento-facial-el-fan-id-vulnera-tus-datos-biometricos>.

Wired UK. «How to Make a Genuinely Inclusive Phone Camera». *Wired UK*. Accedido 29 de julio de 2023. <https://www.wired.co.uk/article/inclusive-cameras-apple-google>.

Wolf, Zachary B. «AI Can Be Racist, Sexist and Creepy. What Should We Do about It? | CNN Politics». *CNN*, 18 de marzo de 2023. <https://www.cnn.com/2023/03/18/politics/ai-chatgpt-racist-what-matters/index.html>.

Zuo, Kevin J., Tomas J. Saun, y Christopher R. Forrest. «Facial Recognition Technology: A Primer for Plastic Surgeons». *Plastic and Reconstructive Surgery* 143, n.o 6 (junio de 2019): 1298e-1306e. <https://doi.org/10.1097/PRS.0000000000005673>.



NORMATIVA Y/O ESTÁNDARES



Convención Americana sobre Derechos Humanos (Pacto de San José).



Principios Globales para las Naciones Unidas para la integridad de la información



EPÍLOGO

ALGUNAS REFLEXIONES EN TORNO A LAS TECNOLOGÍAS EMERGENTES Y DERECHOS HUMANOS



En la era contemporánea, el avance acelerado de las tecnologías emergentes plantea una serie de desafíos sin precedentes para la protección, promoción y garantía de los derechos humanos. Como lo evidencian los trabajos que informan esta obra, herramientas como la inteligencia artificial, el reconocimiento facial, el análisis de big data, la robótica y hasta la biotecnología están transformando nuestras sociedades, generando nuevas formas de interacción, control, exclusión y vigilancia. Este panorama tecnológico, aunque portador de grandes promesas para el desarrollo humano, plantea tensiones éticas y jurídicas fundamentales. ¿Cómo asegurar que estas tecnologías se utilicen de manera compatible con los principios de dignidad humana, igualdad, privacidad y no discriminación? ¿Qué límites debe imponer el Derecho para prevenir abusos y violaciones?

Uno de los retos más visibles es la protección de la privacidad y los datos personales. La capacidad de las tecnologías emergentes para recolectar, procesar y cruzar cantidades masivas de información sobre las personas ha puesto en jaque el control individual sobre sus propios datos. La vigilancia masiva, tanto estatal como corporativa, pone en dilema tanto los derechos civiles y políticos, como derechos económicos, sociales, culturales y ambientales.

En materia de derechos laborales, por ejemplo, el uso de algoritmos para tomar decisiones de contratación, ascenso o despido puede consolidar sesgos o discriminaciones históricas y estructurales, o incluso, generar nuevas formas de exclusiones. La opacidad de estos sistemas — conocida por muchos especialistas tecnológicos como la "caja negra algorítmica"— dificulta el control jurídico y social sobre sus impactos, socavando el derecho a la igualdad y a recursos judiciales efectivos en los Estados del Sistema Interamericano.

A nivel global, los aportes de los órganos de tratados en el sistema universal, así como jurisprudencia de los sistemas regionales de protección, aún se encuentra en una etapa incipiente en relación con la velocidad en que se desarrollan las tecnologías emergentes. Pese a algunos avances, como algunos informes de relatores especiales de Naciones Unidas o ciertos pronunciamientos del Tribunal Europeo de Derechos Humanos, nuestro Sistema Interamericano, todavía no adopta disposiciones que proporcione directrices o vías claras para abordar estas cuestiones, por más de los aportes que el Comité Jurídico Interamericano ha adelantado en materia de datos personales.

El Derecho Internacional de los Derechos Humanos fue diseñado en un contexto histórico y de exigibilidad de derechos muy distinto, y su adaptación al nuevo entorno digital requiere reflexiones profundas sobre la normativa e interpretación normativa a la luz de los tiempos actuales. En este sentido, la labor de los órganos de tratados, las cortes internacionales y los tribunales regionales será clave para establecer estándares jurídicos vinculantes que orienten a los Estados y al sector privado.



La responsabilidad de las empresas tecnológicas es otro punto que no se puede obviar en cuanto a su rol en la protección de los derechos humanos. Aunque no son sujetos tradicionales del Derecho Internacional, su influencia sobre los derechos humanos es cada vez más directa. Por ello, se requiere fortalecer los marcos normativos que regulan su conducta, como los Principios Rectores sobre las Empresas y los Derechos Humanos de la ONU, y explorar vías jurídicas para hacerlas responsables en casos de violaciones graves a derechos de las personas.

La brecha tecnológica en los países del Sistema Interamericano también genera riesgos de nuevas formas del denominado “colonialismo digital”. Muchos Estados en vías de desarrollo carecen de la infraestructura, la regulación y las capacidades técnicas necesarias para proteger eficazmente a las personas en su jurisdicción frente a las vulneraciones asociadas con las tecnologías emergentes. Esto puede profundizar desigualdades estructurales ya existentes.

En este contexto, grupos o colectivos históricamente discriminados como los pueblos indígenas, las personas migrantes, las mujeres, las personas LGBTQ+, y otras poblaciones enfrentan un riesgo mayor de sufrir discriminación y violaciones a sus derechos a través de tecnologías que reproducen sesgos estructurales o invisibilizan su existencia. La interseccionalidad que la Corte Interamericana de Derechos Humanos ha abordado de manera eficaz en casos sobre DESCAs, debe ser una herramienta clave en cualquier enfoque regulador aplicado a la materia que hoy nos ocupa en esta obra.

Por ello, es importante destacar que el principio de precaución ampliamente desarrollado por el Sistema Interamericano, cobra especial relevancia en este campo, frente a tecnologías cuyo impacto sobre los derechos humanos es aún incierto o podría ser potencialmente dañino. Bajo esta tesis, los Estados deben adoptar medidas regulatorias que prioricen la protección de las personas sobre la innovación desregulada.

También es indispensable repensar el concepto de jurisdicción en el entorno digital. En una situación que parece ir en ascenso, las afectaciones o posibles daños a derechos pueden originarse en un país y afectar a personas que se encuentran en otro, dificultando la exigencia de responsabilidad y el acceso a la justicia. Todo ello exige una mayor cooperación internacional y un fortalecimiento de mecanismos jurisdiccionales internacionales que interactúen en favor de las personas.

Desde el IIDH, consideramos que la educación en derechos humanos junto a una alfabetización digital responsable se vuelve esencial para empoderar a la ciudadanía frente a los posibles riesgos tecnológicos. Solo una sociedad informada podrá ejercer vigilancia crítica sobre el uso de estas herramientas, exigir rendición de cuentas y defender sus derechos frente a actores públicos y privados.

Llegado a este punto, conviene preguntarnos, ¿cuáles son aquellas posibles intersecciones positivas entre las tecnologías emergentes y un mejor acceso a derechos como la salud, la educación o la protección del medio ambiente?



En materia de derecho a la salud, las tecnologías emergentes están transformando el acceso a los respectivos servicios, con impactos concretos en equidad, eficiencia y prevención. Sectores como la telemedicina o la salud digital, permiten a personas en zonas rurales o aisladas acceder a consultas médicas sin necesidad de trasladarse grandes distancias, rompiendo barreras geográficas. A su vez, sectores estratégicos como la inteligencia artificial o la disposición de las denominadas “big data”, son aliados institucionales que mejoran la capacidad para realizar diagnósticos tempranos y tratamientos personalizados, detectando patrones en enfermedades de mortalidad infantil, así como en males crónicos o eventuales pandemias, apoyados en dispositivos portátiles como los biosensores que permiten monitorear la salud en tiempo real, permitiendo una mejor gestión del acceso a la salud superando desigualdades.

En el derecho a la educación, la tecnología también ha sido un catalizador para ampliar el acceso, sobre todo en contextos de emergencia o exclusión estructural. Destacan en esta experiencia, las plataformas virtuales de aprendizaje, que disponen de contenidos educativos de alta calidad a estudiantes en todo el mundo, incluyendo aquellos en contextos de crisis humanitarias o desplazamiento. La inteligencia artificial educativa, que tiene un alto grado de adaptabilidad, permite practicar modelos de enseñanza más inclusivos o bien de mayor alcance, como, por ejemplo, los cursos MOOC y que, junto a bibliotecas digitales, posibilitan un acceso al conocimiento sin barreras de costo o incluso de idiomas. Por supuesto, también se reconocen desafíos como la falta de conectividad en donde los Estados tienen la obligación de disponer de la infraestructura necesaria para evitar la profundización del analfabetismo digital o bien, la exclusión tecnológica.

Finalmente, las tecnologías emergentes pueden ser aliadas fundamentales en la defensa del medio ambiente y el cumplimiento del derecho a un entorno sano como lo han destacado recientes opiniones consultivas proferidas por la Corte Interamericana de Derechos Humanos, así como la Corte Internacional de Justicia, en las que se destaca la importancia de repensar mecanismos integrales para la prevención del cambio climático. Esto es posible, si se considera que la inteligencia artificial aporta importantes avances en la optimización de modelos predictivos, contribuyendo a una mejor toma de decisiones gubernamentales para la adopción de políticas de prevención de desastres, sin perjuicio de mencionar la necesaria inversión en tecnologías limpias y energías renovables que permitan transitar hacia economías más sostenibles y con menor impacto ecológico.

Es por todo lo anteriormente dicho, que para el IIDH plantear entendimientos sobre el rol de las tecnologías emergentes desde la perspectiva de derechos es potencialmente transformador, siempre que se implementen con enfoques de equidad, transparencia y control público, así como dotadas de regulación ética que posicione a la persona humana en el centro del desarrollo tecnológico y acompañadas de la cooperación técnica internacional que permita reducir brechas digitales y promueva activamente la transferencia tecnológica solidaria.

José Thompson Jiménez

Director Ejecutivo

Instituto Interamericano de Derechos Humanos

