

INTELIGENCIA ARTIFICIAL Y DERECHOS FUNDAMENTALES: IMPACTO EN LOS DERECHOS DE LA PRIVACIDAD

ARTIFICIAL INTELLIGENCE AND FUNDAMENTAL RIGHTS: IMPACT ON PRIVACY RIGHTS

*Marisol Peña Torres**
*María José Martabit Sagredo***

“El futuro es un futuro donde los niños de hoy no tendrán privacidad.
Todo lo que hagan desde sus primeros pasos será grabado
y asociado con ellos para siempre.
No estamos preparados como sociedad para el fin
de la privacidad y el armamento masivo de información”
(Horacio Roberto Granero (2022)¹)

RESUMEN: Este artículo reflexiona sobre los retos y desafíos que plantean los sistemas de inteligencia artificial (IA) que, sin perjuicio de proveer diversos beneficios al ser humano, abren, también, la puerta para discriminaciones y sesgos que terminan afectando la privacidad de las personas. A partir de la experiencia europea, se sugieren una serie de principios que puedan ser considerados en una futura ley de inteligencia artificial para Chile.

PALABRAS CLAVE: inteligencia artificial, derechos fundamentales, derecho a la privacidad.

* Profesora titular de Derecho Constitucional. Directora del Centro de Justicia Constitucional Universidad del Desarrollo. Correo electrónico: marisolpena@udd.cl

** CEO de Theodora AI. Profesora de la Facultad de Derecho de la Pontificia Universidad Católica de Chile. Correo electrónico: mariajosemartabit@theodora.ai

Esta contribución se enmarca en el proyecto Startup Ciencia SUC230199 de ANID 2023 adjudicado por Theodora Legaltech SpA. Se agradece especialmente la contribución de Paula Godoy Muñoz, abogada del equipo Theodora AI.

¹ GRANERO (2022) p. 107.

ABSTRACT: This article reflects on the challenges raised by Artificial Intelligence (AI) systems that, without prejudice to providing various benefits to human beings, also open the door to discrimination and biases that end up affecting people's privacy. Based on the European experience, a series of principles are suggested that can be considered in a future Artificial Intelligence Law for Chile.

KEYWORDS: artificial intelligence, fundamental rights, right to privacy.

INTRODUCCIÓN

La inteligencia artificial (en adelante IA) –como la globalización– es uno de los temas que han llegado para quedarse entre nosotros. Puede sostenerse, en efecto, que el uso de datos y algoritmos matemáticos para encontrar soluciones a problemas específicos, más o menos sofisticados, es parte de la vida cotidiana de las sociedades contemporáneas.

Pero, así como la IA ha facilitado el desarrollo de procesos de toma de decisiones en diversos ámbitos y de muchos aspectos de nuestro desenvolvimiento cotidiano, también ha generado diversos cuestionamientos. Estos abarcan desde temas generales como su impacto en el funcionamiento de los sistemas democráticos hasta otros más específicos que tienen que ver con los criterios y estándares que deben cumplir los sistemas de IA a fin de que su utilización no se constituya en un riesgo para la misma vida humana.

Una de las preocupaciones más fundamentales que despierta el uso de la IA tiene que ver con sus connotaciones éticas, sobre todo, cuando los nuevos desarrollos científicos y tecnológicos se acercan a producir máquinas que se acerquen lo más posible a lo que es un ser humano o cuando se interviene el cerebro de estos para producir personas moralmente mejores². Como sostiene Milagros Otero:

“memoria, inteligencia y voluntad, que son las tres potencias fundamentales del alma, podrían resultar similares en una máquina perfeccionada y en un ser humano. Pero siempre la primera sería una máquina y el segundo una persona”³.

Agrega que, por mucho que el desarrollo de las máquinas y del sistema de algoritmos que utilizan se acerque a la perfección, existen operaciones específicas de la inteligencia humana que nunca podrían tener las máquinas como, por ejemplo, “las emociones, la conciencia, la intuición, etc.”⁴.

² SALLES (2018) p. 395.

³ OTERO (2023) p. 41.

⁴ *Ibid.*

Otra preocupación que ha levantado el creciente uso de la IA y de las técnicas de tratamiento de datos tiene que ver con la capacidad de regular y controlar a sujetos privados como las megacorporaciones digitales capaces de ejercer una influencia política y social masiva como de adquirir nuevos desarrollos y *startups* en su ámbito propio⁵.

Desde el punto de las repercusiones de la inteligencia artificial en el ámbito de los derechos fundamentales, Carlos Bernal indica que una ventaja consistiría en “la identificación de puntos ciegos en la satisfacción de los derechos fundamentales” que forma parte esencial del Estado de derecho. Agrega:

“Ninguna autoridad individual o colegiada –legisladores, tribunales o reguladores– tiene la capacidad de procesamiento de información necesaria para calcular qué decisiones optimizan la satisfacción de los derechos fundamentales. Para suplir esta deficiencia, estas autoridades pueden valerse del análisis del *big data* de que es capaz la inteligencia artificial”⁶.

No obstante, el mismo autor identifica, también, desafíos importantes para los derechos fundamentales derivados del desarrollo de los cada vez más sofisticados sistemas de IA. Entre dichos desafíos destaca la adecuada y responsable regulación de las plataformas como destinatarias de derechos fundamentales, la clausura algorítmica a la deliberación de un derecho fundamental, la invasión de la intimidad y la discriminación algorítmica⁷ muy relacionada con los sesgos en el manejo y uso de datos que proveen las mencionadas plataformas.

Por su parte, y como señala el proyecto de ley, que se encuentra en segundo trámite constitucional en la Cámara de Diputadas y Diputados, sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías:

“los avances en tecnología de escritura cerebral suponen un gran logro en medicina, (pero) levanta preocupación cuando esta tecnología llegue al mercado, puesto que se trataría de tecnología al alcance de unos pocos, que podría aumentar las brechas sociales entre quienes pueden costear tratamientos de escritura cerebral, permitiendo mejorarse a sí mismos con mayor rapidez, o facilitando su aprendizaje, contra quienes deban seguir atendiendo a los métodos convencionales. La denominada división entre humanos y metahumanos”⁸.

⁵ NEMITZ (2021) p. 131.

⁶ BERNAL (2022) p. 1441.

⁷ *Ibid.*

⁸ Proyecto de ley, iniciado en moción de los senadores Guido Girardi, Carolina Goic, Francisco Chahuán, Juan Antonio Coloma y Alfonso de Urresti, Sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías.

Ahora bien, entre los derechos fundamentales que resultan más impactados por el uso de la IA se encuentran aquellos que se vinculan con el valor de la privacidad (derechos a la vida privada, a la honra, a la protección de los datos personales, a la inviolabilidad del hogar y de las comunicaciones privadas). Las soluciones pueden ir desde:

“generar nuevas e importantes facultades que se interpreten como parte del objeto de algunos derechos fundamentales ya reconocidos y, en su caso, se plasmen en las leyes que los desarrollen”⁹.

Si no se logra una regulación por la vía descrita podría acudirse a la técnica de los derechos implícitos¹⁰ que la jurisprudencia de nuestros tribunales ya ha reconocido¹¹.

Pero, además, se plantea la necesidad de promover cambios constitucionales que incorporen otros derechos, como sugiere el proyecto de ley sobre neuroderechos, que, apelando a los avances científicos en esta materia, se refiere al impulso al reconocimiento de cinco nuevos derechos humanos:

- a) El derecho a la privacidad mental (los datos cerebrales de las personas);
- b) El derecho a la identidad y autonomía personal;
- c) El derecho al libre albedrío y a la autodeterminación;
- d) El derecho al acceso equitativo a la aumentación cognitiva (para evitar producir inequidades) y
- e) El derecho a la producción de sesgos de algoritmos o procesos automatizados de toma de decisiones¹².

Esta propuesta se basa en las investigaciones desarrolladas por el doctor Rafael Yuste, junto a Sara Goering, a través del Morningside Group.

En Chile, los estudios, como la normativa aplicable a la regulación de la IA, son aún incipientes. Entre los artículos académicos destacan los de los académicos Patricio Masbernat y Vincenzo Pasquino¹³ y Pablo López Silva y Raúl Madrid¹⁴. Un panorama genérico de los desafíos que levanta la IA puede encontrarse en la reciente publicación *30 miradas: Inteligencia artificial y educación*

⁹ PRESNO (2023) p. 84.

¹⁰ CASTILLO-CÓRDOVA (2008).

¹¹ Una perspectiva crítica al reconocimiento jurisprudencial de los derechos implícitos en Chile puede encontrarse en CONTRERAS (2011).

¹² Proyecto de ley, iniciado en moción de los senadores Guido Girardi, Carolina Goic, Francisco Chahuán, Juan Antonio Coloma y Alfonso de Urresti, Sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías.

¹³ MASBERNAT y PASQUINO (2023).

¹⁴ LÓPEZ-SILVA y MADRID (2021).

de futuro, de la Universidad del Desarrollo¹⁵. Desde la perspectiva normativa, la dictación de la Ley n.º 21383, que modificó la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas, agregando un párrafo final en el numeral 1) de su art. 19¹⁶ ha sido, sin duda, un primer avance importante. Y, por cierto, no puede soslayarse el proyecto de ley presentado por un grupo de senadores, en el año 2020, ya aludido.

Este artículo persigue identificar los riesgos y problemas que ha abierto el desarrollo de la IA en los derechos fundamentales de las personas, enfocando el análisis en los derechos vinculados al valor de la privacidad. La pregunta orientadora no es si los sistemas de IA podrían reemplazar a los operadores jurídicos, fundamentalmente a los jueces, sino, más bien, si el derecho puede utilizar sus regulaciones para aminorar los riesgos que abren esos sistemas, permitiendo que cumplan el objetivo de ayudarnos a desarrollar una vida mejor y más plena.

I. EL DESARROLLO DE LA INTELIGENCIA ARTIFICIAL.

¿UN NUEVO PARADIGMA EN EL DERECHO?

Para comenzar, debe señalarse que la IA es una disciplina científica que nació en 1956 en el Dartmouth College, en Hanover, Estados Unidos, durante un curso de verano organizado por cuatro investigadores (John McCarthy, Marvin Minsky, Nathaniel Rochester y Claude Shannon)¹⁷. Sin embargo, en dicho año solo nació el término “IA”, pues mucho antes, en 1952, Arthur Samuel creó un *software* capaz de aprender a jugar ajedrez de forma autónoma; e, incluso, de manera anterior a ello, en el año 1943 Warren McCulloch y Walter Pitts presentaron el primer modelo matemático para la creación de una red neuronal¹⁸. Y aun, otros se remontan al año 1936, cuando Alan Turing dio a conocer su artículo sobre “Números calculables” al que se atribuye el inicio de las bases teóricas para todas las ciencias de la computación, y que puede considerarse el origen oficial de la informática teórica¹⁹.

¹⁵ BRAVO Y BRAVO (2023).

¹⁶ Artículo único, 2) Agrégase el siguiente párrafo final, nuevo: “El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella”.

¹⁷ GANASCIA (2018).

¹⁸ DATASCIENTEST (2022).

¹⁹ REBOLLO (2023) p. 19.

Pero ¿qué es la inteligencia artificial? Al respecto, existen múltiples definiciones. Así lo exponen Patricio Masbernat y Vincenzo Pasquino, quienes, citando otros autores, entregan las siguientes:

- primero, “una disciplina académica relacionada con la teoría de la computación cuyo objetivo es emular algunas de las facultades intelectuales humanas en sistemas artificiales”;
- segundo, “ciencia de construir máquinas para que hagan cosas que, si las hicieran los humanos, requerirían de inteligencia”;
- tercero, “ciencia que persigue crear sistemas que piensen o actúen como humanos, o que piensen o actúen racionalmente”²⁰.

Enrique Cáceres, por su parte, ha expresado que por IA:

“podemos entender la rama de la ciencia computacional dedicada al desarrollo de programas cuyos productos finales, de ser atribuibles a un humano, presupondrían procesos mentales inteligentes”²¹.

Asimismo, para Goretty Martínez, la IA es:

“una rama de la informática jurídica que trata de realizar con máquinas, tareas que puede realizar el ser humano aplicando cualquier tipo de razonamiento”²².

A su vez, desde el año 2021, la Comisión Europea –de manera más precisa, el Comité de Inteligencia Artificial– ha estado trabajando en una propuesta de ley que regule los aspectos de esta nueva área. El día 18 de diciembre de 2023, dicho Comité publicó el tercer borrador, en el cual se define a la IA de la siguiente forma:

“Sistema basado en una máquina que, con objetivos explícitos o implícitos, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales”²³.

En concordancia con lo anterior, sería posible señalar que, si bien, la IA no cuenta con una definición uniforme, todas aquellas entregadas –tanto por la doctrina como por diferentes organismos–, son coherentes en identificar dos elementos clave: en primer lugar, la relación con la tecnología, ya sea en términos de máquinas o sistemas computacionales y, en segundo lugar, la idea de que

²⁰ MASBERNAT Y PASQUINO (2023) p. 4.

²¹ CÁCERES (2022) p. 65.

²² MARTÍNEZ (2012) p. 828.

²³ COMMITTEE ON ARTIFICIAL INTELLIGENCE (2023).

dicha tecnología realiza tareas hechas por personas, es decir, la asimilación de la máquina a la persona, de modo que se puede inmiscuir en cualquier aspecto de la vida de una persona. De esta forma, la IA puede significar una gran ventaja para cualquier proceso de la vida cotidiana, dado que realiza las mismas tareas que una persona, pero de una forma más eficiente; sin perjuicio que también tiene desventajas y riesgos²⁴.

Así las cosas, hay dos aspectos relevantes de analizar a lo largo de este apartado. El primero: ¿por qué si la IA surgió hace más de medio siglo, toma relevancia en estos momentos? y, el segundo, ¿cómo impacta la misma en el derecho –como un aspecto importante en la vida de una persona– y cuál es el paradigma a seguir?

Respecto de la primera pregunta, si bien la IA surgió hace más de medio siglo, es hoy cuando ha tomado relevancia, pues el avance tecnológico ha sido tal que la CEPAL lo ha denominado como la “cuarta revolución tecnológica”²⁵ y, si bien ello puede aparejar diversos beneficios, también conlleva riesgos que antes no existían y que impactan los derechos humanos en general, toda vez que estos sistemas se entrenan con dichos datos. De ahí la importancia de las medidas regulatorias de la IA, en la medida que ya se ha reconocido que estos sistemas presentan riesgos únicos tanto para la privacidad de las personas como para la sociedad²⁶.

Es importante tener presente que la nueva Ley de Inteligencia Artificial aprobada por el Parlamento Europeo, el 14 de marzo de 2023 y que, sin duda, está a llamada a ser un referente en esta materia, incorpora reglas que establecen obligaciones para proveedores y usuarios de la IA, las que se clasifican, precisamente, en función del nivel de riesgo que suponen.

Así, existen “sistemas de riesgo inaceptable” como aquellos que tienen que ver con la identificación biométrica en tiempo real y a distancia, así como con el reconocimiento facial. Asimismo, se encuentran los “sistemas de alto riesgo” que, a su vez, se subdividen en:

- a) Aquellos que se utilicen en productos sujetos a la legislación de la Unión Europea sobre seguridad de los productos como juguetes, aviación y automóviles y
- b) Aquellos pertenecientes a ocho ámbitos específicos que deberán registrarse en una base de datos de la Unión Europea, entre los que se encuentran la gestión de la migración, el asilo y el control de fronteras.

²⁴ Uno de los riesgos se asocia a la vulneración de los derechos humanos; por ejemplo, la perpetuación de los sesgos de género. UNESCO (2024).

²⁵ CEPAL (2019).

²⁶ KING; MEINHARDT (2024) p. 19.

Asimismo, se distinguen los sistemas de “riesgo limitado” que están sujetos a obligaciones de transparencia como ocurre con los *chatbots* y *deepfakes*. Finalmente, los sistemas de “riesgo mínimo” no están sujetos a mayores regulaciones como es el caso de los videojuegos y los filtros de spam.

Ahondando en la segunda interrogante, el derecho es un ámbito que no ha escapado a la IA, la cual ha tenido impacto –ya sea positivo o negativo– en diferentes áreas tales como: propiedad intelectual e industrial, protección de datos, contratos, responsabilidad civil extracontractual y contractual, derechos del consumidor; incluso, en la administración de justicia y en la educación jurídica²⁷.

Al respecto, es posible mencionar algunos sistemas de IA que operan dentro de la esfera del derecho. Estos son, en primer lugar, el sistema *Expertus I* y *II*, cuya finalidad es ayudar a la toma de decisiones y a la homogeneización del conocimiento colectivo de la comunidad judicial en el dominio del juicio especial de alimentos²⁸ y simular los procesos cognitivos que realizan los jueces al ponderar los distintos pesos probatorios asignados a las pruebas y contrapruebas ofrecidas por cada una de las partes, así como las razones morales que tienen lugar en casos de confrontación entre el derecho y la moral²⁹, respectivamente.

En segundo lugar, el sistema *Ross*, cuyo objetivo es comprender el lenguaje natural y brindar respuesta en tiempo real a la búsqueda de información sobre precedentes, legislación de nueve países, libros, revistas y noticias relevantes para la solución de un caso, siendo, también, capaz de predecir y notificar de los riesgos que nuevos precedentes o leyes podrían significar para determinado asunto³⁰.

En tercer lugar, el sistema *Vincent*, cuyo objetivo es relacionar los precedentes más relevantes conectados con una sentencia objeto de consulta, representar la relación mediante un grafo dirigido denominado mapa de precedentes y medir el impacto de las citas referenciadas en la argumentación de las decisiones³¹.

En España destacan los sistemas *VeriPol*, que estima la probabilidad de que una denuncia sea falsa y *VioGén*, que señala la peligrosidad de posibles hombres maltratadores e incide en las decisiones de prisión preventiva³².

En último lugar, el sistema *Prometea*, cuyo objetivo es ayudar a los operadores a desahogar el trabajo repetitivo para que puedan dedicar su tiempo

²⁷ MASBERNAT y PASQUINO (2023) pp. 12-18.

²⁸ CÁCERES (2022) p. 69.

²⁹ *Op. cit.* p. 82.

³⁰ *Op. cit.* pp. 85-86.

³¹ CÁCERES (2022) p. 86.

³² CASTELLANOS y MONTERO (2020) p. 73.

a funciones sustanciales. Su operación implica la identificación de patrones de propiedades en una gran cantidad de documentos, así como su correlación con decisiones específicas³³.

No obstante, uno de los ámbitos que más riesgo corre si no se cuenta con una reglamentación clara al respecto, es la esfera de los derechos humanos³⁴. Lo anterior, reconocido por Volker Türk –alto comisionado de Naciones Unidas– quien señala que los recientes avances tecnológicos en inteligencia artificial representan un daño potencial al paradigma de los derechos humanos al no estar contemplados como su fundamento de desarrollo, por lo que tanto gobiernos como empresas deben desarrollar con prontitud protecciones efectivas³⁵.

En este sentido, más que hablar de la inteligencia artificial como un nuevo paradigma en el derecho, lo correcto, en este caso, debiese ser referirse a “los derechos humanos como paradigma de la IA en cuanto ésta se relacione con el ordenamiento jurídico”³⁶. En efecto, la OCDE ha desarrollado algunas re-

³³ CACERES (2022) p. 86.

³⁴ Se ha señalado que los principales problemas de la IA en los derechos humanos son los siguientes:

- (a) El derecho a la privacidad. El riesgo se genera porque los sistemas de IA son capaces de recoger, procesar y analizar volúmenes masivos de datos personales, información sensible y personal, muchas veces sin el consentimiento informado del individuo.
- (b) Riesgos de discriminación indebida y trato desigual. La inteligencia artificial y sus algoritmos pueden perpetuar, replicar y amplificar los sesgos existentes en los datos de base histórica con los que se construye y entrena.
- (c) Respeto de la libertad de expresión y opinión. La moderación automática del contenido y la detección automática de información en plataformas digitales puede amenazar estas libertades al restringir contenido legítimo o permitiendo contenido perjudicial.
- (d) Derecho al trabajo. La IA y la automatización plantean interrogantes sobre el acceso de las personas al empleo, sus condiciones, su precarización y su estabilidad.
- (e) La bioética y derechos humanos. La aplicación de la IA en la medicina, la biología, la biotecnología y la genética, genera dudas respecto de cuestiones éticas y legales relacionadas con la dignidad humana, la integridad física y mental, y los derechos a la salud y a la vida, la propiedad o patentabilidad de organismos vivos y componentes biológicos.
- (f) Seguridad y derecho internacional. Hay asuntos éticos y jurídicos complejos en los ámbitos del derecho internacional humanitario y los derechos humanos en la utilización de IA en el ámbito de la seguridad nacional y en conflictos armados, en la creación y uso de armas autónomas y sistemas de vigilancia avanzados.

³⁵ TÜRK (2023). En el mismo sentido, HERRERA (2023) p. 66.

³⁶ La UNESCO (2023) p. 134 ha señalado que hay cinco ventajas clave en el aprovechamiento de los marcos de derechos humanos en el contexto de la IA:

- La amplia infraestructura internacional, regional y nacional de derechos humanos, toda vez que existen instituciones establecidas que pueden contribuir a la realización de los derechos humanos en el contexto de la IA.
- Un amplio cuerpo normativo de legislación nacional, regional e internacional que ha hecho operativa la aplicación de los derechos humanos en el ámbito digital.

comendaciones que contienen principios, dentro de los cuales, hay uno que indica que los sistemas de inteligencia artificial deben diseñarse respetando el Estado de derecho, los derechos humanos, los valores democráticos y la diversidad, y que deben incluir los mecanismos apropiados como, por ejemplo, permitir la intervención humana cuando sea necesario para garantizar una sociedad justa y equitativa³⁷.

Así lo ha expresado la UNESCO en su 41.º reunión realizada en París el año 2021, donde se reconoció que, si bien la IA tiene potencial para transformar el futuro de la humanidad para mejor y en favor del desarrollo sostenible, también existe una conciencia de los riesgos y desafíos que conlleva, en especial, por lo que respecta a la agravación de las desigualdades y brechas existentes, así como a las implicaciones para los derechos humanos³⁸. Por ello, en el segundo apartado del Proyecto de Recomendación sobre la Ética de la Inteligencia Artificial esto es, los fines y objetivos, se establece:

“la presente recomendación tiene por objeto servir de base para poner los sistemas de IA al servicio de la humanidad, las personas, las sociedades y el medio ambiente y los ecosistemas, así como para prevenir daños. Aspira también a estimular la utilización de los sistemas de IA con fines pacíficos”³⁹.

Con respecto a lo anterior, uno de los casos más vigentes es aquel en que recientemente, el día 29 de febrero de 2024, Elon Musk demandó a OpenAI y Sam Altman⁴⁰ por construir una IA que, si bien en un principio era para la humanidad, sus fines han devenido en otros. La demanda se enfoca en exponer los distintos riesgos que derivan del uso de la inteligencia artificial. Sin embargo, y a pesar de que hoy es más patente y las personas son más conscientes de dichos riesgos, no se trata de algo nuevo.

En efecto, durante el año 2015, Six4Three demandó a Facebook –entidad que se ha visto fuertemente relacionada con la filtración de datos perso-

-
- El hecho de que los derechos humanos proporcionen un lenguaje universal para cuestiones que trascienden las fronteras nacionales, como la IA.
 - Los derechos humanos gozan de legitimidad y apoyo generalizados en todo el mundo.
 - Muchos Estados tienen algún tipo de marco de derechos humanos, aunque no tengan un marco de protección de datos, por lo que utilizar el marco de derechos humanos como base haría que el proceso fuera más inclusivo.

³⁷ MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA (2019).

³⁸ ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA EDUCACIÓN, LA CIENCIA Y LA CULTURA (2021).

³⁹ *Ibid.*

⁴⁰ SUPERIOR COURT OF CALIFORNIA (2024). Elon Musk vs. Samuel Altman; Gregory Brockman; OpenAI.

nales—, pues, durante los años 2011 y 2015, utilizó datos personales de sus usuarios como moneda de cambio para negociar y manipular a competidores. En este sentido, se señaló en la demanda que Facebook proporcionaba datos personales de usuarios solo a aquellos desarrolladores que contrataban publicidad a la red social a través de una empresa subsidiaria o a aquellos que no representaban una amenaza para la red social.

Sin embargo, la situación anterior no salió a la luz por sí misma, sino que, debido a otro caso del año 2018: Cambridge Analytica. Durante el año 2018, una serie de usuarios de Facebook del Reino Unido demandaron a dicho ente debido a que este compartió en forma ilegal datos de usuarios con la firma de investigación “Cambridge Analytica”⁴¹. Con ello, se logró que Meta, matriz de Facebook, aceptara pagar USD 725 000 000 por la afectación y la adquisición ilegítima de dichos datos; no obstante, investigadores se percataron que los documentos que obtuvieron a partir de este juicio, fueron los mismos que en el año 2015, de manera que Meta no cuestionó la autenticidad de los mismos⁴².

Lo curioso de lo anterior y el impacto real de ambos casos tiene relación con la sanción aplicada a Meta, pues mientras en el primero no se señala con claridad cuál fue, en el segundo sí se aplica una sanción de manera tajante, lo que, evidentemente, se debe al cambio de regulación. Asimismo, dicho cambio tiene un impacto real en la reputación y el valor de la compañía, dado que el caso de Cambridge Analytica hizo que el valor de Facebook cayera USD 37 000 000 000⁴³, lo cual impacta aún más que la multa impuesta.

El mismo peligro anterior genera Google, quien, según palabras de Amnistía Internacional:

“[junto a] Facebook dominan actualmente nuestra vida, pues acumulan un poder sin igual sobre el mundo digital por medio de la recopilación y monetización de los datos personales de miles de millones de personas [...] menoscabando la esencia misma de la privacidad, siendo uno de los problemas de derechos humanos que definen nuestra época”⁴⁴ (el destacado es nuestro).

Así, en su informe “Surveillance giants: How the business model of Google and Facebook threatens human rights”⁴⁵ ha catalogado a estas dos plataformas como “la nueva plaza pública global” y de ahí el peligro de no regular o resguardar los datos personales.

⁴¹ BLOOMBERG (2022).

⁴² SOLON and FARIVAR (2019).

⁴³ BBC MUNDO (2018).

⁴⁴ AMNISTÍA INTERNACIONAL (2019a)

⁴⁵ AMNISTÍA INTERNACIONAL (2019b).

Kumi Naidoo, quien está a cargo de dicho informe, ha señalado:

“Internet es esencial para que la gente disfrute de muchos de sus derechos, pero miles de millones de personas no tienen una opción significativa de acceso a este espacio público si no es con las condiciones dictadas por Facebook y Google”.

Agrega, además:

“para colmo, esta no es la Internet a la que la gente se adhirió cuando estas plataformas empezaron a funcionar. Google y Facebook han ido menoscabando nuestra privacidad con el tiempo. Ahora estamos en sus manos. O nos sometemos a esta maquinaria de vigilancia generalizada, en la que se aprovechan fácilmente de nuestros datos para manipularnos e influenciarnos, o perdemos las ventajas del mundo digital”⁴⁶.

Otro de los casos más importantes en relación con la filtración de datos y, por ende, que demuestra la necesidad de una fuerte protección es la de British Airways, entidad que mantenía medidas poco eficientes de seguridad y que, en consecuencia, se vio afectada por un ataque de *skimming* durante el año 2018 –robo de información de tarjetas de crédito utilizado al momento de la transacción– y que afectó casi a quinientas mil personas. La empresa fue multada por la Oficina de la Comisión de Información en Reino Unido con más de doscientos millones de euros, la más grande impuesta en dicho territorio. Asimismo, y al igual que en el caso de Facebook, el no tener un buen sistema de protección de datos influye, también, en la reputación de la empresa, al punto que cuando British Airways fue multada, sus títulos cayeron en la bolsa de inmediato⁴⁷.

Estudios revelaron que en 2021 el costo de las filtraciones de datos alcanzó niveles históricos. De hecho, el informe global de IBM Security “Cost of a Data Breach” señaló que, en el ámbito global, las filtraciones de datos tuvieron un costo de USD 4 024 000 y que en América Latina cada incidente cuesta a las empresas un promedio de USD 1 082 000⁴⁸. El mismo informe, el año 2023, ha establecido que este costo ha aumentado a USD 4 045 000 representando un aumento de un 15,3 respecto al informe del año 2020⁴⁹.

En nuestro país, el problema de la filtración de datos no ha sido algo ajeno, en especial en el ámbito bancario⁵⁰. Un estudio hecho por Fortinet arro-

⁴⁶ AMNISTÍA INTERNACIONAL (2019a).

⁴⁷ *Diario Financiero* (2019).

⁴⁸ *El Mostrador* (2022).

⁴⁹ IBM (2023).

⁵⁰ CNN CHILE (2019).

jó que solo durante el cuarto trimestre del año 2018, Chile recibió más de 23 500 000 de intentos de ciberataques, acaparando el 15 % de las amenazas de América Latina y posicionándose entre los cinco mercados más intimidados por *hackers* en el ámbito regional⁵¹. Es probable que dicho antecedente tenga relación con el estudio realizado por el Observatorio de Sociedad Digital de la Facultad de Economía y Negocios de la Universidad de Chile junto con la consultora Custom Trigger, en el cual se señala que el 93 % de los ciudadanos se sienten muy preocupados de que las organizaciones usen sus datos para otros fines diferentes para los cuales fueron solicitados⁵².

Incluso, en el ámbito público, durante el año 2022 se dio a conocer el *hacking* a los correos del Ministerio de Justicia, entre noviembre de 2021 y enero de 2022, lo cual expuso datos sensibles de menores del Servicio Nacional de Menores –SENAME– y de casos de familia; tales como: nombres, RUT, diagnósticos de salud y vulneraciones que han sufrido, mediaciones, violencia doméstica, entre otros; además del monitoreo que realizaba el gobierno de turno a los candidatos presidenciales⁵³.

Es por todo lo anterior que, como sociedad, debemos establecer una serie de principios que definan, con base en la dignidad de las personas, las cuestiones éticas que rodean los avances en inteligencia artificial, no solo desde un ámbito local, sino partiendo de un enfoque globalizado que permee a los niveles inferiores y que sirva como eje rector en el desarrollo y utilización de este tipo de tecnologías⁵⁴.

Estos esfuerzos ya se han visto reflejados en la recomendación de la UNESCO señalada con anterioridad; en los “Principios de Inteligencia Artificial de Asilomar”⁵⁵, los cuales reconocen de manera expresa en el principio n.º 11, el debido respeto por los derechos humanos. Estados Unidos, siguiendo el modelo europeo, a partir de una orden ejecutiva sobre IA, busca, por su parte, unificar su normativa, de manera que –por el momento–, a falta de aprobación de legislación federal que regule la inteligencia artificial, un número cada vez mayor de agencias federales y legisladores estatales están aclarando cómo se relaciona la regulación existente con la IA dentro de sus áreas jurisdiccionales y proponen una regulación específica⁵⁶.

⁵¹ VERA (2019).

⁵² MAULÉN (2022) p. 6.

⁵³ SEGOVIA y SEPÚLVEDA (2022).

⁵⁴ HERRERA (2023) pp. 77-78.

⁵⁵ Principios desarrollados en el marco de una conferencia que tuvo lugar en Asilomar, California en enero de 2017 y que fue organizada por el Future of Life Institution. MORANDÍN-AHUERMA (2023) p. 5.

⁵⁶ KING; MEINHARDT (2024).

II. EL IMPACTO DE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO A LA PRIVACIDAD: LECCIONES DESDE EUROPA

La defensa y protección de los derechos fundamentales está asociada al corazón del Estado de derecho y, consecuentemente, de la democracia en una era que ya no solo es globalizada, sino que “digital”⁵⁷.

La historia misma del constitucionalismo está ligada a la progresiva importancia que han ido adquiriendo los derechos fundamentales a través del tiempo como concreciones del supremo valor de la dignidad humana. De allí que un sector importante de la doctrina está conteste en que hoy vivimos una etapa de “constitucionalismo de los derechos” que, aunque no haga perder la noción de la Constitución como instrumento al servicio del control del poder, focaliza su atención en el reconocimiento y protección eficaz de derechos clásicos (como los de primera generación) como de los nuevos derechos que se han ido incorporando a las Cartas Fundamentales (derechos económicos, sociales, culturales y derechos colectivos).

Como sostiene Luis Prieto Sanchís:

“el constitucionalismo de los derechos propicia un sistema al menos estático como dinámico: la validez de las normas sigue siendo en parte una cuestión dinámica o de sucesivas habilitaciones de poder; pero solo en parte, porque dicha validez depende siempre del contenido de las normas, es decir de su adecuación a los preceptos sustantivos de la constitución y, en particular, a los derechos fundamentales”⁵⁸.

La evolución y nuevos requerimientos de protección referidos a los derechos fundamentales están marcados por la evolución que la sociedad va experimentando producto de las nuevas exigencias de la convivencia como, asimismo, por los cambios que en esta se van produciendo. Por lo mismo, el preámbulo de la Carta de los Derechos Fundamentales de la Unión Europea indica que es necesario:

“reforzar la protección de los derechos fundamentales al tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos”⁵⁹.

En lo que se refiere a los requerimientos derivados de la era digital, Europa ha mostrado un avance señero que bien puede servir de ejemplo y estímulo

⁵⁷ REBOLLO (2023) p. 13.

⁵⁸ PRIETO (2013) p. 13.

⁵⁹ PARLAMENTO EUROPEO (2000).

lo para sociedades como la nuestra, que hace muy poco ha empezado a reflexionar sobre estos temas. El solo hecho de que el Parlamento Europeo haya aprobado una ley de inteligencia artificial⁶⁰, como se ha señalado, marca un hito normativo que merece relevarse.

Como ha señalado el propio Parlamento Europeo:

“[...] el establecimiento del primer marco regulador del mundo en materia de IA podría suponer una ventaja para la Unión, como pionera, para establecer normas internacionales de IA basadas en los derechos fundamentales, así como para exportar con éxito la IA ‘de confianza’ centrada en el ser humano a todo el mundo [...]”⁶¹.

En esta línea, una serie de resoluciones aprobadas por el Parlamento Europeo ya han abordado aspectos específicos relacionados con la inteligencia artificial como ocurrió con la resolución de 20 de octubre de 2021 sobre los medios de comunicación europeos en la Era Digital, en la que se constata que, además de los efectos de la pandemia del COVID 19 que los estaba afectando, los medios estaban enfrentando desafíos importantes relacionados con la transición digital y su impacto en el modelo de negocio global del sector, el que debía considerar la salvaguarda de los derechos fundamentales de los ciudadanos.

El desarrollo que ha experimentado la IA hasta hoy permite sostener que:

“entre los derechos fundamentales más afectados por la IA estarán los que garantizan la dimensión privada de las personas: la intimidad, la propia imagen, la protección de los datos personales y el secreto de las comunicaciones, reconocidos en los apartados 1 y 4 del art. 8 CE (Constitución de España), en el art. 8 CEDH (Convenio Europeo de Derechos Humanos) y en los arts. 7 y 8 CDFUE (Carta de Derechos Fundamentales de la Unión Europea [...]”⁶².

El derecho a la intimidad, en el que se concentra este estudio, constituye una expresión directa de la dignidad sustancial de toda persona y, en general, impide que terceros penetren en esa esfera reservada, a menos que medie el consentimiento del titular del derecho.

Como sostiene la ministra de nuestra Corte Suprema, Angela Vivanco, intimidad y vida privada:

⁶⁰ Las normas generales sobre IA se aplicarán un año después de su entrada en vigor en el año 2025, en tanto que las obligaciones relativas a los sistemas de alto riesgo entrarán en vigor en tres años.

⁶¹ PARLAMENTO EUROPEO (2022) párrafos 10, 19 y 104.

⁶² PRESNO (2023) p. 37.

“son partes de un todo al que puede darse el nombre de *privacidad* y que actúan como una suerte de círculos concéntricos. El círculo más exterior, relativo a la vida privada, se traduce en una reserva del público de ciertos hechos o actos, que puede ser levantada en las condiciones y circunstancias previstas por el derecho, particularmente *cuando estamos en presencia del consentimiento del propio titular*, del interés público antes mencionado o de ámbitos de reserva previstos por un individuo que entran en conflicto con su propia conducta o con las propias exigencias de publicidad que hace el Derecho. Frente a este ámbito, la intimidad está representada por un círculo más pequeño e interno, que contiene aquellos elementos que son de tal modo personales, que, de suyo, deben quedar sustraídos al conocimiento, a la injerencia y a la intervención de los demás, aun cuando el propio titular admitiera en ello, fundamentalmente en asociación con el respeto por la dignidad del hombre, sus creencias, su conciencia y su identidad”⁶³ (El destacado es nuestro).

Tal como se señaló, el Convenio Europeo de Derechos Humanos, de 1950, en su art. 8, garantiza el respeto a la vida privada y familiar, así como al domicilio y correspondencia agregando que:

“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”.

Por su parte, el art. 7 de la Carta de los Derechos Fundamentales de la Unión Europea, de 2000, asegura, también, el respeto de la vida privada y familiar, como del domicilio y las comunicaciones.

Su art. 8 incorpora, a su vez, la protección de los datos de carácter personal que conciernen a la persona prescribiendo que estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernen y a obtener su rectificación confiando el respeto de estas normas al control de una autoridad independiente.

No debe extrañar que entre las regulaciones pioneras que han impactado en el ámbito de la IA se encuentre la primera directiva de protección de

⁶³ VIVANCO (2006) p. 349.

datos personales en la Unión Europea, del año 1995, y que decantó en el Reglamento de Protección de los Datos Personales, del año 2016.

Como advierte Paul Nemitz, ya desde aquella primera directiva se levantaron argumentos contrarios a una ley de inteligencia artificial que se basaban, en esencia, en que “la ley no puede seguir el veloz ritmo de desarrollo de la tecnología o los modelos comerciales”⁶⁴. El mismo autor advierte que dicha aprehensión se morigera cuando el desafío de regular la IA se materializa en una legislación que sea tecnológicamente neutra. En ese contexto es que el actual Reglamento Europeo de Protección de los Datos Personales ha pasado a constituirse en una guía importante para la inteligencia artificial, al igual que los límites al tratamiento automatizado de datos y los derechos a la información de los afectados⁶⁵.

El reglamento ya mencionado ha sido complementado por una serie de directivas de la Comisión Europea que han ido abordando la regulación de aspectos específicos de la IA. Entre ellas, pueden mencionarse la directiva 85/374, que reguló la responsabilidad derivada de los daños ocasionados por los defectos de fabricación de robots y que, a corto plazo, requirió que el Parlamento Europeo dictara orientaciones más precisas para que el desarrollo de la tecnología robótica se oriente a complementar las capacidades humanas y no a sustituirlas considerando, además, que los seres humanos tengan en todo momento el control sobre las máquinas inteligentes⁶⁶. Además, el reglamento está complementado por la directiva 2002/58/CE del Parlamento Europeo y del Consejo que protege la vida privada y la confidencialidad de las comunicaciones, estableciendo condiciones para cualquier almacenamiento de datos personales y no personales en los equipos terminales y el acceso desde estos.

En el caso de los robots, el desarrollo de las normativas sobre inteligencia artificial ha impactado la disciplina jurídica, entre otros aspectos, al plantear la pregunta de si es posible considerar responsabilidades –como sujetos de derecho– respecto de dichas máquinas inteligentes cuyas funciones se asemejan cada vez más a la forma en que actuaría una persona⁶⁷.

Miguel Ángel Presno Linera ha sostenido al respecto:

“mientras no cambien jurídicamente las cosas, esa titularidad de derechos por parte de las personas físicas se mantendría a lo largo de la vida también en el caso que asistamos, en un futuro más o menos pró-

⁶⁴ NEMITZ (2021) p. 135.

⁶⁵ *Op. cit.* p. 137.

⁶⁶ PARLAMENTO EUROPEO (2017).

⁶⁷ PRESNO (2023) p. 114 y ss.

ximo, a un importante desarrollo de la corriente transhumanista que aboga por conseguir una potente medicina voluntaria o de mejoramiento, que supere las facetas curativas o paliativas, a partir de la farmacología y la genética, y que consiga no sólo la eliminación de genes defectuosos sino que también la creación de genes artificiales capaces de aportar a las células funciones hoy inexistentes”⁶⁸.

En este sentido, parece no existir duda de que las personas “ciborgs”, es decir, los seres humanos con compuestos cibernéticos incorporados a los elementos orgánicos, no dejan de ser personas y, por ende, titulares de derechos fundamentales⁶⁹.

Ahora bien, y como se ha señalado en el primer capítulo de este estudio, la IA puede ayudar a las personas a desenvolverse y crecer en muchos ámbitos de su vida, pero sin perder de vista los riesgos que conlleva su utilización indebida y que terminan afectando los derechos fundamentales.

De allí que merece destacarse que el primer artículo de la nueva Ley de Inteligencia Artificial de la Unión Europea esté centrado en el ser humano:

“El objetivo del presente Reglamento es mejorar el funcionamiento del mercado interior y promover la adopción de una inteligencia artificial (IA) *centrada en el ser humano* y fiable, garantizando al mismo tiempo un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales consagrados en la Carta, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente, frente a los efectos perjudiciales de los sistemas de IA (en lo sucesivo, ‘sistemas de IA’) en la Unión así como prestar apoyo a la innovación” (El destacado es nuestro).

Entre los derechos fundamentales que, como ha dicho el Tribunal Constitucional de Chile, tienen una vinculación más estrecha con la dignidad humana se encuentra la privacidad⁷⁰. En relación con este derecho, debe recordarse que su elemento fundamental consiste en contar con el consentimiento del titular del mismo para revelar datos o información que, de otra forma, solo puede ser conocida por ese mismo titular. En este sentido, el Reglamento de Protección de Datos Personales de la Unión Europea define el consentimiento del interesado como:

“toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, mediante una declaración o

⁶⁸ PRESNO (2023) p. 113.

⁶⁹ *Op. cit.* p. 114.

⁷⁰ TRIBUNAL CONSTITUCIONAL (2006) rol 521, cc. 18-22.

una clara acción afirmativa, el tratamiento de datos personales que le conciernen” (art. 4 n.º 11).

Como puede advertirse, un primer desafío para la adecuada protección del derecho a la privacidad tiene que ver con la educación para el uso de la inteligencia artificial que permita dimensionar el alcance de la autorización que cada uno presta para el tratamiento de datos en bancos automatizados y basados en algoritmos.

La experiencia europea ha develado que la prestación del consentimiento, por parte del titular de los datos personales, no basta para evitar la vulneración de la privacidad. En efecto, ha quedado demostrado que el mero consentimiento no ha resultado suficiente para evitar usos indebidos de los datos que van más allá de la autorización que ha sido concedida por el titular a quienes pertenecen.

Lorenzo Cotino Hueso ha señalado, en este sentido:

“con los sistemas de inteligencia artificial y decisiones automatizadas es muy difícil consentir respecto de unas finalidades de uso de los datos que por lo general ni se conocen, ni se sospechan; ni se puede consentir respecto de unos algoritmos que se utilizarán, también desconocidos”⁷¹.

De esta forma, por ejemplo, cada vez que al entrar a un determinado sitio web se acepta la “política de *cookies*”, no se adquiere conciencia de que ciertos datos personales como la dirección IP y la geolocalización están siendo entregadas a un enorme procesador de datos que, entre otras acciones, podrá constituir un perfil de cada uno para incidir en sus preferencias y libertad de elegir. De allí que, desde la experiencia europea en el uso y tratamiento de datos personales se recomiende borrar, periódicamente, el historial de búsquedas que puede ser utilizado para fines impensados por el titular del derecho.

Además, la Ley de Inteligencia Artificial Europea, impone la obligación a los usuarios de IA de alto riesgo de llevar a cabo una evaluación de impacto relativa a la protección de datos que les impone el art. 35 del Reglamento de Protección de Datos Personales, cuando corresponda.

La falta de previsión en este aspecto puede terminar en que el sistema de IA construya un perfil de la persona del todo ajeno a su personalidad que conducirá a bombardearla con información que le resulta ajena e inconveniente o, lo que es peor, que favorezca la construcción de sesgos (“bias”) que, incluso, puedan impactar en su relación con las autoridades públicas. En otras palabras, debe tenerse especial precaución frente al riesgo de que toda la in-

⁷¹ COTINO (2017) p. 145.

formación que se entrega sea utilizada algorítmicamente “y nos deje desnudos frente a las entidades privadas y las instituciones públicas que puedan acceder a ella”⁷². En definitiva, y como ha advertido el Consejo de Europa esta utilización de los datos para construir perfiles impensados de las personas puede terminar afectando el derecho a la autodeterminación informativa⁷³.

Del mismo modo, la aplicación de los sistemas de inteligencia artificial destinados a la identificación biométrica remota de las personas físicas puede dar lugar a resultados sesgados y a consecuencias discriminatorias cuando tienen que ver con la edad, la etnia, el sexo o la discapacidad. Por ello, se sugiere considerar que estos sistemas de identificación conllevan un alto riesgo –tal y como lo concibe la nueva Ley de Inteligencia Artificial Europea– por lo que exigen la aplicación de requisitos específicos referentes a la capacidad de registro y la vigilancia humana a los mismos. No debe olvidarse que se ha detectado que un sistema de IA puede ser capaz de detectar o deducir las emociones o las intenciones de personas físicas a partir de sus datos biométricos⁷⁴.

Por otro lado, también la práctica europea de protección de los datos personales ha permitido constatar que los sistemas de inteligencia artificial pueden desdibujar la característica de “datos personales” protegidos por el Reglamento Europeo de Protección de Datos Personales impidiendo que puedan aplicarse sus disposiciones en defensa del derecho a la privacidad. Así, Lorenzo Cotino Hueso, ha llamado la atención sobre el hecho:

“[que] si los macrodatos no son datos de personas concretas, identificadas o identificables, no se aplica la legislación sobre protección de datos. Pues bien, una vía para escapar a la aplicación del exigente régimen de protección de datos es la anonimización, esto es, desvincular la información de su titular, por lo que deja de ser dato personal”⁷⁵.

La “anonimización” no debe confundirse con la “seudonimización”, que es definida por el mismo reglamento como:

“el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado *sin utilizar información adicional*, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable” (art. 4 n.º 5). (El destacado es nuestro).

⁷² PRESNO (2023) p. 40.

⁷³ *Op. cit.* p. 41.

⁷⁴ PRESNO (2023) p. 45.

⁷⁵ COTINO (2017) p. 146.

Laura Gómez advierte aquí, también, un riesgo desde el punto de vista del derecho a la privacidad, pues estima que el reglamento “parece orillar este espinoso asunto” que, en España, al menos, ha tenido una salida más eficaz a través de la Ley Orgánica sobre Protección de Datos Personales y Garantía de los Derechos Digitales (Ley 3/2018, de 5 de diciembre) evitando la reidentificación en el ámbito del tratamiento de los datos personales de salud y considerando como una infracción muy grave “la reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados”⁷⁶.

De la misma forma, cobra importancia, en estos casos, el respeto por parte de las empresas que se dedican al tratamiento de los datos personales utilizando sistemas de inteligencia artificial, del principio de “responsabilidad demostrada o *accountability*”, que busca que los mandatos legales sobre el tratamiento de los datos personales sean una realidad verificable y redunden en beneficio de los derechos de las personas, lo cual se podrá lograr mediante la implementación de mecanismos y protocolos internos de seguridad y control para el manejo de los datos eficientes⁷⁷. En otras palabras, hay aquí importantes desafíos para las empresas desde el punto de vista del *compliance*.

Un último alcance digno de relevar a partir del aporte que ha significado el Reglamento para la Protección de los Datos Personales de la Unión Europea tiene que ver con el ámbito de aplicación de su normativa. Su art. 3.1 señala que esta se aplicará:

“al tratamiento de datos personales en el contexto de las actividades del establecimiento de un responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no”.

Probablemente, alguien podría sostener que este precepto es una simple aplicación del amplio movimiento y circulación de datos en la Unión Europea que el reglamento considera entre sus fundamentos. Sin embargo, se trata de una visión que resulta más acorde con los espacios virtuales –más que físicos– propios de esta era globalizada, por lo que debiera tenerse en cuenta por las legislaciones internas de nuestros Estados a la hora de adecuar las regulaciones actuales a los tiempos que se viven, tal y como propone Andrea Martínez analizando la regulación colombiana sobre inteligencia artificial⁷⁸.

⁷⁶ GÓMEZ (2022) p. 103.

⁷⁷ MARTÍNEZ (2019) p. 15.

⁷⁸ *Op. cit.*

III. LECCIONES PARA CHILE Y CONCLUSIONES

Si la inteligencia artificial ha llegado para quedarse resulta necesario potenciar sus ventajas y minimizar sus riesgos frente a lo cual el derecho tiene grandes desafíos.

Como se ha señalado en esta investigación, en Chile se tramita, desde el año 2020, un proyecto de ley sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías. Se trata de un avance significativo, desde el punto de vista de los derechos de la personalidad, que concreta el mandato conferido por la Ley n.º 21383 que modificó el art. 19 n.º 1 de la Constitución Política. Este proyecto de ley apunta a regular la utilización de sistemas de inteligencia artificial, sobre todo, en el área de la medicina, para servir el objetivo de mejorar la condición física y mental de las personas.

Los avances producidos en Europa a partir de las diversas directivas como del Reglamento de Protección de Datos Personales y, finalmente, de la nueva Ley de Inteligencia Artificial de la Unión Europea, como los problemas que ya ha evidenciado su aplicación, permiten extraer varias lecciones útiles para nuestro país en orden a contar, en un futuro no muy lejano, con una ley que regule la aplicación de los diversos sistemas de inteligencia artificial.

Los principios que, a partir de la experiencia europea, podemos relevar, sobre todo, desde el punto de vista de la protección del derecho a la privacidad, serían los siguientes:

1. El principio de legalidad: la regulación de los sistemas de IA que operan en Chile como el sistema de responsabilidades y sanciones debe ser materia de ley sobre la base de lo dispuesto por el art. 19 n.º 26.º de la Constitución Política.
2. El principio rector de toda regulación, en materia de IA, debe ser la promoción de la persona y la defensa de sus derechos fundamentales, con mayor razón, cuando se trata de aquellos que, como la privacidad, tienen una estrecha conexión con el valor de la dignidad humana.
3. El principio de la educación digital destinado a que los usuarios se familiaricen con la dinámica de los sistemas de IA comprendiendo plenamente el alcance y los efectos del uso y tratamiento de datos que ellos realizan.
4. En el mismo sentido anterior, la consagración del principio del consentimiento previo, informado, útil e integral parece de la mayor relevancia de cara a la prevención de perfiles que anulen la autodetermi

nación informativa, de los sesgos y de la utilización de los datos más allá del ámbito del consentimiento entregado⁷⁹.

5. El principio de precaución en el sentido de que los sistemas de IA deben estar sometidos a una permanente evaluación de los algoritmos y mecanismos de cruce de información de datos para evitar efectos indeseados desde el punto de vista de los derechos de las personas. Para estos efectos, parece útil el mecanismo de pruebas anticipadas a la hora de implementar nuevas técnicas y soportes como ha ocurrido con la industria cosmética que utilizaba insumos provenientes de animales.
6. El principio de la responsabilidad demostrada o *accountability digital* que obliga a las empresas dedicadas al uso y tratamiento de datos a una revisión permanente de sus protocolos y técnicas unido a la inserción de esta responsabilidad en los mecanismos de *compliance* implementados por dichas empresas.
7. El principio de redefinición permanente del concepto de “datos personales” y de “datos sensibles” que hoy se contiene en la Ley n.º 19628 con el objetivo de que su tratamiento no los convierta en datos anonimizados ajenos a toda regulación legal.
8. El principio de sanción “ejemplar” que apunte a la eficacia de aquellas que se impongan a quienes realicen un uso indebido de los datos de forma de producir la efectiva inhibición de malas prácticas futuras a la que se aspira.
9. El principio de tecnificación que lleve a considerar la creación de una agencia especializada en la asesoría y control de los sistemas de inteligencia artificial que operan en nuestro país con adecuadas potestades regulatorias.
10. El principio de extraterritorialidad que permita sancionar a aquellas empresas que, como Google o Facebook, operan en espacios virtuales tratando datos cuyos efectos no necesariamente se producen en nuestro país, pero que tienen un claro principio de ejecución en él.

A diferencia de la frase que encabeza este artículo, no pareciera que estemos condenados a vivir el “fin de la privacidad” cuando la experiencia europea entrega una serie de lecciones y sugerencias que podemos empezar a adoptar para que las normas constitucionales y los tratados de derechos humanos

⁷⁹ Una norma como el texto propuesto en el art. 5.º del proyecto de ley sobre neuroderechos, por la Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación del Senado, en el sentido que: “los formularios a través de los que se solicite el consentimiento, contendrán la información de acuerdo a la evidencia disponible sobre los posibles efectos de la neurotecnología respectiva y, cuando corresponda, respecto de las normas de privacidad de datos neuronales personales” puede ser un buen ejemplo.

que resguardan este ámbito de la personalidad puedan seguir siendo eficaces en la era de la inteligencia artificial.

BIBLIOGRAFÍA

- BERNAL PULIDO, Carlos (2022): “Derechos fundamentales e inteligencia artificial”, *I-CON* n.º 20.
- BRAVO, Loreto y BRAVO, Mauricio (2023): *30 Miradas: inteligencia artificial y educación de futuro* (Santiago, Universidad del Desarrollo).
- CÁCERES, Enrique (2022): “La inteligencia artificial aplicada al derecho como una nueva rama de la teoría jurídica”, *Anales de la Cátedra Francisco Suárez*, n.º 57.
- CASTELLANOS CLARAMUNT, Jorge y MONTERO CARO, María Dolores (2020): “Perspectivas constitucionales de las garantías de aplicación de la inteligencia artificial: la ineludible protección de los derechos fundamentales”, *Ius et Ciencia* vol. 6 n.º 2 (Editorial Jurídica de Sevilla).
- CASTILLO-CÓRDOVA, Luis (2008): “Justificación y significación de los derechos constitucionales implícitos”, *Gaceta Constitucional: Jurisprudencia de Observancia Obligatoria para Abogados y Jueces* n.º 5 (Universidad de Piura).
- COCA PAYERAS, Miguel (2023): “Las iniciativas de la Unión Europea sobre Inteligencia Artificial: De la persona electrónica, al difícil equilibrio entre la necesidad de impulsarla y evitar sus riesgos”, *Revista de Derecho Civil* vol. x n.º 2, especial.
- CONTRERAS V., Pablo (2011): “¿Derechos implícitos? Notas sobre la identificación de normas de derecho fundamental”, en Núñez Leiva, J. Ignacio (coord.), *Nuevas perspectivas de derecho público* (Santiago: Editorial Librotecnia).
- COTINO HUESO, Lorenzo (2017): “Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales”, *Dilemata* año 9 n.º 24.
- GANASCIA, JEAN-GABRIEL (2018): “Inteligencia artificial: entre el mito y la realidad”. Disponible en <https://courier.unesco.org/es/articulos/inteligencia-artificial-entre-el-mito-y-la-realidad> [fecha de consulta: 7 de marzo de 2024].
- GÓMEZ ABEJA, Laura (2022): Inteligencia artificial y derechos fundamentales, en Llano Alonso, Fernando H. (dir.), *Inteligencia artificial y filosofía del derecho* (Madrid, Ediciones Laborum).
- GRANERO, Horacio Roberto (2022): “Derechos y garantías concretas frente al uso de inteligencia artificial y decisiones automatizadas, especialmente en el ámbito judicial y de aplicación de la ley”, en Cotino Hueso, Lorenzo (dir.), *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas* (Pamplona: Editorial Thomson Reuters Aranzadi).
- HERRERA, Román (2023): “El paradigma de los Derechos Humanos como base para una regulación de la inteligencia artificial global”, *Universos Jurídicos* año 11 n.º 21.

- KING, Jennifer; MEINHARDT, Caroline (2024): *Rethinking Privacy in the AI Era. Policy Provocations for a Data-Centric World*. Disponible en <https://hai.stanford.edu/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world#:~:text=February%202022%2C%202024-,Rethinking%20Privacy%20in%20the%20AI%20Era%3A%20Policy,for%20a%20Data%2DCentric%20World&text=This%20white%20paper%20explores%20the,harms%20in%20an%20AI%20era> [fecha de consulta: 6 de marzo de 2024].
- LÓPEZ-SILVA, Pablo y MADRID, Raúl (2021): “Sobre la conveniencia de incluir los neuroderechos en la Constitución o en la ley”, *Revista Chilena de Derecho y Tecnología* vol. 10 n.º 1.
- MASBERNAT, Patricio y PASQUINO, Vincenzo (2023): “Inteligencia artificial y su problemático impacto en el derecho”, *Revista de Educación y Derecho* n.º 28.
- MARTÍNEZ, Goretty (2012): “La inteligencia artificial y su aplicación al campo del derecho”, *Alegatos*, n.º 82.
- MARTÍNEZ DEVIA, Andrea (2019): “La inteligencia artificial, el Big Data y la Era Digital: ¿Una amenaza para los datos personales?”, *Revista la Propiedad Inmaterial* n.º 27.
- MORANDÍN-AHUERMA, Fabio (2023): *Principios normativos para una ética de la inteligencia artificial* (Puebla, Universidad Autónoma de Puebla).
- NEMITZ, Paul (2021): “La democracia en la era de la inteligencia artificial”, *Nueva Sociedad* n.º 294 (julio-agosto).
- OTERO PARGA, Milagros (2023): “¿Puede la inteligencia artificial sustituir a la mente humana? Implicaciones de la IA en los derechos fundamentales y en la ética”, *Anales de la Cátedra Francisco Suárez* n.º 57.
- PRESNO LINERA, Miguel Ángel (2023): *Derechos fundamentales e inteligencia artificial* (Madrid: Editorial Marcial Pons).
- PRIETO SANCHÍS, Luis (2013): *El constitucionalismo de los derechos* (Madrid, Editorial Trotta).
- REBOLLO DELGADO, Lucrecio (2023): *Inteligencia artificial y derechos fundamentales* (Madrid, Editorial Dykinson).
- SALLES, Arleen (2018): “Neurociencia y cambio moral: Expectativas y límites”, en García Marzá, Domingo *et al.*, *Ética y filosofía política. Homenaje a Adela Cortina* (Madrid, Editorial Tecnos).
- TÜRK, Volker (2023): “Comentario de Volker Türk, Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre avances en inteligencia artificial. Disponible en www.ohchr.org/es/statements/2023/02/comment-un-high-commissioner-human-rights-volker-turk-advances-artificial [fecha de consulta: 7 de marzo de 2024].
- VIVANCO MARTÍNEZ, Angela (2006): *Curso de derecho constitucional*, tomo II (Santiago, Ediciones Universidad Católica de Chile).

Jurisprudencia

SUPERIOR COURT OF CALIFORNIA (2024): Elon Musk vs. Samuel Altman; Gregory Brockman; OpenAI. Disponible en www.courthousenews.com/wp-content/uploads/2024/02/musk-v-altman-openai-complaint-sf.pdf [fecha de consulta: 10 de febrero de 2024].

TRIBUNAL CONSTITUCIONAL DE CHILE (2006): sentencia de 1/06/2006, rol 52. Disponible en https://tramitacion.tcchile.cl/tc/do_search?proc=1&idCausa=3137&buscador=true [fecha de consulta: 10 de mayo de 2024].

Normas

PARLAMENTO EUROPEO (2000): Carta de Derechos Fundamentales de la Unión Europea. Disponible en www.europarl.europa.eu/charter/pdf/text_es.pdf [fecha de consulta: 15 de mayo de 2024].

PARLAMENTO EUROPEO (2017): Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho Civil sobre Robótica. Disponible en chrome-extension://efaidnbmninnbpcjpcgclclefindmkaj/https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.pdf [fecha de consulta: 15 de mayo de 2024].

PARLAMENTO EUROPEO (2022): Resolución del Parlamento Europeo sobre la IA en la era digital. Disponible en www.europarl.europa.eu/doceo/document/TA-9-2022-0140_ES.html [fecha de consulta: 15 de mayo de 2024].

Proyecto de ley: Sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías. *Boletín* 13828-19. Disponible en www.senado.cl/appsenado/templates/tramitacion/index.php [fecha de consulta: 15 de mayo de 2024].

Documentos

AMNISTÍA INTERNACIONAL (2019a): “La vigilancia generalizada de Facebook y Google representa un peligro sin precedente para los derechos humanos”. Disponible en www.amnesty.org/es/latest/press-release/2019/11/google-facebook-surveillance-privacy/ [fecha de consulta: 10 de febrero de 2024].

AMNISTÍA INTERNACIONAL (2019b): “Surveillance giants: How the business model of Google and Facebook threatens human rights”. Disponible en www.amnesty.org/en/documents/pol30/1404/2019/en/ [fecha de consulta: 10 de febrero de 2024].

BBC MUNDO (2018): “5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US\$37.000 millones en un día”. Disponible en www.bbc.com/mundo/noticias-43472797 [fecha de consulta: 10 de febrero de 2024].

BLOOMBERG (2022): “Meta acepta pagar US\$725 millones por el caso de Cambridge Analytica”. Disponible en www.df.cl/empresas/multinacionales/meta-accepta-

- pagar-us-725-millones-por-el-escandalo-de-cambridge-analytica [fecha de consulta: 10 de febrero de 2024].
- CEPAL (2019): “Revolución tecnológica: desafíos y oportunidades para la industria, el empleo, la igualdad de género y el desarrollo social en América Latina y el Caribe. Disponible en <https://foroalc2030.cepal.org/2019/es/programa/revolucion-tecnologica-desafios-oportunidades-la-industria-empleo-la-igualdad-genero> [fecha de consulta: 5 de marzo de 2024].
- CNN CHILE (2019): “Sernac presenta demanda colectiva contra Correos de Chile por filtración de datos de tarjeta de crédito de consumidores”. Disponible en www.cnnchile.com/pais/sernac-demanda-colectiva-correos-de-chile-filtracion-datos_20191009/ [fecha de consulta: 10 de febrero de 2024].
- COMMITTEE ON ARTIFICIAL INTELLIGENCE (2023): “Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law”. Disponible en www.coe.int/en/web/cm/-/draft-framework-convention-on-artificial-intelligence-human-rights-democracy-and-the-rule-of-law [fecha de consulta: 7 de marzo de 2024].
- DATASCIENTEST (2022): “Inteligencia artificial: definición, historia, usos, peligros”. Disponible en <https://datascientest.com/es/inteligencia-artificiade definicion#:~:text=En%201952%2C%20Arthur%20Samuel%20cre%C3%B3,de%20John%20McCarthy%20en%201956> [fecha de consulta 7 de marzo de 2024].
- Diario Financiero* (2019): “British Airways, multada con más de 200 millones de euros por el robo de datos de sus clientes.” Disponible en www.df.cl/internacional/multinacionales/british-airways-multada-con-mas-de-200-millones-de-euros-por-el-robo-de [fecha de consulta: 10 de febrero de 2024].
- El Mostrador* (2022): “Un 50% de los datos filtrados de las empresas son datos de consumidores”. Disponible en www.elmostrador.cl/agenda-pais/2022/08/04/50-de-los-datos-filtrados-de-las-empresas-son-datos-de-consumidores/ [fecha de consulta: 10 de febrero de 2024].
- IBM (2023): “Cost of a Data Breach Report 2023”. Disponible en www.ibm.com/reports/data-breach [fecha de consulta: 10 de febrero de 2024].
- MAULÉN, Cristián (2022): *El ciudadano y su privacidad. Protección y privacidad de datos*. Disponible en https://media-front.elmostrador.cl/2022/11/Sondeo-El-Ciudadano-y-su-Privacidad-2022_01-2.pdf [fecha de consulta: 10 de febrero de 2024].
- MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA (2019): “Los principios de Inteligencia Artificial de la OCDE”. Disponible en <https://datos.gob.es/es/blog/los-principios-de-inteligencia-artificial-de-la-ocde> [fecha de consulta: 12 de marzo de 2024].
- ORGANIZACIÓN DE LAS NACIONES UNIDAS PARA LA EDUCACIÓN, LA CIENCIA Y LA CULTURA (2021): Resolución 40 C/37. Disponible en www.un.org/unispal/wp-content/uploads/2019/12/UNESCO40C.91s_221119.pdf [fecha de consulta: 27 de junio de 2024].

- SEGOVIA, Macarena y SEPÚLVEDA, Nicolás (2022): “Hackeo a correos del Ministerio de Justicia expone datos sensibles de menores del Sename y de casos de familia”. Disponible en www.ciperchile.cl/2022/09/30/hackeo-a-correos-del-ministerio-de-justicia-expone-datos-sensibles-de-menores-del-sename-y-de-casos-de-familia/ [fecha de consulta: 10 de febrero de 2024].
- SOLON, Olivia and FARIVAR, Cyrus (2019): “Mark Zuckerberg aprovechó los datos de los usuarios de Facebook para luchar contra rivales y ayudar a sus amigos, según muestran documentos filtrados”. Disponible en www.nbcnews.com/tech/social-media/mark-zuckerberg-leveraged-facebook-user-data-fight-rivals-help-friends-n994706 [fecha de consulta: 10 de febrero de 2024].
- UNESCO (2023): *Comentario de Volker Türk, Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre avances en inteligencia artificial*. Disponible en www.ohchr.org/es/statements/2023/02/comment-un-high-commissioner-human-rights-volker-turk-advances-artificial [fecha de consulta: 7 de marzo de 2024].
- UNESCO (2024): *Systematic Prejudices. An Investigation into Bias Against Women and Girls in Large Language Models*. Disponible en <https://ircai.org/project/challenging-systematic-prejudices/> [fecha de consulta: 10 de febrero de 2024].
- VERA V., Vicente (2019): “Estudio asegura que Chile recibió más de 23.500 millones de intentos de ciberataques en un trimestre”. Disponible en www.df.cl/mercados/banca-fintech/estudio-asegura-que-chile-recibio-mas-de-23-500-millones-de-intentos-de [fecha de consulta: 10 de febrero de 2024].