DOCUMENTOS DE TRABAJO
ESCUELA DE GOBIERNO

MÁSTER PROPIO EN PROMOCIÓN Y DEFENSA
INTERNACIONAL DE LOS DERECHOS HUMANOS

El impacto de la Inteligencia Artificial en la protección de datos personales y el acceso a la información

Alumno:
Julián Ariel Madrid Moreno

Profesora Tutora:
Dra. Paula López Zamora

2022/2023
Convocatoria extraordinaria

DT-EG 8/2024

Edita:
Escuela de Gobierno
Universidad Complutense de Madrid

Colección Trabajos Fin de Máster

Autor: Julián Ariel Madrid Moreno

ISSN: 2952-0169

https://www.ucm.es/eg

Madrid, 2024

UNIVERSIDAD COMPLUTENSE MADRID

ESCUELA DE GOBIERNO
UNIVERSIDAD COMPLUTENSE DE MADRID

Máster propio en promoción y defensa internacional de los derechos humanos

El impacto de la Inteligencia Artificial en la protección de datos personales y el acceso a la información

Alumno:

JULIÁN ARIEL MADRID MORENO

Profesora Tutora:
Dra. Paula López Zamora

2022/2023
Convocatoria extraordinaria

ÍNDICE

I. INTRODUCCIÓN.

Hace unos años, se demuestra un avance sin precedentes en el uso de las tecnologías en los hogares. El encierro durante la pandemia, la revolución tecnológica 4.0, acompañado del uso de sistemas automatizados son algunas de las razones que se pueden mencionar.

Las personas de todo el mundo, cada vez con mayor intensidad, se encuentran dependidas de las tecnologías para el quehacer diario de sus vidas. Realizar compras, recibir y ofrecer bienes y servicios, comunicarse de manera instantánea a través de las redes sociales, son utilizados de forma más cotidiana y necesaria para el desarrollo de las sociedades actuales.

Cada vez más, el acceso a la información es clave para agilizar los procesos antes mencionados, facilitando las tomas de decisiones y mejorando la calidad de vida de las personas. Ello en razón de que, con la información al alcance de la mano, las personas pueden acceder a todo tipo de servicios de la información para mejorar sus decisiones a la hora de mejorar la calidad de vida en todos sus aspectos.

La innovación tecnológica ha estado en constante evolución a lo largo de la historia debido a una serie de razones fundamentales que impulsan el progreso y el desarrollo en el mundo. Estas razones abarcan tanto aspectos económicos como sociales, y su interacción ha dado lugar a avances significativos que han transformado la manera en que vivimos, trabajamos y nos comunicamos.

Y es que, un periodo de transición muy corto, en apenas 30 años, se han fraguado innovaciones tecnológicas, de enorme trascendencia, asociadas a los sistemas de gestión de la información. El desarrollo de Internet, las redes sociales, el mundo móvil, el teléfono inteligente, la *tablet*, las tecnologías *cloud*, las tecnologías de interacción persona máquina con reconocimiento de habla, caras, expresiones, el uso del "Big data", la inteligencia artificial, la robótica o la impresión 3D, se encuentran entre los ejemplos más destacados, pero no son los únicos[1].

Todas estas innovaciones tecnológicas, que se engloban bajo el fenómeno de la "digitalización", al actuar de forma conjunta y combinada, están produciendo un

[1] J. L. Goñi Sein, "Innovaciones Tecnológicas, Inteligencia Artificial Y Derechos Humanos En El Trabajo", *Doc. Labor*, núm. 117-Año 2019-Vol. I, Universidad Pública de Navarra, P. 58.

repentino cambio en la realidad productiva, una auténtica revolución, que ha sido calificada como una verdadera "disrupción", en cuanto que vienen a alterar radialmente la forma en que la gente vive y trabaja. Tales innovaciones tecnológicas tienen como base la obtención, gestión y procesamiento de la información. El elemento clave de esta revolución tecnológica es la información, la recopilación ingente de datos, el Big data, y el análisis y tratamiento de los datos, basado en la inteligencia artificial. Y ello se proyecta en todos los órdenes de la vida social[2].

En lo que interesa para el presente trabajo, la Inteligencia Artificial (IA) es una de las tecnologías más disruptivas y transformadoras que está siendo ampliamente utilizada en distintas áreas, desde la atención sanitaria hasta la educación y el comercio electrónico. Esta tecnología tiene la capacidad de mejorar la eficiencia, la productividad y la calidad de vida de las personas, pero también plantea importantes desafíos en términos de protección de los derechos humanos, especialmente en lo que respecta a la protección de datos personales y el acceso a la información.

La inteligencia artificial puede desempeñar un papel fundamental para mejorar el acceso a la información en el mundo digital. Pueden ayudar a reducir la brecha digital, dando a las personas acceso a información de manera accesible y garantizar servicios más eficaces. Los ciudadanos pueden acceder a la información y a los servicios de forma casi instantánea. La digitalización de los servicios supone una mejora, además, para la transparencia y la accesibilidad[3].

También, el vertiginoso desarrollo tecnológico ha permitido que las organizaciones utilicen cada vez más técnicas como la inteligencia artificial, a fin de hacer más eficientes los procesos y la toma de decisiones. Los usos de la IA son tan variados que pueden ser incorporados en sectores desde la agricultura hasta medios de transporte, por lo que tienen una incidencia en todos los espacios de la sociedad. Los usuarios digitales también encuentran en la IA una oportunidad para el procesamiento de información, por ejemplo, relativa a su estado de salud, preferencias comerciales, o simplemente para buscar información en el ciberespacio. Estos beneficios son posibles a

[2] *Ibid*., p. 58
[3] Naciones Unidas, *Inteligencia artificial, gobernanza electrónica y acceso a la información,* ONU, 2022, URL: https://www.un.org/es/observances/information-access-day

partir del análisis masivo y sistemático de la información, que incluye casi siempre, datos personales que identifican o hacen identificables a los humanos[4].

Sin embargo, estos avances también plantean cuestiones sobre los derechos fundamentales y su compatibilidad con el uso de la inteligencia artificial, dado que la inteligencia artificial, como se analizará más adelante, se nutre de datos generales y datos personales. En ese sentido se plantea los interrogantes de cómo protegemos la intimidad de los mismos, si se puede determinar a qué información accedemos y en qué principios jurídicos internacionales se basa[5].

Derivado de lo anterior, existe una constante preocupación respecto del uso masivo de sistemas de IA que para su funcionamiento requieran de información que identifique o haga identificable a la persona detrás del dato. Esto frente a prácticas como los tratamientos indebidos de datos (falta de cumplimiento normativo o de incorporación de límites éticos), la falta de medidas de seguridad o errores en el diseño de la técnica, que podrían traer consigo la violación de derechos humanos: desde el derecho a la vida, el derecho a la no discriminación, el derecho a la salud, hasta el derecho a la privacidad y a la protección de datos personales, por enunciar algunos[6].

Para algunos, la inteligencia artificial puede ser de gran ayuda para las sociedades a superar algunos de los mayores retos de nuestro tiempo. Para otros, en cambio, las tecnologías de IA también pueden tener efectos nocivos e incluso catastróficos, cuando se emplean sin prestar la debida atención a su capacidad de vulnerar los derechos humanos[7].

En ese sentido, algunos autores consideran que mientras mayor sea el riesgo para los derechos humanos, más estrictos deben ser los requisitos legales para el uso de la tecnología de IA. Así por ejemplo, como parte de su labor en materia de tecnología y derechos humanos, la Oficina de Derechos Humanos de la ONU publicó un informe en el que se analiza cómo la IA -incluidas la elaboración automática de perfiles, la toma de

[4] O. A. Mendoza Enríquez, "El derecho de protección de datos personales en los sistemas de inteligencia artificial", *Revista Del Instituto De Ciencias Jurídicas De Puebla*, Vol. 15, No. 48, México, diciembre 2021, p. 180.
[5] Naciones Unidas, *Inteligencia artificial, gobernanza electrónica y acceso a la información,* UN, 2022.
[6] O. A. Mendoza Enríquez, "El derecho de protección de datos personales en los sistemas de inteligencia artificial", *Revista Del Instituto De Ciencias Jurídicas De Puebla*, Vol. 15, No. 48, México, diciembre 2021, p. 180.
[7] Naciones Unidas, *Los riesgos de la inteligencia artificial para la privacidad exigen medidas urgentes – Bachelet*, UN, 2021, URL: https://www.ohchr.org/es/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet

decisiones y otras tecnologías de aprendizaje para las máquinas- afecta al derecho a la intimidad y a otros derechos, incluidos los relativos a la salud, la educación, la libertad de movimiento, la libertad de reunión y asociación pacífica, y la libertad de expresión[8]

Algunas Organizaciones han propuesto medidas para contrarrestar los peligros de vulnerar la intimidad de la información en el uso de la IA. Sin embargo, es fundamental evaluar la efectividad de esta medida en relación con sus posibles impactos en los derechos humanos. Por lo tanto, es fundamental evaluar la efectividad de esta medida en relación con sus posibles impactos en los derechos humanos y establecer medidas para mitigar los posibles daños que pueda llegar a causar[9].

Por otro lado, cuando se está ante tratamientos de información que contienen datos personales a través de sistemas de inteligencia artificial, ya existe un marco normativo transversal de índole local y en algunos casos regional o internacional, centrado, sobre todo, en materia de protección de datos personales, por lo que resulta un desafío del derecho de protección de los datos personales en la IA, ya que no es del todo normativo[10]. Es decir, el marco normativo existente no aborda completamente los desafíos específicos que surgen con el uso de IA en relación con la protección de datos personales. Esto puede deberse a que la tecnología de IA está en constante evolución y puede superar las regulaciones existentes.

Como resultado, es posible que sea necesario adaptar y desarrollar nuevas regulaciones para garantizar que la privacidad y los derechos de las personas se protejan adecuadamente en el contexto de la IA. Esto implica que el derecho de protección de datos personales se enfrenta a un desafío en el ámbito de la IA, ya que el marco normativo actual puede no ser suficiente o completamente aplicable a esta tecnología en constante desarrollo.

Frente a este panorama, es menester aclarar que el derecho a la intimidad y el acceso a la información son derechos fundamentales y básicos en todas las sociedades democráticas. La intimidad se refiere al derecho de las personas a controlar su información personal y a protegerla de cualquier uso no autorizado, mientras que el

[8] *Idem.*
[9] Asamblea General, *A/HRC/51/17: El derecho a la privacidad en la era digital*, Naciones Unidas, 2022, recuperado en: https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age
[10] O. A. Mendoza Enríquez, "El derecho de protección de datos personales en los sistemas de inteligencia artificial", *Revista Del Instituto De Ciencias Jurídicas De Puebla*, Vol. 15, No. 48, México, diciembre 2021, pp. 180-181

acceso a la información se refiere al derecho de las personas a acceder a la información que les concierne y a la información de interés público. Ambos derechos entran en conflicto cuando no existe un control proporcional del uso de la información que almacena la IA.

Frente a esto, el problema jurídico que puede surgir con respecto a lo mencionado se relaciona con la necesidad de abordar adecuadamente las implicaciones legales y éticas de la inteligencia artificial en el contexto de la protección de datos y el acceso a la información.

En primer lugar, podría surgir la cuestión de cómo se están utilizando actualmente los datos personales en el desarrollo y la implementación de sistemas de IA. Esto podría plantear preocupaciones sobre la privacidad y la confidencialidad de los datos, así como sobre el consentimiento informado y el control que las personas tienen sobre sus propios datos. Además, existe la posibilidad de que la IA pueda generar perfiles o discriminación basados en datos personales sensibles, lo que podría perjudicar a los derechos humanos, como la discriminación y la exclusión. Por lo tanto, se debe considerar cómo se protegen los derechos fundamentales en el contexto de la IA y cómo se garantiza la igualdad y la no discriminación.

Asimismo, otro problema jurídico que puede surgir está relacionado con el acceso a la información y la transparencia. La IA puede involucrar algoritmos complejos que toman decisiones automatizadas, lo que puede dificultar la comprensión de cómo se toman esas decisiones y qué datos se utilizan para ello. Esto plantea interrogantes sobre la rendición de cuentas y la responsabilidad, así como sobre el acceso a la información necesaria para impugnar o cuestionar esas decisiones.

En resumen, el problema jurídico asociado al presente trabajo radica en abordar de manera efectiva las implicaciones legales y éticas de la IA en relación con la protección de datos personales y el acceso a la información, considerando cuestiones como la intimidad, la igualdad, la no discriminación o la transparencia.

Por las razones antes expuestas, este trabajo se enfoca en analizar el impacto de la inteligencia artificial en los derechos humanos, especialmente en la privacidad de los datos y el acceso a la información. La creciente aplicación de la inteligencia artificial en diversos ámbitos de la vida ha presentado desafíos significativos para la protección de los

derechos humanos. Se requiere profundizar en este tema para identificar los riesgos y desafíos que la inteligencia artificial representa en el ámbito de los derechos humanos.

Así, resulta relevante examinar si el marco legal de los derechos humanos, en particular en lo referente a la protección de datos personales, ofrece suficiente salvaguardia para la persona frente a las técnicas empleadas por la inteligencia artificial. El objetivo es alcanzar un equilibrio adecuado entre la innovación y la dignidad humana.

A continuación, se presentará al lector una visión conceptual de la inteligencia artificial. Además, se explorará cómo el derecho a la protección de datos personales se ha consolidado como un derecho humano, junto con un análisis del derecho a la intimidad y a la protección de datos personales en el contexto de la inteligencia artificial. Por último, se ofrecerán conclusiones relevantes sobre el tema.

La hipótesis que se plantea en este trabajo es que el uso de la inteligencia artificial puede amenazar la privacidad de los datos y el acceso a la información, lo que afecta negativamente la promoción y defensa de los derechos humanos. Por lo tanto, es necesario analizar cómo la inteligencia artificial puede poner en riesgo estos derechos y proponer soluciones para garantizar su protección.

La metodología que se empleará en este trabajo será una revisión bibliográfica exhaustiva de las principales fuentes de información sobre inteligencia artificial y derechos humanos, incluyendo normas y estándares internacionales, investigaciones recientes y estudios de casos relevantes. Además, se realizará un análisis crítico de los datos y se propondrán soluciones para abordar los desafíos identificados. El objetivo final es contribuir al debate sobre cómo la inteligencia artificial puede ser utilizada de manera responsable y respetando los derechos humanos.

II. CONCEPTOS FUNDAMENTALES SOBRE INTELIGENCIA ARTIFICIAL Y DERECHOS HUMANOS

La principal característica en el ámbito de los derechos humanos de la época contemporánea es el reconocimiento de que todos los seres humanos, por el simple hecho de serlo, son titulares de derechos fundamentales que la sociedad no puede arrebatarles legítimamente. Estos derechos no dependen de su reconocimiento por parte del Estado ni son concesiones otorgadas por él. Tampoco están condicionados por la nacionalidad de la persona o la cultura a la que pertenezca. Son derechos universales que corresponden a

todos los habitantes de la Tierra[11]. La expresión más notable de este gran logro se encuentra en el artículo 1 de la Declaración Universal de Derechos Humanos (ONU 1948) en que todos los seres humanos nacen libres e iguales en dignidad y derechos, dotados de razón y conciencia, y deben comportarse fraternalmente los unos con los otros[12].

En ese sentido los Derechos Humanos, que son universales, tienen trascendencia y gobiernan todos los aspectos de las personas. En este sentido, además, todos los Estados deben comprometerse al estricto respeto de los Derechos Humanos, y, sobre todo, a su garantía.

Sentadas estas premisas, hemos de avanzar y responder a la cuestión de cuál es la relevancia de la inteligencia artificial (IA) para los derechos humanos. Definir la IA no es una tarea sencilla, ya que el concepto de inteligencia en sí mismo no es del todo preciso. En términos coloquiales, se utiliza el término IA cuando una máquina es capaz de imitar las funciones cognitivas propias de la mente humana, como la creatividad, la sensibilidad, el aprendizaje, la comprensión, la percepción del entorno y el uso del lenguaje. Esta tecnología es una herramienta extraordinariamente poderosa que podría tener un efecto transformador e innovador en muchos aspectos de la vida cotidiana, desde el transporte y la fabricación hasta la atención médica y la educación[13].

Así, los Derechos Humanos tiene actualmente un compromiso de adaptar sus fines a las nuevas tecnologías. Hoy en día, todas las personas son dependientes de las nuevas tecnologías, adaptando a sus vidas cotidianas a la informática, a las redes sociales y a los datos informático. Por ello, con el avance y alcance sobre el acceso a la información surgen nuevas necesidades de las personas.

Su uso está en constante aumento en todos estos sectores, así como en el sistema de justicia, la policía y el ejército. La IA puede aumentar la eficiencia, generar nuevos conocimientos sobre enfermedades y acelerar el descubrimiento de medicamentos innovadores. La inteligencia artificial se utiliza ampliamente para crear recomendaciones personalizadas para los consumidores, basadas, por ejemplo, en sus búsquedas y compras anteriores u otros comportamientos en línea. La IA desempeña un papel crucial en el

[11] A. E. Grigore, "Derechos humanos e inteligencia artificial", *IUS ET SCIENTIA*, Vol. 8, Nº 1, marzo de 2022, pp. 165-175

[12] Naciones Unidas, "Declaración Universal de los Derechos Humanos", diciembre 1948, URL: https://www.un.org/es/about-us/universal-declaration-of-human-rights.

[13] A. E. Grigore, "Derechos humanos e inteligencia artificial", *IUS ET SCIENTIA*, Vol. 8, Nº 1, marzo de 2022, pp. 165-175.

comercio, optimizando productos, planificando inventarios, gestionando procesos logísticos, entre otros. El desarrollo de tecnologías inteligentes tiene un profundo impacto en la sociedad[14].

Un área en la que la IA ha demostrado su valía es en la atención médica. La capacidad de procesar y analizar grandes volúmenes de datos médicos ha abierto nuevas posibilidades para la detección temprana de enfermedades y la predicción de patrones de salud. Esta tecnología no solo acelera el proceso de diagnóstico, sino que también desempeña un papel crucial en la investigación de nuevos tratamientos y medicamentos. La capacidad de analizar datos a nivel molecular ha permitido el diseño de moléculas farmacéuticas de manera mucho más eficiente, acortando los tiempos de desarrollo y prueba.

Así tambien, el sistema de justicia y las fuerzas de seguridad también han incorporado la IA para mejorar la eficiencia y precisión en sus operaciones. Desde la detección de patrones delictivos hasta la identificación de sospechosos a través de análisis de imágenes, la IA ha fortalecido la capacidad de las fuerzas del orden para mantener la seguridad. Sin embargo, su implementación plantea cuestiones éticas y de privacidad que deben ser abordadas cuidadosamente para evitar posibles abusos y discriminación.

En última instancia, el desarrollo de tecnologías inteligentes ha redefinido la relación de las personas con la tecnología y ha acelerado la automatización en diversos campos. A medida que la IA continúa avanzando, es fundamental considerar su impacto en términos de empleo, igualdad y seguridad.

En los sentidos antes expuestos, el desarrollo de la IA se ha acelerado gracias a los incentivos tecnológicos y humanos actuales. Como se mencionó, existen avances significativos en tecnologías inteligentes en campos como la agricultura, la manufactura, la medicina, la educación, los vehículos autónomos y el entretenimiento. Además, las implicaciones de carácter social, económico, ético y legal que conlleva son temas de reflexión y debate en todo el mundo[15].

Pero su uso indebido, intencional o no, también puede dañar los derechos de las personas. Y es que la creciente presencia de la inteligencia artificial en diversas esferas de la sociedad ha abierto un intenso debate sobre la ética y la legalidad de su uso,

[14] *Idem.*
[15] *Idem.*

especialmente cuando se trata de situaciones donde los sistemas inteligentes pueden tener un impacto directo en los derechos y la seguridad de las personas.

Un ejemplo pertinente de esta problemática se presenta en el contexto de los vehículos autónomos. Imagina que un automóvil autónomo atropella a un peatón. La cuestión de la responsabilidad se vuelve compleja. ¿Debería recaer en el propietario del vehículo, quien podría argumentar que no estaba al mando en ese momento? O, por otro lado, ¿debería considerarse la responsabilidad del diseñador o programador de la inteligencia artificial que controla el automóvil? Este dilema pone de relieve la necesidad de establecer reglas claras y definir roles en situaciones donde la tecnología inteligente toma decisiones que afectan la vida de las personas.

Otro punto de debate, además de la responsabilidad directa, es sobre como los sistemas de IA también pueden amplificar prejuicios y discriminación inherentes a los datos con los que son entrenados. Verbigracia, si un algoritmo de contratación se entrena con datos históricos que reflejan sesgos de género o racial en las contrataciones previas, es muy probable que el sistema continúe reproduciendo estos patrones injustos al tomar decisiones. Esto pone de manifiesto la importancia de la equidad y la diversidad en la recopilación y selección de datos de entrenamiento, así como en la supervisión constante de los resultados generados por la IA.

La cuestión ética y legal se amplía aún más cuando se trata de sistemas de IA que aprenden de manera autónoma y toman decisiones sin intervención humana directa. En estos casos, ¿quién es responsable de las decisiones tomadas por el sistema? ¿Cómo se pueden establecer límites y salvaguardias para evitar consecuencias indeseadas? Estas preguntas plantean desafíos fundamentales para la regulación y el diseño responsable de sistemas inteligentes.

Otro ejemplo es el de experimentos en procesamiento automático del lenguaje, que muestran cómo los sistemas aprenden a asociar la palabra mujer con profesiones más cercanas a las humanidades y al hogar, mientras que a la palabra hombre, la relacionan con profesiones con un mayor componente matemático[16].

Es así como el potencial tanto positivo como negativo de la inteligencia artificial exige una reflexión profunda sobre su implementación y su impacto en la sociedad. La ética y la legalidad en la IA son cuestiones intrínsecamente entrelazadas que deben ser

[16] *Idem.*

abordadas con un enfoque multidisciplinario y colaborativo, involucrando a expertos en tecnología, ética, leyes y políticas públicas para garantizar que la innovación tecnológica avance de manera responsable y beneficiosa para todos.

Es por ello que, en el presente trabajo, a los fines de su comprensión se analizara algunos aspectos relevantes entre la Inteligencia Artificial y los Derechos Humanos. Luego, se desarrollará las implicancias que tiene las nuevas tecnologías para analizar como inciden los mismos sobre los Derechos Humanos. Su razón radica en comprender la magnitud y complejidad de la problemática planteada en la sociedad interconectada.

1. Tendencias y desafíos actuales en la intersección entre inteligencia artificial y derechos Humanos

El desarrollo expuesto en el apartado anterior justifica el creciente interés de algunas organizaciones internacionales en la complejidad de este tema. Una de ellas es la UNESCO, del cual ha aprobado el primer marco ético sobre inteligencia artificial. Este histórico documento establece valores y principios comunes que guiarán la construcción de la infraestructura jurídica necesaria para asegurar un desarrollo saludable de la inteligencia artificial[17].

Vemos así la importancia y relevancia creciente de abordar el tema de la inteligencia artificial. La iniciativa de la UNESCO al aprobar el primer marco ético sobre inteligencia artificial es un hito significativo. Este documento histórico establece valores y principios compartidos que servirán como base para la creación de una infraestructura legal sólida que garantice un desarrollo ético y beneficioso de la inteligencia artificial[18].

La inteligencia artificial está presente en todos los aspectos de nuestras vidas, facilitando nuestras rutinas diarias y logrando resultados destacables en campos especializados como la detección del cáncer y la creación de entornos inclusivos para personas con discapacidades. También tiene el potencial de abordar desafíos globales como el cambio climático, el hambre y la reducción de la pobreza[19].

[17] Naciones Unidas, “Primer acuerdo mundial sobre la ética de la inteligencia artificial”, UNESCO, 2021, URL: https://news.un.org/es/story/2021/11/1500522

[18] UNESCO, “Recomendación sobre la Ética de la Inteligencia Artificial”, 2021, URL: https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa

[19] Naciones Unidas, “Primer acuerdo mundial sobre la ética de la inteligencia artificial”, UNESCO, 2021, URL: https://news.un.org/es/story/2021/11/1500522

Lo expresado destaca el impacto positivo y transformador que la inteligencia artificial tiene en nuestra sociedad. Desde mejorar nuestras rutinas diarias hasta lograr avances significativos en campos como la salud y la inclusión, la IA demuestra su potencial para resolver problemas globales apremiantes. Es emocionante pensar en cómo la inteligencia artificial puede seguir contribuyendo al progreso y afrontando desafíos importantes en beneficio de toda la humanidad.

Sin embargo, esta tecnología también plantea desafíos sin precedentes. Por ejemplo, si nunca hubo -o no se reconoce- la participación de mujeres y LGBTIQ+ en determinados ámbitos de la vida y, por ende, no existen datos que den cuenta de eso, probablemente la IA reproducirá por defecto este tipo de disparidades[20]. También, la IA es vulnerable a los ataques de hackers y otros delincuentes cibernéticos. Al igual que cualquier otro sistema informático, los sistemas de IA pueden ser objeto de ataques que pueden interrumpir su funcionamiento u obtener información confidencial. Además, los ataques a la IA pueden tener un impacto mucho más significativo que los ataques a los sistemas tradicionales, ya que la IA está involucrada en muchas decisiones críticas y puede tener consecuencias graves si falla[21]. Hasta ahora, no había normas universales que abordaran estos problemas.

En ese sentido, se resalta los desafíos que la tecnología de inteligencia artificial presenta en relación con cuestiones de prejuicio, privacidad y vigilancia masiva. Estos problemas son preocupantes, ya que pueden perpetuar desigualdades y vulnerar derechos fundamentales. Es crucial establecer normas universales y marcos éticos sólidos que aborden estos problemas, para garantizar que la inteligencia artificial se desarrolle de manera responsable y respete los valores fundamentales de equidad, privacidad y autonomía.

Son las problemáticas expuestas por las que emite la UNESCO resulta elemental para que la inteligencia artificial pueda aportar a la sociedad y reducir los riesgos que conlleva los problemas antes planteados. Las problemáticas de transparencia, rendición de cuentas y privacidad son los ejes centrales que garantiza que las transformaciones digitales promuevan los derechos humanos.

[20] TELAM, "Cómo la inteligencia artificial reproduce la discriminación de género", 2023, URL: https://www.telam.com.ar/notas/202303/621747-discriminacion-genero-algoritmos.html

[21] Fórum Español para la Prevención y la Seguridad Urbana, "El uso de la inteligencia artificial y los riesgos para la seguridad pública", 2023, URL: https://fepsu.es/el-uso-de-la-inteligencia-artificial-y-los-riesgos-para-la-seguridad-publica/

Por otra parte, resulta importante dichas recomendaciones, con el fin de aprovechar los beneficios de la inteligencia artificial y mitigar los riesgos asociados. Es alentador ver que se enfoca en garantizar que las transformaciones digitales sean respetuosas de los derechos humanos y contribuyan a los Objetivos de Desarrollo Sostenible. La inclusión de aspectos como transparencia, rendición de cuentas y privacidad muestra una preocupación por abordar los desafíos éticos y legales que surgen con la IA. Además, al centrarse en áreas políticas clave, como la gobernanza de datos, la educación, la cultura, el trabajo, la atención sanitaria y la economía, se reconoce la necesidad de un enfoque integral para garantizar que la IA se utilice de manera responsable y beneficiosa para la sociedad.

Asimismo, el documento introduce una serie de conceptos clave, tales como la Proporcionalidad, para que la IA no exceda los límites preestablecidos para alcanzar metas u objetivos legítimos y deben adaptarse al contexto de su uso. La Supervisión y determinación humanas, debido a que los humanos son ética y legalmente responsables de todas las etapas del ciclo de vida de los sistemas de IA. Tambien se habal de Gestión medioambiental, con el fin de que los sistemas de IA contribuyan a la interrelación pacífica de todos los seres vivos y respetar el entorno natural, especialmente en la extracción de materias primas. Y, por último, y no el menos importante, la igualdad de género, para que las tecnologías de la IA no produzcan brechas de género que existen en el mundo real, en particular en lo que respecta a los salarios, la representación, el acceso y la difusión de estereotipos. Por ello, el documento enfatiza en todo lo necesario para adoptar medidas políticas, incluida la discriminación positiva, para evitar estos grandes escollos.[22]

Por lo expuesto, es menester tomar medidas adicionales para proteger a las personas en relación con sus datos personales. Es alentador ver que se promueve la transparencia y el control de los individuos sobre sus datos, incluyendo el acceso y la eliminación de registros. También se resalta la necesidad de mejorar la protección de los datos y fortalecer la capacidad de los organismos reguladores para hacer cumplir estas medidas. Esta apreciación personal reconoce la importancia de empoderar a las personas

[22] Ministerio de Asuntos Exteriores, Union Europea y Cooperación, “La UNESCO da un gran paso hacia el primer instrumento normativo sobre la ética de la IA”, 2020, URL: https://www.exteriores.gob.es/RepresentacionesPermanentes/unesco/es/Comunicacion/Noticias/Paginas/Articulos/La-UNESCO-da-un-gran-paso-hacia-el-primer-instrumento-normativo-sobre-la-%C3%A9tica-de-la-IA.aspx

en cuanto a su privacidad y control sobre sus datos, y apoya la idea de regulaciones más sólidas y efectivas para garantizar la protección de los derechos individuales en el entorno digital.

Y es que el pacto no es óbice en advertir que este tipo de tecnologías son muy invasivas, vulneran los derechos humanos y las libertades fundamentales, y se utilizan de forma generalizada.[23]

También, establece las bases para herramientas que ayudarán a supervisar y evaluar la implementación de estos sistemas y su impacto en las personas, la sociedad y el medio ambiente, lo que se podría utilizar para mejorar de forma notable los distintos pronósticos meteorológicos a nivel mundial. Esta tecnología permite analizar datos en tiempo real y con un margen de error mínimo acerca de catástrofes meteorológicas.[24]

Así las cosas, la IA representa una herramienta muy importante para solucionar problemáticas de gran valor para la sociedad, respetando los valores éticos que requieren estas nuevas tecnologías para la aplicación cotidiana. Así, esta apreciación permite valorar la inclusión de medidas que protejan los derechos individuales y promuevan el uso ético de la inteligencia artificial, al tiempo que destaca su potencial para abordar desafíos globales urgentes.

No obstante, es importante entender que la intersección entre la inteligencia artificial (IA) y los derechos humanos es un tema complejo y de creciente importancia en el ámbito jurídico. A medida que la IA se vuelve más omnipresente en diversas áreas de la sociedad, es fundamental comprender y abordar los conceptos fundamentales relacionados con la IA y los derechos humanos. En ese sentido, existen algunos conceptos jurídicos que se encuentran interrelacionados con la IA y del cual justifica la complejidad de dicha intersección entre los Derechos Humanos y la IA.

En primer lugar, se encuentra lo que se conoce como “transparencia”. La transparencia en los sistemas de IA implica la capacidad de comprender cómo funcionan y cómo toman decisiones. Esto es esencial para garantizar la responsabilidad y la

[23] Inter Press Service, “La Unesco clama por ética urgente para la inteligencia artificial”, 2023, URL: https://ipsnoticias.net/2023/03/la-unesco-clama-por-etica-urgente-para-la-inteligencia-artificial/

[24] Cámara Valencia, “Inteligencia Artificial como clave para la preservación del medio ambiente y de la industria forestal”, 2023, URL: https://ticnegocios.camaravalencia.com/servicios/tendencias/inteligencia-artificial-como-clave-para-la-preservacion-del-medio-ambiente-y-de-la-industria-forestal/#:~:text=La%20Inteligencia%20Artificial%20tambi%C3%A9n%20se,m%C3%ADnimo%20acerca%20de%20cat%C3%A1strofes%20meteorol%C3%B3gicas

rendición de cuentas. Desde una perspectiva de derechos humanos, la transparencia es crucial para evitar discriminación, sesgos o decisiones arbitrarias que puedan afectar los derechos y libertades fundamentales de las personas.

En segundo lugar, íntimamente relacionado con el anterior, encontramos los principios de igualdad y no discriminación. La IA puede influir en la igualdad y la no discriminación de diversas formas. Por ejemplo, si los algoritmos utilizados en sistemas de selección de empleo tienen sesgos ocultos, podrían perpetuar discriminaciones existentes en la sociedad. Los principios de igualdad y no discriminación consagrados en los instrumentos de derechos humanos deben aplicarse al desarrollo, implementación y uso de la IA para evitar que se violen estos derechos fundamentales.

En tercer lugar, se visibiliza la privacidad y protección de datos. La IA implica la recopilación y el procesamiento de grandes cantidades de datos personales. La protección de los datos personales es esencial para salvaguardar el resto de derechos fundamentales de las personas. Los sistemas de IA deben cumplir con las leyes de protección de datos aplicables y garantizar la seguridad y confidencialidad de la información personal.

En cuarto lugar, existe una tendencia hacia el derecho a la autonomía y la toma de decisiones. La IA puede afectar la capacidad de las personas para tomar decisiones autónomas. Por ejemplo, en el ámbito de la toma de decisiones médicas, si un sistema de IA proporciona recomendaciones sin la participación y el consentimiento informado del individuo, podría socavar su derecho a la autonomía y a tomar decisiones sobre su propio cuidado y bienestar.

En quinto lugar, se deslumbra la responsabilidad y rendición de cuentas. La IA plantea desafíos en términos de responsabilidad cuando se producen daños o violaciones de derechos. Es importante establecer mecanismos claros para determinar quién es responsable en caso de daños causados por sistemas de IA y cómo se pueden exigir cuentas. Esto implica la asignación de responsabilidades entre desarrolladores, proveedores de IA, usuarios y otros actores involucrados.

En sexto y último lugar, se encuentra el acceso a la justicia. La IA puede tener implicaciones en el acceso a la justicia y el ejercicio de los derechos legales. Por ejemplo, los sistemas de IA pueden ser utilizados en la toma de decisiones judiciales, lo que plantea interrogantes sobre la imparcialidad y el debido proceso. También es importante

garantizar que las personas afectadas por decisiones automatizadas tengan acceso efectivo a recursos y remedios legales en caso de violaciones de sus derechos.

Así, para el desarrollo y justificación de los objetivos del presente trabajo, se desarrollará y desmenuzará las implicancias de la IA respecto a las implicancias de la IA sobre el acceso a la información y la intimidad de los datos utilizados y qué consecuencias puede traer ello para evitar consecuencias no propicias para los Derechos Humanos.

Es así que, para el siguiente apartado y en el resto del desarrollo del presente trabajo, se enfocará en analizar detalladamente las implicaciones de la Inteligencia Artificial en relación con la privacidad y la protección de datos personales, con un enfoque específico en cómo la IA puede impactar la visibilización y el respeto de estos derechos fundamentales. A través de un análisis exhaustivo de casos, regulaciones y jurisprudencia pertinentes, se busca explorar cómo las aplicaciones de la IA pueden comprometer o reforzar la privacidad, y cómo los sistemas de IA pueden ser diseñados y regulados para garantizar el cumplimiento de los estándares de derechos humanos en este contexto.

Por ello, se espera que este trabajo de investigación arroje luz sobre las tensiones inherentes entre los avances tecnológicos impulsados por la IA y la necesidad de respetar y proteger los derechos humanos, en particular la privacidad y la protección de datos personales. Al identificar las mejores prácticas y las áreas de mejora en la regulación y diseño de sistemas de IA, se pretende contribuir al desarrollo de un marco normativo y ético que permita aprovechar el potencial de la tecnología sin comprometer la dignidad y los derechos de las personas.

En síntesis, es importante destacar que este trabajo de tesis se centrará exclusivamente en la interacción entre la Inteligencia Artificial y la privacidad/protección de datos personales, y no abordará las otras implicaciones mencionadas en la introducción. El enfoque estará en analizar cómo la IA impacta la visibilización y el respeto de estos derechos específicos, y no en un análisis integral de todas las implicaciones.

2. Antecedentes sobre el derecho de acceso a la información como derecho humano: Contexto nacional argentino.

La conceptualización del acceso a la información como un derecho es aún reciente. En los últimos años ha comenzado a discutirse en algunos países, como Argentina, sobre la justificación y los alcances de este derecho, que aún no ha adquirido un perfil definitivo en la Jurisprudencia. La sumaria intención de este trabajo es la de señalar algunos elementos teóricos útiles para afinar dicha conceptualización, justificación y alcances, como el de su exigibilidad ante los Tribunales de justicia.

El acceso a la información se presenta como un derecho en constante evolución y discusión en distintos países del mundo y de la región. Ello destaca la necesidad de clarificar su justificación, alcance y su exigibilidad ante los tribunales de justicia.

Así, el acceso a la información resulta ser un tema fundamental en el ámbito de los derechos humanos pues será el camino encargado de garantizar el disfrute de algunos derechos, así como el límite de algunos otros – como el derecho a la protección de datos enfrentado al derecho a la transparencia en las IA. Este derecho está consagrado en diferentes instrumentos internacionales, de los cuales se desarrollarán a continuación.

2.1 Naciones Unidas

Desde el Sistema de la Organización de las Naciones Unidas, Desde 1946 la Asamblea General de la Organización de las Naciones Unidas (en adelante la "ONU"), trabajó con el concepto de libertad de información. En su Resolución 59 (1) de 1946 la Asamblea General afirmó que "la libertad de información es un derecho humano fundamental y la piedra angular de todas las libertades a las que están consagradas las Naciones Unidas" y que abarca "el derecho a juntar, transmitir y publicar noticias"[25].

El artículo 19 del Pacto Internacional de Derechos Civiles y Políticos de Naciones Unidas (PIDCP) adoptado por la Asamblea General en su Resolución 2200 A (XXI), de 16 de diciembre de 1966, vigente desde 1976, cuyo texto es similar al de la Declaración Universal, establece que *toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de*

[25] ONU, Resolución de la Asamblea General No. 59(1), *Calling of an International Conference on Freedom of Information*, 1946, disponible en: http://daccessdds.un.org/doc/RESOLUTION/GEN/NR0/033/10/IMG/NR003310.pdf?OpenElement

toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección[26].

La Comisión de Derechos Humanos de Naciones Unidas creó la Relatoría Especial para la Libertad de Opinión e Información en marzo de 1993. Desde 1998 el Relator Especial de las Naciones Unidas sobre Libertad de Opinión y Expresión ha declarado inequívocamente que el derecho de acceso a la información en poder de las autoridades del Estado está protegido por el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos[27]. Posteriormente, en su informe anual de 1999 el referido Relator enfatizó el derecho de acceso como derecho en sí mismo y destacó ciertos principios que lo rigen[28].

2.2 Consejo de Europa

Esta Organización Internacional Europea, establecida en 1949 y con sede en Estrasburgo, está compuesta por 46 países europeos[29]. Su principal objetivo es promover y proteger los derechos humanos y el Estado de Derecho. Dentro del Consejo de Europa se han registrado avances significativos en el ámbito del acceso a la información. Tanto la Asamblea Parlamentaria como el Comité de Ministros han desempeñado un papel importante en este sentido. Asimismo, el Tribunal Europeo de Derechos Humanos, en su función judicial, ha emitido varias decisiones que han contribuido a sentar precedentes y establecer estándares relacionados con el acceso a la información. Estas decisiones han sido fundamentales para el fortalecimiento de los derechos individuales y la promoción de la transparencia en la región[30].

Es destacada la importancia de la Asamblea Parlamentaria y el Comité de Ministros del Consejo de Europa en la promoción del acceso a la información. Estas

[26] Comisión Interamericana De Derechos Humanos, "Estudio Especial sobre el Derecho de Acceso a l Información", *Relatoría Especial Para La Libertad De Expresión,* Organización De Los Estados Americanos, 2007, p. 16.
[27] Informe del Relator Especial sobre la protección y promoción del derecho a la libertad de opinión y expresión, UN doc. E/CN.4/1998/40; Informe del Relator Especial sobre la protección y promoción del derecho a la libertad de opinión y expresión, UN doc. E7CN.4/1999/64.
[28] *Idem*.
[29] Estatuto del Consejo de Europa, 1949, disponible en: http://conventions.coe.int/ Treaty/Commun/QueVoulezVous.asp?NT=001&CM=8&DF=4/2/2007&CL=ENG
[30] Comisión Interamericana De Derechos Humanos, "Estudio Especial sobre el Derecho de Acceso a l Información", Relatoría Especial Para La Libertad De Expresión, Organización De Los Estados Americanos, 2007, p. 17

instituciones han desempeñado un papel relevante en la promoción de políticas y medidas que garantizan un acceso efectivo a la información por parte de los ciudadanos.

El artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, adoptado por el Consejo de Europa en 1950 y en vigor desde 1953, garantiza el derecho a la libertad de expresión. Cabe destacar que este artículo no hace mención explícita al derecho de buscar información. No obstante, establece que toda persona tiene el derecho a la libertad de expresión, el cual abarca la libertad de opinión y la libertad de recibir y comunicar información e ideas, sin interferencia de las autoridades públicas y sin tener en cuenta las fronteras[31].

Repetimos que, aunque el artículo no menciona explícitamente el derecho de buscar información, establece el derecho a la libertad de expresión, que incluye la libertad de opinión y la libertad de recibir y comunicar información e ideas sin interferencia de las autoridades públicas y sin importar las fronteras. Esta protección amplia a la libertad de expresión es esencial para promover el acceso a la información y el intercambio de ideas en el contexto europeo, fortaleciendo así la democracia y el pluralismo.

2.3 Unión Europea

La transparencia es uno de los principios fundamentales de la Unión Europea (UE). Exige que la UE haga pública información sobre formulación de políticas y gasto y que respete el principio de libertad de información. Estos principios están establecidos en los tratados de la UE[32].

El derecho a la información en la Unión Europea se reconoce y protege en varios instrumentos legales y principios fundamentales. La Carta de los Derechos Fundamentales de la Unión Europea establece en su artículo 11 el derecho a la libertad de expresión y a recibir o impartir información, sin interferencias de las autoridades públicas.

Por otra parte, el Tratado de Funcionamiento de la Unión Europea amplía estos puntos. Dispone que las instituciones de la UE tienen la obligación de actuar públicamente y garantizar que los ciudadanos o toda persona física o jurídica que resida

[31] *Ibid*, p.18.
[32] Unión Europea, "Acceso a información", URL: https://european-union.europa.eu/principles-countries-history/principles-and-values/access-information_es, consultado 05/07/2023.

o tenga su domicilio social en un país de la UE pueda acceder a los documentos (artículo 15)[33]

Además, el Tribunal de Justicia de la Unión Europea ha reconocido el derecho de acceso a la información como un principio fundamental del derecho de la Unión Europea. En varias sentencias, el Tribunal ha establecido que los ciudadanos tienen derecho a acceder a los documentos de las instituciones de la Unión Europea, sujeto a ciertas limitaciones legítimas establecidas para proteger otros intereses, como la seguridad o la privacidad.

Por otra parte, la Unión Europea también ha promovido activamente el acceso a la información a través de la Directiva 2003/98/CE sobre reutilización de la información del sector público. Esta directiva establece un marco jurídico para la reutilización de la información del sector público, con el objetivo de fomentar la transparencia y promover la innovación. Esta transparencia será esencial para establecer unos estándares mínimos de ética en el desarrollo y empleo de Inteligencias Artificiales.

En resumen, en la Unión Europea se reconocen y protegen el derecho a la información y el acceso a los documentos públicos como elementos fundamentales para garantizar la transparencia, la participación ciudadana y el buen gobierno.

2.4 Sistema Interamericano de Derechos Humanos

En lo que respecta a la Organización de los Estados Americanos (OEA) y al Sistema Interamericano de Protección de los Derechos Humanos, en 1948 los Estados americanos adoptaron la Declaración Americana de los Derechos y Deberes del Hombre, cuyo artículo IV establece *que toda persona tiene derecho a la libertad de investigación, opinión, expresión y difusión del pensamiento por cualquier medio*. En 1969 se suscribió la Convención Americana sobre Derechos Humanos. En el numeral 1 del artículo 13 del mencionado instrumento claramente se expresa *que toda persona tiene derecho a la libertad de pensamiento y de expresión*. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección[34].

[33] *Idem*.
[34] Comisión Interamericana De Derechos Humanos, "Estudio Especial sobre el Derecho de Acceso a l Información", *Relatoría Especial Para La Libertad De Expresión,* Organización De Los Estados

Además, se menciona la Convención Americana sobre Derechos Humanos de 1969, la cual en el numeral 1 del artículo 13, establece claramente el derecho a la libertad de pensamiento y expresión. Este derecho abarca la libertad de buscar, recibir y difundir información e ideas de cualquier índole, sin importar las fronteras, ya sea de forma oral, escrita, impresa, artística o por cualquier otro medio elegido por la persona. Estos instrumentos jurídicos reflejan el compromiso de los Estados americanos con la promoción y protección de la libertad de expresión y acceso a la información como elementos fundamentales para el desarrollo democrático y el respeto de los derechos humanos en la región.

Así, tanto los órganos políticos de la Organización de los Estados Americanos (OEA), como la Asamblea General, y los órganos del Sistema Interamericano de Protección de los Derechos Humanos, como la Comisión Interamericana y la Corte Interamericana, han otorgado un amplio contenido al derecho a la libertad de pensamiento y expresión establecido en el artículo 13 de la Convención.

En este sentido, desde el año 2003 la Asamblea General ha emitido cuatro resoluciones específicas sobre el acceso a la información en las que resalta su relación con el derecho a la libertad de pensamiento y de expresión[35]. En la última resolución de 3 de junio de 2006 la Asamblea General de la OEA instó a los Estados a que respeten y hagan respetar el acceso a la información pública a todas las personas y a promover la adopción de disposiciones legislativas o de otro carácter que fueran necesarias para asegurar su reconocimiento y aplicación efectiva[36].

En 1997 la Comisión Interamericana de Derechos Humanos creó la Relatoría Especial para la Libertad de Expresión. En octubre de 2000 la Comisión Interamericana aprobó la Declaración de Principios sobre la Libertad de Expresión elaborada por la Relatoría Especial, cuyo Principio 4 reconoce que el *acceso a la información en poder*

Americanos, 2007, p. 14, URL: http://cidh.oas.org/relatoria/section/Estudio%20Especial%20sobre%20el%20derecho%20de%20Acceso%20a%20la%20Informacion.pdf

[35] Resolución AG/RES. 1932 (XXXIII-O/03) de 10 de junio de 2003 sobre "Acceso a la Información Pública: Fortalecimiento de la Democracia"; Resolución AG/RES. (XXXIV-O/04) de 8 de junio de 2004 sobre "Acceso a la Información Pública: Fortalecimiento de la Democracia"; Resolución AG/RES. 2121 (XXXV-O/05) de 7 de junio de 2005 sobre "Acceso a la Información Pública: Fortalecimiento de la Democracia"; y AG/RES. 2252 (XXXVI-O/06) de 6 de junio de 2006 sobre "Acceso a la Información Pública: Fortalecimiento de la Democracia".

[36] Resolución AG/RES. 2252 (XXXVI-O/06) de 6 de junio de 2006 sobre "Acceso a la Información Pública: Fortalecimiento de la Democracia", punto resolutivo 2.

del Estado es un derecho fundamental de los individuos. Los Estados están obligados a garantizar el ejercicio de este derecho[37].

En resumen, es importante que los Estados y la sociedad en su conjunto promuevan y respeten el ejercicio pleno de este derecho, fomentando un entorno en el que se fomente la diversidad de opiniones y se garantice la libre circulación de información e ideas. Al mismo tiempo, es necesario que se establezcan mecanismos adecuados para proteger a las personas y grupos vulnerables de discursos de odio y propaganda que inciten a la violencia o a acciones ilegales. De esta manera, se puede lograr un equilibrio entre la protección de los derechos individuales y el bienestar colectivo.

3. Análisis del impacto de la inteligencia artificial en el acceso a la información

En los últimos años, la mayoría de los trabajos de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (Unesco) realizados para conmemorar el Día Internacional del Acceso Universal a la Información se centran en el análisis de los riesgos y beneficios de la inteligencia artificial en el contexto de los principios de buena gobernanza. Ante el avance de las tecnologías y la importancia de este derecho humano y el conocimiento público en la era de la información, estos temas son prioritarios, y para su análisis requieren de un enfoque multidisciplinario, abierto, transparente e inclusivo que integre a la totalidad de los actores involucrados e interesados. En el centro de esta deliberación deben estar siempre las personas y sus derechos humanos[38].

En el enfoque antes mencionado, es fundamental abordar de manera exhaustiva y colaborativa los desafíos y oportunidades que la inteligencia artificial presenta en relación al acceso universal a la información.

Como se ha reiterado a lo largo del presente trabajo, la inteligencia artificial (AI) es una poderosa herramienta que favorece y potencializa la expansión y eficiencia de las tecnologías en todos los ámbitos. Al mejorar la capacidad de los sistemas a través de la

[37] CIDH, Declaración de Principios sobre Libertad de Expresión, Principio 4. Ver también Principios de Lima, Principio 1 "El acceso a la información como derecho humano".
[38] B. L. Ibarra Cadena, "Inteligencia artificial y acceso a la información", *MILENIO,* URl: https://www.milenio.com/opinion/blanca-lilia-ibarra-cadena/columna-blanca-lilia-ibarra-cadena/inteligencia-artificial-y-acceso-a-la-informacion

información y los datos, mediante estas tecnologías se favorece la accesibilidad, el almacenamiento, la optimización de las tareas y la facilitación de los procesos[39].

Así las cosas, la inteligencia artificial ha demostrado ser una herramienta invaluable en el avance tecnológico. Su capacidad para mejorar la eficiencia y la accesibilidad en diferentes áreas es evidente. Al aprovechar la información y los datos, estas tecnologías tienen el potencial de optimizar tareas y agilizar procesos, lo que puede tener un impacto positivo en diversas industrias y en nuestra vida diaria. Sin embargo, precisamente por este "aprovechamiento" de la información y datos, es fundamental abordar los desafíos éticos y sociales que surgen con el uso de la inteligencia artificial, garantizando la transparencia, la responsabilidad y la equidad en su aplicación.

Así, como mencionamos anteriormente, la Unesco, a través de su informe "El aporte de la inteligencia artificial y las TIC avanzadas a las sociedades del conocimiento: una perspectiva de derechos, apertura, acceso y múltiples actores", alertó sobre algunos de los riesgos de la IA en el derecho a la libertad de expresión, en concreto, se advirtió que la personalización de los contenidos digitales por parte de la IA, si bien posibilita el acceso a contenidos y conexiones relevantes, también podría manipular la forma en que la gente ejerce su derecho a la información, y su derecho a formarse una opinión.[40]

En definitiva, el informe de la Unesco resalta la necesidad de examinar detenidamente los riesgos asociados a la inteligencia artificial en relación con los derechos fundamentales, como la libertad de expresión, la libertad de prensa, la igualdad y la participación en la vida pública. Es preocupante que la personalización de los contenidos digitales por parte de la IA pueda influir en la forma en que las personas acceden a la información y forman sus opiniones. Además, la dependencia de los algoritmos en los motores de búsqueda y las redes sociales plantea desafíos en términos de neutralidad y acceso a una amplia variedad de información. Es esencial abordar estos problemas de manera responsable para garantizar un entorno digital inclusivo y respetuoso de los derechos humanos.

Así, por ejemplo, el uso de la inteligencia artificial podrá optimizar el flujo de datos y de información a disposición de las organizaciones públicas (también de las

[39] *Idem*.
[40] UNESCO, "El aporte de la inteligencia artificial y las TIC avanzadas a las sociedades del conocimiento: una perspectiva de derechos, apertura, acceso y múltiples actores", 2021, URL: https://unesdoc.unesco.org/ark:/48223/pf0000375796

privadas) para resolver cuestiones que antes requerían múltiples pasos, procedimientos y fases. O que, incluso, ni siquiera podían resolverse. Una inteligencia artificial bien "entrenada", con acceso al flujo informativo, simplifica y facilita exponencialmente las actividades de una organización y puede obtener resultados que serían imposibles de lograr con los cerebros humanos[41].

Por ejemplo, a partir de la digitalización de las historias clínicas de los pacientes, un sistema de inteligencia artificial podría garantizarles a ellos y a las autoridades sanitarias, un seguimiento y acceso a los datos sanitarios, optimizando exponencialmente la atención médica y permitiendo a los ciudadanos acceder a esa información a partir de un asistente digital21. Si bien excede seguir ampliando en este artículo todas estas cuestiones, este tipo de tecnología, al servicio de los derechos, se vuelve en sí misma un derecho. Mucho más aún, si consideramos que la ley de Argentina Digital 27.078 (arts. 1 y 2) declara de interés público el desarrollo de las tecnologías de la información y de la comunicación (TIC), habla de garantizar el derecho humano a las comunicaciones, telecomunicaciones y, también, el acceso los servicios de TIC[42].

4. Análisis del impacto de la inteligencia artificial en la privacidad de los datos

Además de todo lo mencionado hasta el momento, es evidente como la recopilación y utilización de información personal para entrenar y mejorar los sistemas de IA plantea implicaciones jurídicas significativas.

La IA se basa en gran medida en el análisis de grandes cantidades de datos (*big data)* para identificar patrones y tomar decisiones. Estos datos provienen de diversas fuentes, como redes sociales, registros médicos, transacciones financieras y registros gubernamentales, entre otros. Si bien la recopilación de datos en sí misma puede ser legal, el problema radica en cómo se utilizan y protegen esos datos.

En este contexto, uno de los principales desafíos es garantizar que los datos utilizados para entrenar los modelos de IA sean anónimos y que se respete el derecho a la privacidad de los individuos involucrados. La información personal sensible, como la orientación sexual, las creencias religiosas, el estado de salud o los antecedentes penales,

[41] J. G. Corvalán, "Inteligencia artificial: retos, desafíos y oportunidades - Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia", *Revista de Investigações Constitucionais*, vol. 5, núm. 1, pp. 295-316, 2018.
[42] *Ibid.*.

puede ser utilizada de manera inadvertida o intencionada para obtener resultados discriminatorios o invasivos.

Además, la IA puede llevar a la creación de perfiles de usuario altamente detallados, lo que permite a las empresas y organizaciones obtener información íntima sobre los individuos. Esto plantea preguntas sobre quién tiene acceso a estos perfiles y cómo se utilizan. Si se toman decisiones que afectan a las personas basadas en estos perfiles, como la negación de empleo o servicios, es fundamental garantizar que no se violen derechos fundamentales, como la igualdad de oportunidades o la no discriminación.

Otro aspecto relevante es el consentimiento informado de los usuarios. A menudo, los términos y condiciones que aceptamos al utilizar aplicaciones o servicios de IA contienen cláusulas extensas y complejas que describen cómo se recopila y utiliza nuestra información. Sin embargo, la falta de transparencia y comprensión de estas políticas puede llevar a que los usuarios cedan inadvertidamente su derecho a la privacidad sin darse cuenta.

Desde el punto de vista legal, muchos países han promulgado leyes y regulaciones para proteger la privacidad y los datos personales, como el Reglamento General de Protección de Datos (RGPD) en la Unión Europea. Estas regulaciones establecen requisitos claros sobre cómo deben recopilarse, almacenarse y procesarse los datos personales, y ofrecen a los individuos ciertos derechos, como el acceso a sus datos y el derecho a ser olvidados.

Sin embargo, la rápida evolución de la IA plantea desafíos para la legislación existente. Es necesario evaluar constantemente si las leyes actuales son suficientes para proteger los derechos de privacidad en el contexto de la IA. Además, los avances tecnológicos pueden superar rápidamente las regulaciones existentes, lo que requiere una adaptación constante por parte de los legisladores.

Por todo ello, tanto Ciberseguridad e Inteligencia Artificial (IA) son dos temas que actualmente están en el centro de atención de la sociedad. La creciente presencia de la IA en diferentes ámbitos -desde la salud hasta la industria- ha motivado a un aumento en el riesgo de ciberataques y ha puesto en peligro la seguridad de la información. Su uso cada vez más frecuente ha generado un debate sobre los desafíos que implica su

intervención. Aunque la IA puede ofrecer beneficios significativos, también conlleva ciertos peligros que deben ser considerados[43].

Ahora bien, abordar el tema de la inteligencia artificial requiere tener un plan de seguridad sólido que aborde las amenazas específicas asociadas con este tipo de sistemas, ya que son susceptibles de ser manipulados. Es esencial mantener la transparencia en todo lo relacionado con la IA, no solo por motivos de seguridad, sino también desde una perspectiva ética. En este sentido, resulta crucial prever cómo se llevan a cabo las decisiones y de qué manera se manipulan los datos. Es innegable que la IA tiene un enorme potencial y puede resultar de gran ayuda, incluso en la lucha contra el fraude y los delitos cibernéticos. Sin embargo, no se puede pasar por alto las preocupaciones que la rodean. Un aspecto inquietante es la posibilidad de que se introduzcan sesgos en los datos utilizados para entrenar los modelos de IA. Si estos sesgos no reflejan adecuadamente la diversidad de la población en general, existe un riesgo real de que los sistemas tomen decisiones equivocadas. Esto adquiere una relevancia crítica en ámbitos como el empleo, la justicia, la salud o la vivienda, ya que podría perpetuar situaciones de exclusión y discriminación.[44]

¿Y qué sucede con la privacidad de nuestros datos? Los sistemas de inteligencia artificial tienen esta capacidad impresionante para analizar enormes volúmenes de información, incluyendo datos personales y sensibles. Es precisamente esta característica la que los vuelve atractivos para posibles usos ilegales o perjudiciales. A pesar de todo, lo que más me inquieta acerca de la IA son los dilemas éticos que implica. Su aplicación en cuestiones de seguridad física genera inquietudes significativas en cuanto a la privacidad, los derechos civiles y la posibilidad de que se utilice de manera indebida para llevar a cabo vigilancia masiva. Por otro lado, existe la preocupación de que los algoritmos puedan generar resultados erróneos, llegando incluso a señalar erróneamente a personas inocentes como posibles amenazas en ciertas ocasiones.[45]

[43] D. Ionadi, "Inteligencia artificial: ¿Una aliada o un peligro?", *Forbes Argentina,* URL: https://www.forbesargentina.com/columnistas/inteligencia-artificial-una-aliada-o-peligro-n32903, 2023.
[44] *Idem*.
[45] *Idem*.

III. PRIVACIDAD DE LOS DATOS Y ACCESO A LA INFORMACIÓN EN EL CONTEXTO DE LA INTELIGENCIA ARTIFICIAL A LA LUZ DE LOS DERECHOS HUMANOS

1. La seguridad, elemento esencial en la protección de los derechos fundamentales

Definitivamente, ante todos los desafíos planteados, el problema de la seguridad en la red y en el tratamiento de datos, aparece como uno de los temas centrales para enfrentar tales retos. Las medidas de seguridad que todos —empresas, gobierno y personas— deben adoptar son el punto clave mediante el cual se puede conseguir una protección adecuada de los derechos de las personas y usuarios en la sociedad de la información y el conocimiento. En particular, el derecho a la intimidad puede verse protegido utilizando la tecnología para combatir a la tecnología, por expresarlo de alguna manera[46].

Precisamente, las autoridades de protección de datos europeas tienen una función esencial en este caso, toda vez que deben establecer políticas y asesoría a las empresas y personas para la adecuada adopción de medidas de seguridad. Éstas son parte de las funciones que la nueva Ley Federal de Protección de Datos en Posesión de Particulares le asignó al IFAIPD en Argentina. En España es la Agencia Española de Protección de Datos (AEPD) y el Observatorio para la Seguridad de la Información, del INCIBE (Instituto Nacional de Ciberseguridad), los que se encargan de realizar estudios para apoyar a las personas y al sector empresarial para el cumplimiento adecuado de la ley vigente y de los preceptos constitucionales[47].

La AEPD ha puesto mucho énfasis en las medidas de seguridad que se deben plantear en Internet. Por un lado, en cuanto a medidas físicas y de cifrado de la información personal que aparece en bases de datos u otros medios, pero también, por ejemplo, en cuanto a los modernos servicios en ese ámbito, tales como las redes sociales. Ha realizado estudios en donde destaca la importancia, nuevamente, de una autorregulación, en este caso social, para protegerse, a través de las medidas a adoptar para la privacidad de los perfiles.[48]

---

[46] Arellano Toledo W. & Ochoa Villicaña A. M., "Derechos de privacidad e información en la sociedad de la información y en el entorno TIC", Rev. IUS vol.7 no.31 Puebla, jun. 2013, URL: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100010

[47] *Idem*

[48] *Idem*

Hablando sobre la protección de los datos en sí, pensando en los desafíos que quedan por resolver, la AEPD ha expresado su deseo de que la definición de datos personales sea lo suficientemente amplia y compleja como para "prever las posibles evoluciones y abordar todas las áreas grises que existen dentro de su alcance, garantizando al mismo tiempo el uso legítimo de la flexibilidad". La Agencia tiene la idea de anticiparse a las situaciones que puedan surgir con las tecnologías de la información y la comunicación, y en ese sentido, sugiere la creación de símbolos o iconos informativos que indiquen cómo se manejan los datos de protección. También propone promover acciones informativas que ayuden a difundir la importancia de la protección de datos y las medidas de seguridad entre la población. Además de esto, la AEPD considera que es crucial fortalecer aún más la "consideración legal del deber de información" que las empresas tienen hacia sus clientes, consumidores o usuarios, especialmente aquellas que operan en el ámbito de la seguridad de la información y comunicación. Este deber de proporcionar información adecuada y relevante es fundamental para obtener un "consentimiento válido". En términos legales, esto significa que el consentimiento debe ser otorgado sin ningún tipo de manipulación o error, como se establece en el derecho civil.[49]

Es importante resaltar que los derechos fundamentales que hemos mencionado hasta ahora, aunque deben ser ejercidos sin restricciones, también tienen límites, ya sean explícitos o implícitos. En otras palabras, el ejercicio de estos derechos está sujeto a ciertas limitaciones que surgen debido a las necesidades de la vida en sociedad. Esta noción no contradice la creencia de que el individuo debe ser el foco central de cualquier comunidad organizada. Más bien, refuerza la idea de garantizar una existencia completa, pacífica y respetuosa hacia los derechos y la dignidad humana.[50]

Si bien, por no ser el asunto central de este artículo, no se tratará aquí la cuestión de si los bienes jurídicos que protege el Estado y su seguridad están por encima de los derechos fundamentales y en qué medida, sí nos parece oportuna esa apreciación sobre los valores que deben darse a cada uno de los dos ámbitos. Por ejemplo, se limitan algunas vertientes de la autodeterminación informativa, por razones de seguridad nacional[51]. Lo

[49] *Idem*
[50] Tórtora Aravena H., "Las limitaciones a los derechos fundamentales", *Estudios constitucionales,* vol.8 no.2 Santiago, 2010, URL: scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002010000200007#n1
[51] *Idem*

afirmado anteriormente lo podemos encontrar en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, del cual esta ley regula la protección de datos personales y establece las bases para el ejercicio de los derechos digitales. En su artículo 58, se establecen las excepciones al derecho a la protección de datos personales por motivos de seguridad nacional y defensa.[52]

Así tambien, existe limitaciones sobre la base de Ley Orgánica 2/1986, Fuerzas y Cuerpos de Seguridad. Esta ley regula las competencias y funciones de las fuerzas y cuerpos de seguridad del Estado. En su artículo 11, se establecen los límites al derecho a la protección de datos en el ejercicio de las funciones de seguridad.[53]

Finalmente, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. Esta ley establece el marco legal para el funcionamiento del Centro Nacional de Inteligencia (CNI) en España. Si bien no se especifica directamente la limitación de la autodeterminación informativa, el CNI tiene competencias en materia de seguridad nacional y defensa que pueden implicar restricciones en el acceso y tratamiento de datos personales.[54]

Es por eso que ante situaciones de este tipo y ante las posibles colisiones de dos derechos fundamentales (acceso a la información e intimidad de datos), en aquellos casos en que sucede, se habla del principio de proporcionalidad. La proporcionalidad mencionada debe estar presente en "las medidas limitadoras que se adopten. Ello, sin perjuicio de que en caso de conflicto con otros bienes y/o derechos constitucionales deban ceder ante otros intereses dignos de protección"[55].

La seguridad de los datos personales, en términos de confidencialidad, integridad y disponibilidad, debe estar respaldada por medidas de protección apropiadas y sensatas. Estas medidas pueden ser de naturaleza técnica, administrativa u organizativa, y su objetivo es prevenir cualquier tipo de manipulación o uso no autorizado o ilegal de los datos. Esto incluye la gestión del acceso a los datos, la prevención de la pérdida, la

[52] Ley Orgánica 3/2018, "Protección de Datos Personales y garantía de los derechos digitales", España, 2018, URL: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

[53] Ley Orgánica 2/1986, "Fuerzas y Cuerpos de Seguridad", España, 1986, URL: https://www.boe.es/buscar/pdf/1986/BOE-A-1986-6859-consolidado.pdf

[54] Ley 11/2002, "Reguladora del Centro Nacional de Inteligencia", España, 2002, URL: https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628

[55] Tórtora Aravena H., "LAS LIMITACIONES A LOS DERECHOS FUNDAMENTALES", *Estudios constitucionales,* vol.8 no.2 Santiago, 2010, URL: scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002010000200007#n1

destrucción o el daño de los mismos, así como la protección contra cualquier revelación no deseada, incluso en situaciones accidentales. Estas medidas de seguridad deben ser evaluadas de manera constante para asegurarse de que sigan siendo efectivas y adecuadas. Es esencial someterlas a auditorías periódicas y actualizarlas cuando sea necesario para mantenerse alineadas con los riesgos cambiantes y las tecnologías emergentes.[56]

De acuerdo con el principio mencionado, aquellos encargados del manejo de datos deben establecer y mantener medidas tanto de índole administrativa como técnica. Esto es esencial para erigir resguardos de seguridad que aseguren la confidencialidad, integridad y disponibilidad de los Datos Personales bajo su control o supervisión. Además, se deben asegurar de que estos Datos Personales no sean utilizados o revelados sin el consentimiento explícito de la persona titular o de una autoridad legítima. Asimismo, es fundamental evitar la pérdida, destrucción o daño accidental de estos datos. En términos generales, al tomar decisiones sobre las medidas de protección de Datos Personales, se deben considerar diversos factores, como: i) el posible impacto en los derechos de los individuos titulares de los datos, incluido el valor que dichos datos podrían tener para terceros no autorizados; ii) los costos asociados con la implementación de estas medidas; iii) los propósitos para los cuales se tratan los datos; y iv) la naturaleza específica de los Datos Personales involucrados, especialmente cuando se trata de Datos Sensibles.[57]

La naturaleza de las medidas de seguridad implementadas puede variar dependiendo de la sensibilidad de los datos en cuestión. Los "Datos Sensibles," como una categoría dentro de los datos personales, se definen por su capacidad para revelar detalles como el origen racial y étnico, opiniones políticas, creencias religiosas, filosóficas o morales, afiliación sindical, así como información relacionada con la salud o la vida sexual de una persona. Estos son los tipos de datos que todos desean mantener a salvo de la interferencia de terceros, dado que están intrínsecamente ligados a la esfera más privada

[56] OEA, "Principios Actualizados sobre la Privacidad y la Protección de Datos Personales", Comité Jurídico Interamericano, 2021, URL: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf
[57] *Idem*

de un individuo. Por lo tanto, estos datos merecen una protección más sólida y enérgica para garantizar su seguridad.[58]

Ahora bien, en necesario aclarar que la tarea de salvaguardar los datos personales de las personas se vuelve una tarea cada vez más difícil. Ello en razón de que actualmente, con el avance de nuevos medios de comunicación, masivos e instantáneos, no existen las suficientes herramientas técnicas por parte del Estado para lograr controlar la divulgación de información que pueda perjudicar a las personas que resultan expuestas. Casos de "filtración", destrucción, modificación de la información personal de las personas resulta más frecuente en los tiempos actuales.

No obstante, tambien hay que aclarar que no toda información que se filtre, modifique, o destruya conduzca indefectiblemente a una "responsabilidad por parte del gestor de datos", es decir, a aquella persona o institución (sea pública o privada) que tiene la custodia, en calidad de garante, de proteger y salvaguardar la información sensible de su usuario. Para ello, se requiere una valoración "razonada e informada", entre el nivel de daño ocasionado por la vulneración de los datos personales y las medidas y salvaguardias implementadas, siempre y cuando estás últimas hayan sido "razonables y adecuadas".[59]

Surge aquí el interrogante acerca de la manera y los criterios apropiados para establecer qué acciones gubernamentales, orientadas hacia la preservación de determinados intereses, pueden considerarse como apropiadas y razonables. En este contexto, la solución puede hallarse en el Principio 6 referente a la Privacidad y Protección de Datos Personales de la Organización de los Estados Americanos (OEA), cuyo comité interamericano establece pautas para asegurar que la salvaguardia de los datos sea sensata y adecuada. De acuerdo con esta directriz, la garantía de sensatez y adecuación en la preservación de los datos debe fundamentarse en métodos y técnicas de seguridad de la información que se alineen con las prácticas de excelencia generalmente reconocidas. Esto también involucra considerar factores tales como el constante cambio de las amenazas a la privacidad, con un énfasis en las amenazas cibernéticas, la utilización

[58] E. M. Ferrero & A. Schutz, "Tráfico de datos personales: su afectación a los derechos personalísimos", *Revista Perspectivas de las Ciencias Económicas y Jurídicas*, Vol. 3, N° 2, Santa Rosa: FCEyJ (UNLPam), EdUNLPam, 2013 , p. 57, DOI http://dx.doi.org/10.19137/perspectivas-2013-v3n2a03.

[59] OEA, "Principios Actualizados sobre la Privacidad y la Protección de Datos Personales", Comité Jurídico Interamericano, 2021, Principio 6, URL: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

de los métodos y técnicas más vanguardistas en el campo de la seguridad de la información, la contextualización dentro del panorama general y, por último, la proporcionalidad y necesidad intrínsecas de las medidas adoptadas[60].

Bajo tales parámetros, la evaluación de las medidas podría demostrar ser tanto variables como inestables. Esta premisa establece que una práctica que fuese aceptable apenas hace unos meses, podría, en el presente, ser considerada como invasiva, arriesgada o perjudicial para la privacidad personal. Del mismo modo, una limitación que en otro momento pareciera fundamentada, podría quedar desfasada o injusta a la luz de los avances tecnológicos. En este contexto, el desafío más importante resultaría adecuar normativas lo suficientemente flexibles, de tal manera que se molden a la actualización de las nuevas tecnologías sin caer en desuso o ambigüedad de las mencionadas prácticas[61].

Lo citado previamente, pone de relieve la importancia de considerar los valores fundamentales y los derechos individuales en un mundo tecnológico en constante cambio. Las prácticas que pueden haber sido aceptables en un momento dado pueden volverse cuestionables cuando se aplican de manera invasiva o perjudicial para la privacidad y los derechos de las personas.

Entonces, el desafío radica en asegurarse de que los avances tecnológicos no comprometan los principios éticos básicos, como la privacidad, la autonomía y la equidad. La actualización constante de las prácticas y regulaciones debe realizarse con un enfoque en la protección de los derechos humanos y el bienestar de las personas. Esto también implica considerar la distribución equitativa de los beneficios y riesgos tecnológicos para evitar aumentar las brechas sociales y económicas.

Son por estas razones en que la seguridad de los datos personales exige medidas de protección adecuadas para mantener la confidencialidad, integridad y disponibilidad de la información. Estas medidas, de naturaleza técnica, administrativa u organizativa, buscan prevenir el uso no autorizado, la manipulación y la pérdida de datos. La evaluación constante y las auditorías son esenciales para mantener la efectividad de estas medidas, mientras se adaptan a los riesgos cambiantes y tecnologías emergentes.

[60] *Idem*
[61] *Idem*

Los responsables de los datos deben establecer tanto medidas administrativas como técnicas para garantizar la seguridad de los datos bajo su custodia. Deben asegurarse de obtener el consentimiento para el uso y revelación de datos, así como evitar la pérdida o daño accidental. Al tomar decisiones sobre la protección de los datos, es vital considerar factores como el impacto en los derechos de los titulares, los costos y los propósitos del tratamiento de datos.

Los datos sensibles, que revelan información íntima, merecen una protección más robusta. Sin embargo, la tarea de salvaguardar los datos se vuelve desafiante en la era de la comunicación instantánea y los riesgos de filtración y modificación de datos son más frecuentes.

Aunque la filtración o modificación de datos no siempre conduce a la responsabilidad del gestor de datos, se requiere una evaluación informada del daño y las medidas implementadas. La solución podría encontrarse en pautas como el Principio 6 de la Privacidad y Protección de Datos Personales de la OEA, que busca asegurar la sensatez y adecuación de las medidas de seguridad.

La evaluación de estas medidas puede ser variable y susceptible a cambios, dada la evolución tecnológica. El desafío reside en brindar orientación sólida a los responsables de datos mientras se mantiene la relevancia en el ámbito tecnológico. En consecuencia, las medidas deben ser revisadas y actualizadas periódicamente para lograr una mejora continua.

2. Estado democrático y la creciente tensión entre el derecho de acceso a la información y la protección de datos personales

Como ya se explicó en reiteradas oportunidades en el presente trabajo, el acceso a la información es un pilar fundamental de una sociedad democrática. La posibilidad de acceder a datos y conocimientos es esencial para el empoderamiento de los ciudadanos y para garantizar la rendición de cuentas de las instituciones. Sin embargo, el uso de IA para la toma de decisiones y la generación de información también ha planteado la pregunta sobre quién tiene acceso a los algoritmos y modelos subyacentes, lo que puede dificultar la comprensión y el escrutinio de las decisiones automatizadas.

Así las cosas, La colisión entre la protección de datos personales y el acceso a la información a menudo crea un dilema ético. Por un lado, el acceso completo a los

algoritmos y datos utilizados en sistemas de IA podría aumentar la transparencia y el escrutinio público, evitando la discriminación algorítmica y la toma de decisiones sesgada. Por otro lado, la divulgación excesiva de información podría comprometer la privacidad y la seguridad de los datos individuales.

Por ello, como un primer acercamiento al presente subapartado, consiste en tener en cuenta que unos de los desafíos radican en encontrar un equilibrio entre estos dos aspectos. Desde la perspectiva de los derechos humanos, este equilibrio implica diseñar sistemas de IA que sean transparentes en sus operaciones y decisiones, permitiendo que los individuos comprendan cómo se utilizan sus datos. Al mismo tiempo, es necesario establecer salvaguardias sólidas para prevenir el acceso no autorizado y el uso indebido de datos.

En ese sentido es que, en un país democrático, el derecho de acceso a la información pública constituye una prerrogativa fundamental sobre la que se asienta el régimen democrático. Este derecho proporciona a los ciudadanos la posibilidad de conocer y participar activamente en los asuntos de interés público, fomentando así la transparencia, la rendición de cuentas y la toma de decisiones informada. Al garantizar el acceso a la información, se fortalece la base democrática de la sociedad y se promueve una ciudadanía informada y empoderada.

Por ejemplo, En Argentina, el derecho de acceso a la información pública está reconocido en la Constitución Nacional y en la Ley de Acceso a la Información Pública (Ley 27.275). Esta prerrogativa fundamental permite a los ciudadanos acceder a información de carácter público, tanto en organismos estatales como en entidades privadas que presten servicios públicos. El acceso a la información promueve la transparencia, la participación ciudadana y el control democrático, fortaleciendo así el sistema republicano del país. A través de este derecho, los ciudadanos argentinos pueden obtener información relevante sobre la gestión del gobierno, la toma de decisiones y los asuntos de interés público, lo que contribuye a una mayor rendición de cuentas y a una sociedad más informada y participativa.

En menester recordar que, para el país en mención, Argentina, como país miembro de la Organización de los Estados Americanos (OEA), está vinculada al Sistema Interamericano de Derechos Humanos. Este sistema se compone de la Convención Americana sobre Derechos Humanos, conocida como Pacto de San José, y la Comisión

Interamericana de Derechos Humanos (CIDH) y la Corte Interamericana de Derechos Humanos (Corte IDH).

Argentina ha ratificado la Convención Americana sobre Derechos Humanos y, por lo tanto, se compromete a respetar, proteger y garantizar los derechos humanos reconocidos en dicha convención. La CIDH tiene la responsabilidad de promover y proteger los derechos humanos en el continente americano y puede recibir denuncias de violaciones de derechos humanos en Argentina. Además, Argentina ha aceptado la competencia de la Corte IDH, lo que significa que los individuos y grupos pueden presentar casos ante la corte después de haber agotado los recursos legales internos.

La vinculación de Argentina con el sistema interamericano de derechos humanos fortalece la protección de los derechos humanos en el país. Permite la supervisión internacional de las garantías fundamentales, así como el acceso a mecanismos de justicia regional en caso de violaciones de derechos humanos. Esto contribuye a la consolidación del Estado de derecho y la promoción de una cultura de respeto a los derechos humanos en Argentina.

En este sentido, el acceso a la información es definido por la Comisión Interamericana de Derechos Humanos como una de las garantías más sólidas de la democracia moderna, afirmando que existe una relación directa entre el acceso a la información y el funcionamiento de la democracia[62]. En esta línea de pensamiento, el Tribunal Europeo de Derechos Humanos manifestó que este derecho constituye uno de los fundamentos esenciales de la sociedad democrática[63].

El derecho de acceso a la información importa una herramienta legal para alcanzar la transparencia, pero también como medio de fiscalización y participación efectiva de todos los sectores de la sociedad sin discriminación, que involucran directamente a la población[64]. Así, el derecho de acceso a la información refuerza la idea de que las instituciones y las autoridades deben ser transparentes y responsables ante la sociedad. Permite que las personas tomen decisiones informadas y participen activamente en

[62] Comisión IDH, "Informe sobre la compatibilidad entre las leyes de desacato y la Convención Americana sobre Derechos Humanos", en Informe Anual de la Comisión Interamericana de Derechos Humanos 1994, Washington D.C., 1995, disponible en http://www.oas.org/es/cidh/ expresion.
[63] Tribunal Europeo de Derechos Humanos, 07/12/1976, Caso "Handyside vs. Reino Unido".
[64] Basterra, Marcela I., "Acceso a la información pública y transparencia. Ley 27.275 y decreto reglamentario 206/2017. Comentados, anotados y concordados". Editorial Astrea y Jusbaires. 2017, p. 3

asuntos que les afectan. Al fomentar la participación y la fiscalización, se promueve una mayor equidad y justicia en la toma de decisiones

Por otro lado, el derecho a la intimidad personal se encuentra estrechamente vinculado con aspectos de la vida humana que son inescindibles para el desarrollo de todo individuo, como también para la existencia de un orden social y político justo que los proteja. Esta libertad confiere al individuo la facultad de excluir de su esfera de soberanía personal cualquier intromisión arbitraria o injustificada[65]. Por ello, el respeto por el derecho a la intimidad es esencial para el reconocimiento de la dignidad humana y el valor intrínseco de cada individuo. La capacidad de controlar la información personal y mantener ciertos aspectos de la vida fuera del escrutinio público es fundamental para la autonomía y la autodeterminación.

El derecho de acceso a la información pública y la protección de datos personales poseen sus propias áreas de influencia, donde las normas se implementan sin injerencia, respetando la lógica de las garantías tuteladas. No obstante, debemos reconocer que no siempre estos derechos resultan complementarios y en algunas ocasiones el ejercicio de uno de ellos supone un límite para el otro. En tal sentido, se ha afirmado que el acceder a determinada información puede a la vez socavar el legítimo interés de otra persona en conservar en privado sus datos personales[66]. En tal sentido, se deben sopesar los beneficios de la transparencia y el acceso a la información contra la necesidad de preservar la privacidad y la autonomía individual. Garantizar que la obtención de información no debe implicar un daño innecesario sobre los derechos de las personas. En algunos casos, la exposición de datos personales puede llevar a consecuencias negativas, como discriminación o abuso.

Verbigracia, se debe admitir que, en algunos casos, ciertos pedidos de acceso a la información pública pueden socavar el legítimo interés de una persona en preservar sus datos personales, afectando su derecho a la intimidad y privacidad. Ante esta situación, y en virtud de la importancia de estas prerrogativas, se torna indispensable establecer un diseño institucional suficiente para efectivizar la protección y el ejercicio adecuado de ambos derechos[67]. Por eso, un enfoque ético sobre la información implica considerar el

[65] Basterra M. L., "La tensión entre el derecho de acceso a la información y la protección de datos personales", *op. Cit.*
[66] *Idem*.
[67] *Idem*.

contexto y el propósito del acceso al mismo. Es importante cuestionar si la divulgación de ciertos datos es necesaria y justificable en términos de interés público. La ética también requiere salvaguardar la confidencialidad de ciertos datos personales, especialmente cuando su revelación no es esencial para lograr los objetivos de transparencia.

En este contexto, en el ámbito internacional existen marcos legales que han abordado soluciones para abordar el choque entre la salvaguardia de datos y el derecho de acceso a la información. Ejemplificando, la Ley Española 19/2013[68], en su artículo 15, contempla la opción de permitir el acceso a información que involucre datos personales con el consentimiento del titular. Si este no es el caso, la entidad correspondiente podría tomar una decisión a favor de la solicitud tras sopesar el interés público en la divulgación y los derechos de las personas cuyos datos estén involucrados. Al realizar esta evaluación, se considerará la minimización del perjuicio para los afectados, así como la justificación de los solicitantes basada en el ejercicio de sus derechos o su calidad de investigadores que buscan el acceso por fines históricos, científicos o estadísticos, entre otros aspectos relevantes[69].

Dentro del contexto de la región interamericana, la Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública, aprobada por la Asamblea General de la OEA el 21 de octubre de 2020[70], aborda en su artículo 40 la posibilidad de limitar el acceso a la información en casos donde esto podría infringir el derecho a la privacidad, incluyendo aspectos relacionados con la vida, salud o seguridad. En relación a este aspecto, la ley establece que estas excepciones no deben ser aplicadas cuando el individuo haya otorgado su consentimiento para la divulgación de sus datos personales o cuando las circunstancias indiquen claramente que la información fue entregada a la autoridad como parte de la información sujeta al régimen de publicidad[71].

[68] Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno, publicada en el BOE, 10/12/2013, URL: https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887
[69] Basterra M. L., "La tensión entre el derecho de acceso a la información y la protección de datos personales", *op. cit*
[70] Ley Modelo de Acceso a la Información Pública de la Organización de Estados Americanos, aprobada el 29/04/2010 disponible en http://www.oas.org/es/sla/ddi/acceso_informacion.asp
[71] Basterra M. L., "La tensión entre el derecho de acceso a la información y la protección de datos personales", *op. cit*

En Argentina, como otro ejemplo, se reguló el procedimiento interno a través de la Resolución de la Agencia de Acceso a la Información Pública 5 [72] que prevé la intervención obligatoria de la Dirección Nacional de Protección de Datos Personales, en todos los pedidos de acceso a la información estatal que afecten o potencialmente puedan afectar a la protección de datos de personas determinadas o determinables.

La normativa responde a los "Principios sobre el Derecho de Acceso a la Información" del Comité Interamericano [73], que expresan que en caso de que exista conflicto entre ambas prerrogativas, deben aplicarse criterios de proporcionalidad para garantizar y proteger a cada uno de esos derechos basados en el interés que los justifica[74].

Las autoridades encargadas de resolver estos conflictos deben valorar las circunstancias concretas, para ponderar y decidir qué derecho debe primar en cada caso. Debemos recordar que la Corte Suprema[75], manifestó que la negativa de información fundamentada en el resguardo de la privacidad de los beneficiarios no puede ser admitida, cuando no se relaciona con datos sensibles, ya que desatiende el interés público que hay en el pedido que se dirige a controlar eficazmente el modo en que los funcionarios ejecutan una política social. Además, indicó que en la ponderación debe prevalecer el principio de máxima divulgación de la información pública[76].

Se debe buscar un equilibrio entre el derecho de las personas a controlar la forma en que se recopilan, almacenan y utilizan sus datos personales de manera segura y protegida, por un lado y, el derecho de acceso a la información pública, por el otro. A través de la ponderación, las autoridades deberán analizar la estructura de mandatos de optimización de las normas que posibilitan el ejercicio de un derecho en su máxima expresión, dentro de las posibilidades jurídicas y reales existentes. Sin duda, la tarea de ponderación de un derecho sobre otro es una actividad jurídica compleja que no puede realizarse de forma automática, sino que requerirá por parte de las autoridades que la realicen, un análisis exhaustivo de los elementos claves y la utilización de mecanismos,

[72] Agencia de Acceso a la Información Pública de la Nación Argentina, Resolución de la Agencia de Acceso a la Información Pública Nº 5, publicada en el BO el 05/02/2018, URL: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-5-2018-306577
[73] Aprobados por CJI/RES. 147 (LXXIII-O/08) el Comité Jurídico Interamericano el 07/08/2008.
[74] Agencia de Acceso a la Información Pública de la Nación Argentina, Resolución de la Agencia de Acceso a la Información Pública Nº 5, publicada en el BO el 05/02/2018, URL: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-5-2018-306577
[75] CSJN, 26/03/2014, "CIPPEC c. Estado Nacional - Ministerio de Desarrollo Social s/ Amparo".
[76] Basterra M. L., "La tensión entre el derecho de acceso a la información y la protección de datos personales", *op. cit*

para arribar a una solución que posibilite efectivizar el derecho fundamental prioritario en el caso, con la menor afectación posible al otro[77].

En resumen, el equilibrio entre el derecho de acceso a la información y la protección de datos personales es una cuestión compleja tanto desde una perspectiva legal como ética. La elaboración de regulaciones claras y la consideración cuidadosa de los posibles conflictos entre estos derechos son esenciales para garantizar que ambos sean respetados de manera equitativa.

IV. ABORDAJE Y ALGUNAS POSIBILIDADES DE CONCILIACIÓN DE LA TENSIÓN ENTRE ACCESO A LA INFORMACIÓN PÚBLICA Y LA PROTECCIÓN DE DATOS PERSONALES EN EL CONTEXTO HISPANO AMERICANO.

1. Los posibles mecanismos de ponderación de derechos.

Algunos autores, para resolver la tensión descrita en el apartado anterior, entienden que debe desprenderse de la aplicación de los llamados "test del daño" y del "test del interés público", como herramientas que permiten sopesar los valores en conflicto para determinar qué bien jurídico debe primar, teniendo en cuenta las particularidades de cada caso[78].

Es claro que la valoración de los bienes jurídicos en colisión resulta una tarea judicial difícil y compleja que exige considerar exhaustivamente las características particulares de cada pedido de acceso a la información. La vulneración de la privacidad que puede darse ante la publicación de ciertos datos personales o el interés público que puede tener alguna información, no resulta igual en todas las solicitudes de acceso[79]. La valoración de bienes jurídicos en conflicto siempre implica considerar tanto las necesidades colectivas como los derechos individuales. La ética demanda un equilibrio entre la transparencia y la protección de la privacidad. La clave es determinar cuándo el interés público es lo suficientemente fuerte como para justificar la exposición de información personal.

Es por razones recién expuestas por los que se recurren a las pruebas del daño y del interés público, consistente en una evaluación de los valores en oposición -en este

[77] *Idem*.
[78] *Idem*.
[79] *Idem*.

caso publicidad y transparencia contra la privacidad e intimidad de los afiliados- para poder constatar de manera cierta si la primera pone en riesgo concreto a la segunda, de forma tal que amerite una restricción en el acceso a la información[80].

Algunos funcionarios sobre la materia advierten que, en diversos organismos de control, tribunales y legislaciones, utilizan estas técnicas para resolver conflictos jurídicos similares al presente. En tal sentido, el Departamento de Derecho Internacional de la OEA explica la necesidad de contar con las pruebas de equilibrio entre derechos, a fin de que el acceso a la información pueda coexistir armónicamente con otras prerrogativas, como el derecho a la privacidad y seguridad. Agrega, "Las pruebas de los daños y las pruebas del interés público deben establecer criterios especiales a ser aplicados por la justicia y los tribunales administrativos. Éstos deberían ser establecidos por la constitución o la legislación de nivel superior. Constituyen herramientas importantes para que los órganos de supervisión puedan balancear los derechos en conflicto caso por caso. La carga de realizar dichas pruebas no recaerá en el peticionario" [81].

En Argentina, el decreto 206/2017 [82] reglamentario de la ley 27.275, dispone que los sujetos obligados no podrán negarse a otorgar la información solicitada amparándose en la protección de datos personales "(...) si el daño causado al interés protegido es menor al interés público de obtener la información" [83]. En consecuencia, no basta con acreditar que la información requerida contenga datos personales, sino que además debe ponderarse el daño causado por la divulgación y el interés público que supone el acceso a la información requerida[84].

1.1 El test del daño

La prueba del daño se puede definir como la realización de un balance entre el interés de retener la información requerida y el interés de divulgarla, con el objeto de

[80] *Idem*.
[81] *Idem*.
[82] Decreto 206/2017 publicado en el BO el 28/03/2017
[83] *Ibídem*, artículo 8º.
[84] Basterra M. L., "La tensión entre el derecho de acceso a la información y la protección de datos personales", *op. cit*

determinar si el beneficio público obtenido ante la divulgación es mayor que el daño que podría causar su revelación[85].

Diversas legislaciones receptan esta herramienta, por ejemplo, en México, la Ley Federal de Transparencia y Acceso a la Información Pública [86] determina que el sujeto obligado deberá, en todo momento, aplicar una prueba de daño para denegar el acceso a la información[87]. Además, establece parámetros para su aplicación, expresando que se deberá justificar que: "I. La divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo al interés público o a la seguridad nacional; II. El riesgo de perjuicio que supondría la divulgación supera el interés público general de que se difunda, y III. La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio"[88]

Dentro del sistema interamericano la ya mencionada propuesta de Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública [89], desarrolla el concepto en el artículo 35, que establece:(…) 1. Al invocar la existencia de una causal de reserva ante una solicitud de Información, el sujeto obligado deberá aplicar la prueba del daño. 2. La prueba de daño debe establecer que la divulgación de la Información solicitada puede generar un daño real, demostrable e identificable. En la aplicación de dicha prueba, el sujeto obligado deberá acreditar por escrito: a) que la divulgación de la Información representa un riesgo real, demostrable e identificable de perjuicio significativo a un bien jurídico o derecho tutelado claramente identificado en una ley. No podrá ser utilizado como justificación un daño o perjuicio hipotético. b) que no hay un medio alternativo menos lesivo para el interés público de conocer la Información. c) que el riesgo del perjuicio que supondría la divulgación de la Información supera el interés público de que ésta se difunda. d) que la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio. e) que la

[85] Covarrubias Cuevas, Ignacio, "Las falencias del test de interés público como instrumento de ponderación entre el acceso a la información pública y la vida privada", Revista de Derecho de la Pontificia Universidad Católica de Valparaíso no. 38, Chile, 2012, disponible en https:// scielo.conicyt.cl/
[86] Ley General de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el 04/08/2015
[87] *Ibídem*, artículo 102.
[88] *Ibídem*, artículo 104.
[89] Propuesta de Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública 2.0 elaborada por el Departamento de Derecho Internacional el 03/03/2020, disponible en http://www.oas.org/es/sla/ddi/acceso_informacion.asp.

restricción no atenta contra la esencia misma del derecho a la Información. f) la concurrencia de los requisitos de temporalidad, legalidad y razonabilidad"[90].

En ese sentido, el Departamento de Derecho Internacional (DDI) de la Secretaría de Asuntos Jurídicos de la OEA, organismo encargado de su elaboración, explica que el daño real significa que la información solicitada debe representar un peligro real —y no hipotético— ante el interés público. Asimismo, el daño demostrable se da cuando en caso de divulgarse los datos requeridos, el perjuicio al interés público resulta mayor que si se restringe el acceso a ellos. Finalmente, el daño identificable se comprueba cuando la entrega de la información supone una afectación grave para las partes involucradas en los hechos[91].

También afirma, que el requisito de proporcionalidad consagrado en el inciso d) del artículo 35, implica demostrar que el perjuicio al bien jurídico es mayor que el interés público de divulgar la información[92].

Igualmente, agrega que los requisitos normados en el inc. f) deben entenderse en el contexto que se detalla a continuación: a) La temporalidad supone que la reserva de la información sea impuesta por un tiempo determinado, mientras dure la causal que impide su difusión; b) El requisito de legalidad, implica que el sujeto requerido debe analizar el marco legal vigente y demostrar que las limitaciones al acceso a la información pública están dirigidas a la protección de derechos de idéntica o superior importancia; c) La razonabilidad significa que no basta con que el sujeto obligado se ampare en una ley para denegar la divulgación, sino que también es necesario que justifique la adopción de esa limitación, con el objeto de reducir la arbitrariedad y evitar denegaciones injustificadas al derecho de acceso[93].

En conclusión, la prueba de daño surge, en el ámbito del acceso a la información pública, ante la necesidad de establecer nuevos estándares legales que ayuden a realizar interpretaciones más adecuadas a fin de garantizar el derecho y al mismo tiempo, restringir al mínimo la afectación a otras prerrogativas fundamental.

[90] Basterra M. L., "La tensión entre el derecho de acceso a la información y la protección de datos personales", *op. cit*
[91] *Ídem*.
[92] *Idem*.
[93] *Idem*.

1.2 El test del interés público

En sentido similar al test del daño, la prueba de interés público supone un proceso idéntico de valoración que tiene lugar cuando los bienes afectados por la divulgación de la información se relacionan con los derechos individuales de las personas [94]. Así, se afirma que es un mecanismo de ponderación entre el beneficio que implica dar a conocer la información pedida, contra el daño que su divulgación genera en los derechos de las personas [95].

La Ley Federal de Transparencia y Acceso a la Información Pública de México determina que, para resolver el recurso de revisión interpuesto ante la denegatoria del pedido, se debe aplicar esta prueba cuando exista una colisión de derechos, con base en los elementos de idoneidad, necesidad y proporcionalidad. Agrega que "(...) se entenderá por: I. Idoneidad: La legitimidad del derecho adoptado como preferente, que sea el adecuado para el logro de un fin constitucionalmente válido o apto para conseguir el fin pretendido; II. Necesidad: La falta de un medio alternativo menos lesivo a la apertura de la información, para satisfacer el interés público, y III. Proporcionalidad: El equilibrio entre perjuicio y beneficio a favor del interés público, a fin de que la decisión tomada represente un beneficio mayor al perjuicio que podría causar a la población"[96].

La aplicación de esta prueba también es receptada por la jurisprudencia chilena. Así, se recurrió a este mecanismo para resolver un amparo interpuesto ante el Consejo para la Transparencia de Chile (CPLT) [97], fundado en la denegatoria de un pedido de acceso a la información por parte del Ministerio de Vivienda y Urbanismo (MINVU), por considerar que la información requerida resultaba protegida por la Ley de Protección de datos [98]. El CPLT precisa que; "Dicho análisis consiste en ponderar si el interés público que se obtendría con la entrega de la información justifica su divulgación y vence, con ello, la reserva. En este caso, los bienes jurídicos en juego son, por una parte, la publicidad de la información (…), y, por otra, la protección de la vida privada y datos personales

[94] Covarrubias Cuevas, Ignacio, *ob. cit*
[95] Octavo Certamen de Ensayo en Materia de Transparencia y Acceso a la Información Pública, Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo, 2016, disponible en http://www.idaipqroo. org.mx, p. 13.
[96] *Idem*.
[97] Decisión amparo del Consejo para la Transparencia de Chile C926, 12/10/2012, disponible en https://www. consejotransparencia.cl/.
[98] Ley 19.628 sobre Protección de la Vida Privada y protección de datos de carácter personal de Chile publicada el 28/08/1999.

concernientes a un tercero" [99]. Finalmente, el Consejo concluye que, en el caso en análisis, no concurre un interés público prevalente en conocer la información requerida, rechazando el amparo interpuesto[100].

También a este concepto se refiere la Propuesta de Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública, que impone la obligación al sujeto requerido de aplicar la prueba de interés público, al invocar la existencia de una causal de confidencialidad ante una solicitud de acceso. Al igual que la legislación mexicana, deberá realizarse sobre la base de los elementos de idoneidad, necesidad y proporcionalidad, los cuales son definidos con idénticos criterios [101].

Esta herramienta igualmente es utilizada en materia de acceso a la información ambiental. Así, el Acuerdo de Escazú [102] del cual Argentina es parte [103], expresa "Cuando aplique la prueba de interés público, la autoridad competente ponderará el interés de retener la información y el beneficio público resultante de hacerla pública, sobre la base de elementos de idoneidad, necesidad y proporcionalidad" [104].

En Argentina, la Agencia de Acceso a la Información Pública [105] estableció criterios orientadores sobre este mecanismo. El organismo explica que, en virtud del principio de facilitación, consagrado en el artículo 1º de la ley 27.275, la reserva de información no puede ampararse únicamente en las excepciones previstas en el artículo 8º, sino que es necesario además verificar que el interés público comprometido no sea mayor al daño que podría generar la publicidad, pues en ese caso correspondería igualmente otorgar acceso a la información. Agrega, que se debe analizar la idoneidad, necesidad y proporcionalidad de la medida restrictiva de acceso a la información, en consideración de la finalidad que se persigue y del interés público comprometido en cada caso[106].

---

[99] Decisión amparo del Consejo para la Transparencia de Chile C926, op. cit. considerando 6º.
[100] Basterra M. L., "La tensión entre el derecho de acceso a la información y la protección de datos personales", *LA LEY*, URL: https://marcelabasterra.com.ar/wp-content/uploads/2021/09/Suple-Constitucional-31-agosto-2021.-La-tenci%C3%B3n-entre-el-D.-a-la-informaci%C3%B3n-y-la-Protecci%C3%B3n-de-datos-personales-Marcela-Basterra.pdf, 2021.
[101] Propuesta de Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública, op. cit., artículo 36.
[102] Acuerdo Regional sobre el Acceso a la Información, la Participación Pública y el Acceso a la Justicia en Asuntos Ambientales en América Latina y el Caribe, firmado el 04/03/2018 en Escazú, Costa Rica.
[103] Ley 27.566 publicada en el BO el 19/10/2020.
[104] Ibídem, artículo 5.
[105] Resolución 268/19 de la Agencia de Acceso a la Información Pública, publicada el 10/01/2020
[106] Basterra M. L., "La tensión entre el derecho de acceso a la información y la protección de datos personales", *LA LEY*, URL: https://marcelabasterra.com.ar/wp-content/uploads/2021/09/Suple-

En primer lugar, la idoneidad significa que la medida restrictiva del derecho de información sea un instrumento idóneo para cumplir la finalidad que se busca a través de su imposición, es decir, debe ser una medida efectivamente conducente para los objetivos legítimos e imperiosos que mediante ella se persiguen, tal como lo ha definido la Relatoría Especial para la Libertad de Expresión [107].

La legitimidad, según el criterio de la Corte IDH en el caso "Caso Claude Reyes vs. Chile" [108], exige una necesidad cierta e imperiosa de efectuarse la limitación, es decir, que el objetivo no puede alcanzarse razonablemente por un medio menos restrictivo de derechos. En otras palabras, en caso de existir varias opciones para lograr ese objetivo, debe aplicarse la que restrinja en menor medida el derecho a la información[109].

Por último, la proporcionalidad implica que las restricciones sean estrictamente proporcionales al fin legítimo que las justifica, para lo cual debe determinarse si el sacrificio del derecho a la información que esta conlleva resulta exagerado o desmedido frente a las ventajas que mediante la misma se obtienen[110].

Todo lo explicado trae correlación frente a la problemática con lo sucedido durante la pandemia, del cual presentaba la misma problemática central. En 2020, la Comisión Interamericana de Derechos Humanos (CIDH) adoptó la resolución 1/2020 titulada "Emergencia Sanitaria y Derechos Humanos en las Américas". Entre las recomendaciones se encuentran que las restricciones de derechos deben ajustarse a los principios "pro persona", proporcionalidad, temporalidad, y deben tener como finalidad legítima el estricto cumplimiento de objetivos de salud pública. En el marco de la emergencia, las autoridades estatales tienen el deber de asegurar el respeto a los derechos humanos, así como informar a la población. A su vez, están expuestas a un mayor escrutinio y a la crítica pública[111].

Constitucional-31-agosto-2021.-La-tenci%C3%B3n-entre-el-D.-a-la-informaci%C3%B3n-y-la-Protecci%C3%B3n-de-datos-personales-Marcela-Basterra.pdf, 2021.

[107] CIDH-OEA, Relatoría Especial para la Libertad de Expresión, "Marco Jurídico Interamericano sobre el derecho de libertad de expresión", 30/12/2009, párr. 87, disponible en http://www.oas.org/es/cidh/expresion

[108] CIDH, Caso de "Claude Reyes y otros", sentencia del 19/09/2006, Serie C No. 151, párr. 91.

[109] Basterra M. L., "La tensión entre el derecho de acceso a la información y la protección de datos personales", *LA LEY*, URL: https://marcelabasterra.com.ar/wp-content/uploads/2021/09/Suple-Constitucional-31-agosto-2021.-La-tenci%C3%B3n-entre-el-D.-a-la-informaci%C3%B3n-y-la-Protecci%C3%B3n-de-datos-personales-Marcela-Basterra.pdf, 2021.

[110] *Idem*.

[111] Gracia Andía M. & Colombato I., "Tensiones entre el derecho al acceso a la información y la protección de datos personales en la vacunación contra el COVID-19 en Argentina", *Revista Digital de Ciencias Sociales*, vol. VIII, núm. 15, pp. 27-54, 2021, Universidad Nacional de Cuyo.

Por su parte, deben protegerse los datos personales de la población, especialmente los datos sensibles. Los Estados, proveedores de servicios de salud y otros actores involucrados en la contención de la emergencia deberán obtener el consentimiento de los titulares al recopilar y compartir datos sensibles. Estos solo deben ser almacenados durante la emergencia y con el fin limitado de abordarla. Los titulares conservarán el derecho a solicitar su eliminación. Más recientemente, en abril de 2021, la CIDH adoptó la resolución 1/2021 "Las vacunas en el marco de las obligaciones interamericanas de derechos humanos". En ella reafirma que los Estados tienen la obligación de proporcionar información adecuada y suficiente sobre estas vacunas y deben contrarrestar la desconfianza que pueda surgir de la sociedad civil, así como fortalecer la confianza en las instituciones de salud pública[112].

Recomienda que los Estados proporcionen proactivamente información procesable, comprensible, útil, veraz y fidedigna sobre los aspectos de interés público relacionados con la campaña de vacunación. Sugiere el uso de formatos abiertos y que se consideren la accesibilidad y las particularidades de los grupos en situación de vulnerabilidad. Los Estados deben salvaguardar los datos personales recolectados por los servicios médicos en los procedimientos de vacunación. Sin embargo, la CIDH aclara que el deber de protección de datos confidenciales no puede menoscabar la obligación de máxima difusión de los Estados con respecto a los procedimientos de inoculación[113].

La CIDH refiere que, con sujeción a la obligación de transparencia activa emanada de la asignación de recursos públicos a la vacunación, los Estados deberán divulgar proactivamente aquella información relativa a la adquisición, importación, distribución, priorización y aplicación de vacunas, así como los procedimientos de vigilancia y control aplicados. También aquellos que reciban recursos públicos para la fabricación, venta, distribución y/o aplicación de vacunas deben transparentar la información relacionada con estas actividades. La CIDH también considera que los Estados deben ajustarse al estricto régimen interamericano de excepciones a la divulgación de información, en la aplicación de reservas de confidencialidad de la información relacionada con las vacunas. De esta manera, la reserva debe estar relacionada con uno de los objetivos legítimos que

[112] *Idem*.
[113] *Idem*.

la justifican y debe superar los criterios de daño y de interés público. Tampoco pueden aplicarse las excepciones en casos de graves violaciones[114].

Así por ejemplo, en febrero de 2021, la Autoridad de Acceso a la Información Pública (AAIP) publicó la "Guía de Acceso a la Información, Datos Personales y Vacunación". El documento destaca que cuando una entidad sujeta a la ley 27.275 divulga información que incluye datos personales, ya sea de forma proactiva o reactiva, se considera una cesión de datos personales realizada "en virtud de una obligación legal" (artículo 1 de la ley 27.275; artículo 5, inciso 2 (b) y artículo 11, incisos 3 (a) y 3 (b) de la ley 25.326). En este sentido, es necesario realizar un análisis caso por caso para evaluar el interés público, ya que el riesgo para la privacidad debido a la divulgación de datos personales y el interés público involucrado pueden variar[115].

La guía reafirma que, en el contexto de una crisis sanitaria y escasez generalizada de vacunas, existe un fuerte interés público en conocer si las vacunas se distribuyen de acuerdo con el plan estratégico del Ministerio de Salud. Durante la emergencia sanitaria, los datos de las personas vacunadas en cumplimiento de esta normativa podrán ser publicados de manera desidentificada (pueden divulgarse datos como edad, sexo, fecha de vacunación y etapa del plan de vacunación, pero no datos que permitan la identificación personal, como nombre o número de identificación). Solo en caso de que la persona haya dado su consentimiento libre, expreso e informado, de acuerdo con el artículo 5 de la ley 25.326, se podrán divulgar datos que permitan la identificación personal[116]. Con este ejemplo, puede visualizarse el equilibrio entre el interés público y la privacidad individual es crucial. La divulgación de datos desidentificados permite que la sociedad acceda a información valiosa sobre la distribución de vacunas sin comprometer la privacidad personal. Sin embargo, la posibilidad de divulgar datos identificativos solo con el consentimiento informado es un enfoque ético y respetuoso de la privacidad individual. Así, desde el punto de vista ético, se exige que se respeten los derechos de las personas a tomar decisiones informadas sobre la divulgación de sus datos personales. Esto se refleja en la mención del consentimiento libre y expreso. Además, la divulgación de datos desidentificados permite la transparencia sin exponer a las personas a riesgos de privacidad.

[114] *Idem*.
[115] *Idem*.
[116] *Idem*.

En relación con la excepción sobre datos personales establecida en la ley 27.275 (artículo 8), la AAIP establece que no puede invocarse si el daño causado a la privacidad es menor que el interés público de obtener la información. En este sentido, se considerarán de interés público aquellos datos relacionados con la transparencia en la gestión pública, asuntos necesarios para el control político sobre las instituciones, hechos relacionados con la administración de fondos públicos, malversación de fondos o incumplimiento en el ejercicio de funciones públicas, y cualquier otra cuestión relacionada con personas que actúan en el ámbito público, como funcionarios públicos o políticos[117].

Por lo tanto, la información sobre si un funcionario público ha recibido una vacuna debe considerarse pública, ya que tienen una expectativa de privacidad menor que el resto de las personas. La ciudadanía debe poder controlar a quién el Estado considera "personal estratégico", ya que su acceso a la vacunación no se basa en cuestiones de salud, sino en su función, por lo que no se aplican las disposiciones de protección de datos sensibles.

Por último, la AAIP enfatiza que el control ciudadano solo puede llevarse a cabo si la información publicada es veraz, completa y oportuna, y que cualquier análisis que implique un test de interés público o una prueba de daño debe considerar el contexto en el que se produce la colisión de derechos o normas.

En resumen, la prueba de interés público, como enfoque para tomar decisiones en situaciones donde se enfrentan derechos individuales y el interés público, refleja la complejidad inherente a los dilemas éticos y legales. En un mundo cada vez más conectado y donde la información fluye constantemente, se encuentran situaciones en las que la revelación de información puede beneficiar a la sociedad en general, pero también puede impactar negativamente la privacidad y los derechos individuales.

La consideración de elementos como la idoneidad, la necesidad y la proporcionalidad en la aplicación de esta prueba permite una evaluación integral de las circunstancias. La idoneidad asegura que el derecho preferente sea el adecuado para lograr un objetivo válido y constitucional. La necesidad plantea la pregunta de si existen alternativas menos invasivas para satisfacer el interés público, lo que garantiza que la revelación de información sea necesaria y no excesiva. La proporcionalidad, por su parte, busca el equilibrio entre el beneficio de la divulgación de información y el daño potencial

[117] *Idem*.

a los derechos individuales, con el objetivo de maximizar el bienestar colectivo sin imponer cargas innecesarias a las personas afectadas.

En última instancia, la prueba de interés público se convierte en una herramienta valiosa para guiar decisiones equitativas y éticas en un mundo donde la información y los derechos individuales a menudo compiten. Su aplicación resalta la importancia de mantener un equilibrio entre el acceso a la información en beneficio del público y la protección de la privacidad y la dignidad de las personas, asegurando que ninguna de estas consideraciones es sacrificada en detrimento de la otra.

V. CONCLUSIONES

En el presente trabajo se buscó visibilizar sobre el impacto entre la inteligencia artificial y los derechos humanos. Durante el desarrollo del mismo, se pueden extraer varias enseñanzas y reflexiones importantes para el mismo.

La digitalización, con el desarrollo de la tecnología de la información y la comunicación, incluyendo la inteligencia artificial, ha provocado una transformación radical en la forma en que las personas viven y trabajan, con avances significativos en eficiencia, productividad y calidad de vida. Sin embargo, esta evolución también ha planteado desafíos en cuanto a la protección de los derechos humanos.

Por un lado, la inteligencia artificial tiene un papel fundamental en mejorar el acceso a la información en el entorno digital, permitiendo reducir la brecha digital y ofrecer servicios más eficientes. No obstante, es crucial garantizar que dicho acceso sea transparente y respete los derechos fundamentales de las personas.

Por otro lado, el uso de la inteligencia artificial implica el manejo de datos personales, lo cual genera inquietudes en términos de privacidad y protección de datos. Por tanto, es fundamental establecer un marco normativo sólido y efectivo que asegure la protección de los datos personales, evitando su uso inapropiado o no autorizado.

En ese sentido, el desarrollo e implementación de sistemas de inteligencia artificial generan desafíos éticos y legales relacionados con la privacidad, confidencialidad, consentimiento informado y control de datos personales. Además, existe el riesgo de crear perfiles discriminatorios basados en información sensible, lo que podría tener un impacto negativo en los derechos humanos. Por tanto, es imprescindible

abordar de manera adecuada las implicaciones legales y éticas de la inteligencia artificial, con el fin de asegurar la igualdad y prevenir la discriminación.

Así, la complejidad de los algoritmos empleados en la inteligencia artificial puede dificultar la comprensión de cómo se toman decisiones y qué datos se utilizan para ello. Por lo tanto, resulta esencial asegurar la transparencia en el funcionamiento de los sistemas de inteligencia artificial, así como establecer mecanismos efectivos de rendición de cuentas en caso de decisiones incorrectas o perjudiciales.

La intersección entre la Inteligencia Artificial, la protección de datos personales y el acceso a la información plantea cuestiones profundas en relación con los derechos humanos. A medida que avanzamos en esta era digital, es esencial abordar estos desafíos de manera colaborativa, involucrando a legisladores, expertos en tecnología y defensores de los derechos humanos para garantizar que los avances en IA se alineen con los valores fundamentales de privacidad, transparencia y empoderamiento de los individuos en la sociedad.

Así las cosas, el marco normativo actual en cuanto a la protección de datos personales puede resultar insuficiente o inadecuado para abordar la rápida evolución tecnológica de la inteligencia artificial. Por tanto, es fundamental adaptar y desarrollar nuevas regulaciones que aseguren una protección adecuada de la privacidad y los derechos de las personas en el contexto de la inteligencia artificial.

Por ello, una de las propuestas de solución al problema resultaría esencial lograr una armonización adecuada entre las normativas de acceso a la información y la protección de datos personales. Esto implica establecer un marco legal claro y coherente que permita conciliar de manera efectiva ambos derechos, evitando conflictos y contradicciones.

La presencia y creciente influencia de la Inteligencia Artificial agrega una capa adicional de complejidad a la colisión entre datos personales y acceso a la información. A medida que los sistemas de IA se vuelven más sofisticados en la recolección y análisis de datos, se generan desafíos únicos en la aplicación de los principios de ponderación y proporcionalidad. La IA puede procesar grandes volúmenes de información de manera rápida y automática, lo que a su vez plantea preguntas sobre cómo se debe equilibrar el acceso a esta información con la protección de la privacidad individual. La toma de decisiones basada en algoritmos complejos también puede oscurecer el proceso de

determinar cómo se llega a ciertas conclusiones, lo que subraya la importancia de la transparencia y la supervisión en la intersección entre la IA y los derechos humanos. Por lo tanto, al analizar situaciones en las que la IA entra en juego en el conflicto entre el acceso a la información y la protección de datos, se vuelve aún más crucial aplicar criterios de ponderación y proporcionalidad para garantizar que las decisiones tomadas sean equitativas y respeten los derechos fundamentales de todas las partes involucradas.

Para el cumplimiento de esos objetivos, resultaría fundamental contar con la participación de autoridades competentes en la materia, como las agencias de protección de datos, para asegurar que las decisiones sean tomadas por expertos con conocimientos especializados en ambos derechos. Estas autoridades deben desempeñar un papel activo en los procesos de solicitud y divulgación de información, garantizando el cumplimiento de los requisitos legales y los principios de protección de datos.

Asimismo, sería de vital importancia impulsar la transparencia y la educación en relación con los derechos de acceso a la información y la protección de datos personales. Esto implica informar a la ciudadanía sobre sus derechos y responsabilidades, así como fomentar una cultura de protección de datos y conciencia acerca de la relevancia de la privacidad en la sociedad digital.

En concordancia con lo anterior, es imprescindible fomentar la cooperación internacional y el intercambio de mejores prácticas en este ámbito. Los países pueden beneficiarse al aprender de las experiencias de otros y colaborar de manera conjunta para enfrentar los desafíos compartidos en relación con el equilibrio entre el acceso a la información y la protección de datos personales.

En el eje central de la investigación, la valoración exhaustiva de los bienes jurídicos en conflicto debe ser meticulosa y compleja, tomando en consideración las características específicas de cada solicitud de acceso a la información. No todas las solicitudes son iguales, por lo tanto, es fundamental evaluar el alcance de la vulneración de la privacidad y el interés público en cada caso.

El test del daño es una herramienta que permite determinar si el beneficio público derivado de la divulgación de la información es superior al daño que podría causar su revelación. Se busca analizar si la divulgación de la información representa un riesgo real, demostrable e identificable de perjuicio significativo a un bien jurídico o derecho claramente protegido por ley.

Al igual que el test del daño, el test del interés público busca equilibrar el beneficio de divulgar la información con el daño que esto puede causar a los derechos individuales de las personas. Se realiza una ponderación entre el interés de retener la información y el beneficio público de divulgarla, considerando criterios de idoneidad, necesidad y proporcionalidad.

Las pruebas de equilibrio entre derechos permiten que el acceso a la información coexista armoniosamente con otras prerrogativas, como el derecho a la privacidad y la seguridad. Los tribunales y la justicia deben aplicar criterios especiales que consideren la proporcionalidad, temporalidad, legalidad y razonabilidad.

Por un lado, es esencial contextualizar las pruebas del daño y del interés público en el marco normativo vigente y en las circunstancias específicas de cada caso, considerando objetivos legítimos e imperiosos, así como riesgos reales, demostrables e identificables, evitando especulaciones o hipótesis.

Por otro lado, la protección de los datos personales, especialmente los sensibles, debe ser garantizada. Los Estados y los actores involucrados en la recopilación y tratamiento de datos deben obtener el consentimiento de los titulares, limitar el almacenamiento de datos al tiempo necesario y asegurar su eliminación una vez cumplido su propósito.

La transparencia y la rendición de cuentas en la gestión estatal, el uso de recursos públicos y el control político son de interés público y deben ser promovidas. Los ciudadanos deben tener acceso a información veraz, completa y oportuna para ejercer un control efectivo sobre las instituciones.

Finalmente, las excepciones a la divulgación de información deben ser aplicadas de manera proporcional, teniendo en cuenta los principios de necesidad y proporcionalidad. Debe demostrarse que el perjuicio al bien jurídico es mayor que el interés público de divulgar la información.

Por eso, estas enseñanzas apuntan a encontrar un equilibrio adecuado entre el derecho de acceso a la información y la protección de datos personales, reconociendo la importancia y los beneficios de ambos derechos para una sociedad democrática y digitalmente avanzada. La búsqueda de soluciones efectivas y equitativas requiere un enfoque multidisciplinario, la participación de todas las partes interesadas y el respeto de los principios fundamentales de los derechos humanos y el Estado de derecho.

Finalmente, es dable destacar que, a medida que la Inteligencia Artificial (IA) avanza y se integra cada vez más en nuestra sociedad, su interacción con el marco jurídico y ético se convierte en un tema crucial. La creación de regulaciones y políticas que aborden cuestiones éticas y de responsabilidad relacionadas con la IA será esencial para garantizar su desarrollo y uso responsable. Los desafíos éticos que rodean la equidad, la transparencia y la toma de decisiones automatizadas también deben abordarse de manera colaborativa y multidisciplinaria, involucrando a expertos en tecnología, juristas, filósofos y defensores de los derechos humanos. La protección de los derechos fundamentales, como la privacidad y la seguridad de los datos, debe seguir siendo una prioridad mientras se fomenta la innovación y el avance tecnológico. En este contexto, la definición de responsabilidad en casos de decisiones tomadas por sistemas de IA y la búsqueda de mecanismos efectivos de rendición de cuentas serán áreas clave de enfoque.

En conclusión, el futuro de la IA será un terreno de evolución constante. A medida que la tecnología continúa transformando nuestras vidas, la sociedad deberá abordar los desafíos éticos y legales de manera proactiva y colaborativa, asegurando que la IA se desarrolle y utilice de manera responsable y en línea con los valores fundamentales de los derechos humanos y la equidad.

BIBLIOGRAFÍA

Artículos en revistas científicas especializadas

A. E. Grigore, "Derechos humanos e inteligencia artificial", *IUS ET SCIENTIA*, Vol. 8, Nº 1, marzo de 2022

Arellano Toledo W. & Ochoa Villicaña A. M., "Derechos de privacidad e información en la sociedad de la información y en el entorno TIC", *Rev. IUS*, vol.7 no.31 Puebla, jun. 2013, URL: https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100010.

B. L. Ibarra Cadena, "Inteligencia artificial y acceso a la información", *MILENIO*, URl: https://www.milenio.com/opinion/blanca-lilia-ibarra-cadena/columna-blanca-lilia-ibarra-cadena/inteligencia-artificial-y-acceso-a-la-informacion.

D. Lonadi, "Inteligencia artificial: ¿Una aliada o un peligro?", *Forbes Argentina*, URL: https://www.forbesargentina.com/columnistas/inteligencia-artificial-una-aliada-o-peligro-n32903, 2023.

E. M. Ferrero & A. Schutz, "Tráfico de datos personales: su afectación a los derechos personalísimos", *Revista Perspectivas de las Ciencias Económicas y Jurídicas*, Vol. 3, N° 2, Santa Rosa: FCEyJ (UNLPam), EdUNLPam, 2013 , p. 57, DOI http://dx.doi.org/10.19137/perspectivas-2013-v3n2a03.

Gracia Andía M. & Colombato I., "Tensiones entre el derecho al acceso a la información y la protección de datos personales en la vacunación contra el COVID-19 en Argentina", *Revista Digital de Ciencias Sociales*, vol. VIII, núm. 15, pp. 27-54, 2021, Universidad Nacional de Cuyo.

I. Covarrubias Cuevas, "Las falencias del test de interés público como instrumento de ponderación entre el acceso a la información pública y la vida privada", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso,* no. 38, Chile, 2012, disponible en https:// scielo.conicyt.cl/.

J. G. Corvalán, "Inteligencia artificial: retos, desafíos y oportunidades - Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia", *Revista de Investigações Constitucionais*, vol. 5, núm. 1, pp. 295-316, 2018.

J. L. Goñi Sein, "Innovaciones Tecnológicas, Inteligencia Artificial Y Derechos Humanos En El Trabajo", *Doc. Labor*, núm. 117-Año 2019-Vol. I, Universidad Pública de Navarra, P. 58.

M. L. Basterra, "La tensión entre el derecho de acceso a la información y la protección de datos personales", *LA LEY*, URL: https://marcelabasterra.com.ar/wp-content/uploads/2021/09/Suple-Constitucional-31-agosto-2021.-La-tenci%C3%B3n-entre-el-D.-a-la-informaci%C3%B3n-y-la-Protecci%C3%B3n-de-datos-personales-Marcela-Basterra.pdf, 2021.

M. L. Basterra, *Acceso a la información pública y transparencia. Ley 27.275 y decreto reglamentario 206/2017. Comentados, anotados y concordados*, Editorial Astrea y Jusbaires. 2017, p. 3

O. A. Mendoza, "El derecho de protección de datos personales en los sistemas de inteligencia artificial", *Revista Del Instituto De Ciencias Jurídicas De Puebla*, Vol. 15, No. 48, México, diciembre 2021.

H. Tórtora Aravena, "Las limitaciones a los derechos fundamentales*", Estudios constitucionales*, vol.8 no.2 Santiago, 2010, URL: scielo.cl/scielo.php?script=sci_arttext&pid=S0718-52002010000200007#n1.

V. Cámara, "Inteligencia Artificial como clave para la preservación del medio ambiente y de la industria forestal", 2023, URL: https://ticnegocios.camaravalencia.com/servicios/tendencias/inteligencia-artificial-como-clave-para-la-preservacion-del-medio-ambiente-y-de-la-industria-forestal/#:~:text=La%20Inteligencia%20Artificial%20tambi%C3%A9n%20se,m%C3%ADnimo%20acerca%20de%20cat%C3%A1strofes%20meteorol%C3%B3gicas.

Jurisprudencia

CIDH, Caso "Claude Reyes y otros", sentencia del 19/09/2006, Serie C No. 151, párr. 91.

Consejo para la Transparencia de Chile, Decisión amparo C926, 12/10/2012, disponible en https://www. consejotransparencia.cl/.

CSJN, 26/03/2014, "CIPPEC c. Estado Nacional - Ministerio de Desarrollo Social s/ Amparo".

Tribunal Europeo de Derechos Humanos, 07/12/1976, Caso "Handyside vs. Reino Unido".

Normativa

Decreto 206/2017 publicado en el BO el 28/03/2017, España.

Estatuto del Consejo de Europa, 1949, disponible en: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=001&CM=8&DF=4/2/2007&CL=ENG.

Ley 11/2002, "Reguladora del Centro Nacional de Inteligencia", España, 2002, URL: https://www.boe.es/buscar/act.php?id=BOE-A-2002-8628

Ley 19.628 sobre Protección de la Vida Privada y protección de datos de carácter personal de Chile publicada el 28/08/1999.

Ley 19/2013 de Transparencia, Acceso a la Información Pública y Buen Gobierno, publicada en el BOE, 10/12/2013, URL: https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887

Ley 27.566 publicada en el BO el 19/10/2020.

Ley General de Transparencia y Acceso a la Información Pública, publicada en el Diario Oficial de la Federación el 04/08/2015.

Ley Orgánica 2/1986, "Fuerzas y Cuerpos de Seguridad", España, 1986, URL: https://www.boe.es/buscar/pdf/1986/BOE-A-1986-6859-consolidado.pdf

Ley Orgánica 3/2018, "Protección de Datos Personales y garantía de los derechos digitales", España, 2018, URL: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

Naciones Unidas, "Declaración Universal de los Derechos Humanos", diciembre 1948, URL: https://www.un.org/es/about-us/universal-declaration-of-human-rights.

Documentos

Acuerdo Regional sobre el Acceso a la Información, la Participación Pública y el Acceso a la Justicia en Asuntos Ambientales en América Latina y el Caribe, firmado el 04/03/2018 en Escazú, Costa Rica.

Agencia de Acceso a la Información Pública de la Nación Argentina, *Resolución de la Agencia de Acceso a la Información Pública Nº 5*, publicada en el BO el 05/02/2018, URL: https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-5-2018-306577.

Asamblea General, *A/HRC/51/17: El derecho a la privacidad en la era digital, Naciones Unidas*, 2022, recuperado en: https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age.

CIDH-OEA, Relatoría Especial para la Libertad de Expresión, "Marco Jurídico Interamericano sobre el derecho de libertad de expresión", 30/12/2009, párr. 87, disponible en http://www.oas.org/es/cidh/expresion.

Comisión IDH, "Informe sobre la compatibilidad entre las leyes de desacato y la Convención Americana sobre Derechos Humanos", en Informe Anual de la Comisión Interamericana de Derechos Humanos 1994, Washington D.C., 1995, disponible en http://www.oas.org/es/cidh/ expresión.

Comisión Interamericana De Derechos Humanos, "Estudio Especial sobre el Derecho de Acceso a l Información", Relatoría Especial Para La Libertad De Expresión, Organización De Los Estados Americanos, 2007, p. 14, URL: http://cidh.oas.org/relatoria/section/Estudio%20Especial%20sobre%20el%20derecho%20de%20Acceso%20a%20la%20Informacion.pdf.

Comité Jurídico Interamericano, "CJI/RES. 147 (LXXIII-O/08)", 2008.

Departamento de Derecho Internacional de la OEA, *Propuesta de Ley Modelo Interamericana 2.0 sobre Acceso a la Información Pública 2.0*, 2020, disponible en http://www.oas.org/es/sla/ddi/acceso_informacion.asp.

Fórum Español para la Prevención y la Seguridad Urbana, "El uso de la inteligencia artificial y los riesgos para la seguridad pública", 2023, URL: https://fepsu.es/el-uso-de-la-inteligencia-artificial-y-los-riesgos-para-la-seguridad-publica/.

Informe del Relator Especial sobre la protección y promoción del derecho a la libertad de opinión y expresión, UN doc. E/CN.4/1998/40.

Informe del Relator Especial sobre la protección y promoción del derecho a la libertad de opinión y expresión, UN doc. E7CN.4/1999/64.

Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo, *Octavo Certamen de Ensayo en Materia de Transparencia y Acceso a la Información Pública*, 2016, disponible en http://www.idaipqroo. org.mx, p. 13.

Inter Press Service, "La Unesco clama por ética urgente para la inteligencia artificial", 2023, URL: https://ipsnoticias.net/2023/03/la-unesco-clama-por-etica-urgente-para-la-inteligencia-artificial/.

Ley Modelo de Acceso a la Información Pública de la Organización de Estados Americanos, aprobada el 29/04/2010 disponible en http://www.oas.org/es/sla/ddi/acceso_informacion.asp.

Ministerio de Asuntos Exteriores, Union Europea y Cooperación, "La UNESCO da un gran paso hacia el primer instrumento normativo sobre la ética de la IA", 2020, URL: https://www.exteriores.gob.es/RepresentacionesPermanentes/unesco/es/Comunicacion/Noticias/Paginas/Articulos/La-UNESCO-da-un-gran-paso-hacia-el-primer-instrumento-normativo-sobre-la-%C3%A9tica-de-la-IA.aspx

Naciones Unidas, "Inteligencia artificial, gobernanza electrónica y acceso a la información", *ONU*, 2022, URL: https://www.un.org/es/observances/information-access-day

Naciones Unidas, "Los riesgos de la inteligencia artificial para la privacidad exigen medidas urgentes –Bachelet", *UN*, 2021, URL: https://www.ohchr.org/es/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet

Naciones Unidas, "Primer acuerdo mundial sobre la ética de la inteligencia artificial", *UNESCO*, 2021, URL: https://news.un.org/es/story/2021/11/1500522

OEA, "Principios Actualizados sobre la Privacidad y la Protección de Datos Personales", *Comité Jurídico Interamericano*, 2021, URL: https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf

ONU, Resolución de la Asamblea General No. 59(1), *Calling of an International Conference on Freedom of Information*, 1946, disponible en: http://daccessdds.un.org/doc/RESOLUTION/GEN/NR0/033/10/IMG/NR003310.pdf?OpenElement

Resolución 268/19 de la Agencia de Acceso a la Información Pública, publicada el 10/01/2020

Resolución AG/RES. (XXXIV-O/04) de 8 de junio de 2004 sobre "Acceso a la Información Pública: Fortalecimiento de la Democracia".

Resolución AG/RES. 1932 (XXXIII-O/03) de 10 de junio de 2003 sobre "Acceso a la Información Pública: Fortalecimiento de la Democracia".

Resolución AG/RES. 2121 (XXXV-O/05) de 7 de junio de 2005 sobre "Acceso a la Información Pública: Fortalecimiento de la Democracia".

Resolución AG/RES. 2252 (XXXVI-O/06) de 6 de junio de 2006 sobre "Acceso a la Información Pública: Fortalecimiento de la Democracia".

TELAM, "Cómo la inteligencia artificial reproduce la discriminación de género", 2023, URL: https://www.telam.com.ar/notas/202303/621747-discriminacion-genero-algoritmos.html.

UNESCO, "El aporte de la inteligencia artificial y las TIC avanzadas a las sociedades del conocimiento: una perspectiva de derechos, apertura, acceso y múltiples actores", 2021, URL: https://unesdoc.unesco.org/ark:/48223/pf0000375796

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

Unión Europea, "Acceso a información", URL: https://european-union.europa.eu/principles-countries-history/principles-and-values/access-information_es, consultado 05/07/2023.