ISSN 3008-9484 | DOI 10.5281/zenodo.14507797 **Diálogos y Voces Judiciales** | Vol. 2, Nº 2 (diciembre de 2024): 1-19

NUEVOS DESAFÍOS DE LA RESPONSABILIDAD CIVIL ANTE LA INNOVACIÓN

New Challenges in Civil Liability Amidst Innovation

Dr. Mariano R. Zurueta[*]

Universidad Nacional de Jujuy
marianozurueta@gmail.com
https://orcid.org/0009-0009-5907-7102

RECIBIDO: 14/11/2024 - ACEPTADO: 21/11/2024

Resumen: La inteligencia artificial y la responsabilidad civil (o derecho de daños) se encuentran vinculados desde el momento en que las máquinas procesan grandes volúmenes de información. Cuestiones como la validez de las decisiones que tomen las máquinas sin intervención humana, en particular si causan daños a terceros, son objeto de este trabajo, el cual se propone visibilizar los supuestos dañosos que plantea la tecnología, la inteligencia artificial, los algoritmos y en concreto los vehículos autónomos, los presupuestos de responsabilidad civil, las propuestas regulatorias en el derecho comparado y en la Argentina, de modo que los damnificados puedan recibir una reparación razonable y proporcionada que a la vez evite una excesiva responsabilidad al dueño o usuario.

Palabras clave: algoritmo, inteligencia artificial, vehículos autónomos.

Abstract: Artificial intelligence and civil liability (or tort law) are connected from the moment machines process large volumes of information. Issues such as the validity of decisions made by machines without human intervention, particularly if they cause harm to third parties, are the focus of this work, which aims to highlight the potential damages posed by technology, artificial intelligence, algorithms, and specifically autonomous vehicles. It examines the foundations of civil liability, regulatory proposals in comparative law and in Argentina, so that victims can receive reasonable and proportionate compensation while avoiding excessive liability for the owner or user.

Keywords: algorithm, artificial intelligence, autonomous vehicles

La tecnología desde hace varias décadas que viene produciendo cambios drásticos en nuestras costumbres (v.gr., TV, radio, teléfono, celular, internet)[1], situación que se ha visto agravada (por su preocupación) con el arribo de la inteligencia artifi-

* Doctor en Derecho (Universidad Nacional de Rosario, 2018), Magister en Derecho Privado (UNR, 2010), Docente de la Cátedra de Derecho Privado (Facultad de Cs. Económicas, Universidad Nacional de Jujuy), y Diplomado en Derecho e Innovación (UNT, 2022). Vocal de la Cámara de Apelaciones en lo Civil, Comercial y Familia de la Provincia de Jujuy.

1 La tecnología irrumpe de manera súbita en la vida de los sujetos para darles mayor confort (automotores, celulares, computadoras, etc.) a punto tal de modificar sus costumbres: hoy en día es normal ver personas caminando en la calle, haciendo fila en los bancos, o cualquier otro trámite, mirando un aparato llamado celular sin siquiera mirar a su alrededor, lo que supone la paradoja de conectarse virtualmente con mucha gente, pero sin atender a las presencias físicas de su entorno.

cial[2], y todo lo que aún falta por descubrir de este nuevo invento, no siendo, ciertamente, el derecho ajeno a ello.

Esta situación de confort y beneficios que aportan los aparatos tecnológicos para la vida de los seres humanos también en muchos casos traen aparejados riesgos y perjuicios para terceros (v.gr., accidentes de tránsito[3], supuestos de electrocución, etc.), lo que supuso que en el siglo XX debiera adoptarse la *teoría del riesgo creado* para dar respuesta legal a esos casos en donde la culpa no resultaba suficiente para imputar al autor material del hecho dañoso (factor objetivo de atribución - arts. 1757, 1758, 1759, 1762 y 1769 CCCN).[4]

En los últimos años el desarrollo tecnológico evidencia nuevos supuestos de responsabilidad civil para analizar, en donde el intérprete jurídico debe dar respuesta de justa reparación frente a estos nuevos casos de lesión a la integridad psicofísica y/o patrimonial a fin de garantizar el principio de no dañar a otros (*alterum no laedere*)[5], sin perjuicio –claro está– del debate necesario que ello supone entre los operadores jurídicos.

---

2 También denominada por muchos como la Cuarta Revolución Industrial, *cf*. Chartzman Birenbaum (2022) y Fossaceca (h.) y Moreyra (2020).

3 En el año 2022 según Luchemos por la Vida, hubo 6.184 muertes por accidentes de tránsito, un 4% de aumento con respecto a 2021 (pero menor al año 2019 que registró 6627 muertes por accidentes de tránsito); algo entendible dado que se continuó incorporando transporte de pasajeros restringido durante la pandemia. https://www.autoweb.com.ar/2023/01/24/accidentes-de-transito-en-2022-hubo-mas-muertos-que-en-pre-pandemia/

4 El Código Civil y Comercial define conceptualmente a los factores objetivos en los arts. 1721 y 1722 al afirmar que la atribución de un daño al responsable puede basarse en factores objetivos o subjetivos, siendo que el factor de atribución será objetivo cuando la culpa del agente es irrelevante a los efectos de atribuir responsabilidad. En tales casos, el responsable se libera demostrando la causa ajena (hecho del damnificado, hecho de un tercero por quien no se debe responder, caso fortuito o fuerza mayor, imposibilidad de cumplimiento, uso de la cosa en contra de la voluntad expresa o presunta del dueño o guardián - arts. 1729 a 1732, 1758, 1° párrafo in fine, y conc. CCCN), excepto disposición legal en contrario. *Cf*. Kemelmajer de Carlucci, A. (Código Civil, Tomo 5), Rinessi (2001).

5 La Corte Suprema de Justicia de la Nación reconoció en tres (3) fallos dictados el mismo día el principio de no dañar a otros como un principio general del derecho y que cuenta con jerarquía constitucional fundado en el art. 19 de la carta magna, y que ciertamente dicho criterio fuera sostenido invariablemente hasta alcanzar su mayor desarrollo en Aquino. Así: CSJN, 5/8/86, Santa Coloma, Luis I. c/ Ferrocarriles Argentinos, JA, 1986-IV-624; CSJN, 5/8/86, Gunther, Fernando Raúl c/ Nación Argentina, ED, 120-522; CSJN, Luján, Honorio c/ Centro Médico del Sud SA, LL, 2000-D-467. El principio *alterum non laedere*, entrañablemente vinculado a la idea de reparación, tiene raíz constitucional y la reglamentación que hace el Código Civil en cuanto a las personas y a las responsabilidades consecuentes no las arraiga con carácter exclusivo y excluyente en el derecho privado, sino que expresa un principio general que regula cualquier disciplina jurídica (considerando 14). IDEM: CSJN,19/12/1995, H. B. T. y otra v. Roveda, Arturo N., LL 1996-C-489; DJ 1996-2-325; CSJN, Lew, Benjamín, Jorge y otro v. Estado nacional-Ministerio del Interior-Policía Federal s/beneficio de litigar sin gastos, Fallos 320:2001; CSJN, 17/9/1996, Empresa Ferrocarriles Argentinos v. Gálvez, Orlando y otros, LL 1997-B-431; ED 174-42, con nota de Jorge Bustamante Alsina; íd., 24/8/1995, P., F. F. v. Empresa Ferrocarriles Argentinos, LL 1995-E-17; CSJN, 24/8/1995, P. F. F. v. Empresa Ferrocarriles Argentinos, LL 1995-

La inteligencia artificial[6] permite la resolución de problemas, la búsqueda de resultados y la adopción de decisiones en poco tiempo mediante la utilización de datos y algoritmos; con ello, lo que intenta la IA es imitar la mente humana por medio de programación de sistemas que aprenden autónomamente[7], sobre la base de un conjunto de datos sobre los cuales un algoritmo hace una predicción (Danesi, 2021)[8].

Si bien no existe consenso en torno al concepto de IA, sí se puede afirmar que es un hito tecnológico que posee habilidades propias de los seres humanos. Quizás, el primer motivo por el cual no haya una definición aceptada de la IA, se debe a que

---

E-17; íd., 21/9/2004, Aquino Isacio v. Cargo Servicios Industriales SA, ED 210-881; LL 2004-F-90. CSJN, 24/8/1995, Pérez, Fredy Fernando v. Empresa Ferrocarriles Argentinos s/sumarios, Fallos 318:1599. ídem: CSJN, 17/3/98, Peón, Juan D. y otra c/ Centro Médico del Sud S.A., LL 2000-D, 467; CSJN, Ontiveros, Stella c/ Prevención ART S.A., La Ley, 23/8/17; *cf*. Pizarro (2013, p. 16) y Picasso (2022, p. 365).

6 Este concepto de IA también engloba muchas otras subáreas como la informática cognitiva (*cognitive computing*: algoritmos capaces de razonamiento y comprensión de nivel superior al humano), el aprendizaje automático (*machine learning*: algoritmos capaces de enseñarse a sí mismos tareas), la inteligencia aumentada (*augmented intelligence*: colaboración entre humanos y máquinas) o la robótica con IA (IA integrada en robots).

Otra distinción de IA es aquella que distingue entre IA débil (*narrow* AI) e IA fuerte (*general* AI). La IA débil es capaz de realizar tareas específicas, y cuyo objetivo es la resolución de problemas. Es decir, si tomamos al ser humano como entidad inteligente de referencia, la IA débil busca el desarrollo de programas que resuelvan problemas concretos y acotados, actuando como si fueran humanos. Independientemente de cómo estén implementados esos sistemas, se busca que se comporten de manera que parezca que poseen inteligencia humana (Martínez y Rodríguez, 2021, p. 46 y ss.). Por su parte, la comunicación 237 (2018) de la Comisión Europea refiere que el término "inteligencia artificial" se aplica a los sistemas que manifiestan un comportamiento inteligente, por ser capaces de analizar su entorno y pasar a la acción —con cierto grado de autonomía— con el fin de alcanzar objetivos específicos. Asimismo, se deja aclarado que los sistemas basados en la IA pueden consistir simplemente en un programa informático (p. ej., asistentes de voz, programas de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento facial y de voz), pero la IA también puede estar incorporada en dispositivos de hardware (p. ej., robots avanzados, automóviles autónomos, drones o aplicaciones del internet de las cosas).

La IA fuerte es capaz de realizar las mismas tareas intelectuales que un ser humano: se busca crear máquinas o sistemas que tengan todas las habilidades mentales de los seres humanos, o incluso que superen la inteligencia humana (super-inteligencia), aunado a la conciencia, sensibilidad, autoconocimiento y sabiduría. No se conoce al día de hoy un sistema de IA fuerte. *Cf*. Danesi (2018a, p. 39).

7 Esto supone que el sistema crea las reglas con base en los datos que le proporcionamos y luego aplica esas reglas para hacer las predicciones, a la par que aprende de las interacciones que hace una vez que es puesto en circulación. *Cf*. Danesi, *op cit*. En el dictamen 2017/C 288/01 del Comité Económico y Social se precisa que el objetivo fundamental de la investigación y del desarrollo en materia de IA es la automatización de comportamientos inteligentes como razonar, recabar información, planificar, aprender, comunicar, manipular, observar e incluso crear, soñar y percibir. *Cf*. Caraballo (2021, p. 273 y ss.), Corvalán (2021, p. 5 y ss.) y Corvalán et al. (2021, p. 15 y ss.).

8 Los algoritmos son un conjunto de instrucciones o reglas para que ejecute una computadora o robot, y que se utilizan para hacer cálculos, resolver problemas y tomar decisiones, pero ese robot solo puede hacer lo que está programado, solo puede moverse según esas instrucciones, a menos que se lo programe para que aprenda nuevas instrucciones. *Cf*. Corvalán *et al*., *ob. cit*., p. 21; Caraballo, *ob. cit*., p. 281 y ss.; y Mohadeb *et al*. (2021, pp. 257-8).

versa sobre una tecnología multidisciplinaria y en plena evolución, cuyos alcances y limitaciones aún no están demarcados; sin embargo, resulta sumamente importante tener en cuenta que los datos –en este contexto– desempeñan un rol fundamental, porque todo el sistema se nutre, mueve y retroalimenta, en función de grandes volúmenes de ellos. Son el alma de la inteligencia artificial.

También puede suceder que esos datos –o conjuntos de datos– presenten *sesgos*, que pueden estar establecidos en el propio conjunto, o ser infundidos por la intervención humana. Ello, desde luego, afecta la transparencia y explicabilidad del sistema, máxime cuando tienen incidencia negativa sobre las personas, porque podrían provocar un trato discriminatorio, que vulnere su derecho a la igualdad y a la no discriminación (Sánchez Caparrós, 2021, p. 302 y ss.).

Aparece, de este modo, la noción de "sesgo algorítmico", entendido este como las respuestas que dan los sistemas de IA, pero que aparecen parciales, prejuiciosas, distorsionadas, y que se agravan cuando afectan derechos humanos, producen discriminaciones, trabajan sobre la base de estereotipos y profundizan diferencias en la sociedad (Danesi, 2021). Estos sesgos pueden ser de diversa índole —históricos, injustos, de interacción, latente y de selección—, pero en todos, lo que subyace y está presente, es la utilización de datos de manera prejuiciosa, y con fines discriminatorios.

Lo anterior destierra la creencia de que los sistemas de IA son neutros y deciden objetivamente, pues "lo cierto es que se entrenan con datos. Si estos datos incluyen sesgos injustos, estos sistemas van a amplificar estructuralmente estos prejuicios provenientes de los datos, consolidando y expandiendo la discriminación, dando lugar a un círculo vicioso que terminará por excluir definitivamente a muchas personas, sobre todo a aquellas que pertenecen a grupos vulnerables" (Sánchez Caparrós, 2021, p. 308).

La situación descripta se agrava frente a técnicas conocidas como de "caja negra", es decir, aquellas a las que –por la manera en que están diseñados los sistemas y su complejidad– no se puede tener acceso, no resulta posible explicar la secuencia que utilizan y que, por tanto, resultan difíciles de controlar. Como derivación, es claro que, si un sistema de IA es entrenado con datos afectados por algún sesgo, los resultados van a expresar el mismo sesgo, reproduciéndolo y hasta ampliándolo, provocando así perjuicios de diversa índole.

Hechas estas definiciones sobre IA, algoritmos y sesgos, en la siguiente sección se analizan los supuestos que la modernización, la robótica y la IA le plantean a la responsabilidad civil, refiriéndonos al caso de los vehículos autónomos. Se hace referencia tanto al derecho comparado como al argentino, además de esbozar algunas propuestas de regulación. En la tercera sección se profundiza en diversas problemáticas legales que presenta la IA. Dado lo novedoso del tema, en la conclusión se sugiere que

no existe una única propuesta regulatoria correcta, siendo aconsejable y necesaria una regulación en supuestos específicos de daños derivados del uso de la IA.

I – INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD CIVIL

La IA y la responsabilidad civil se encuentran vinculados desde el momento en que las máquinas procesan grandes volúmenes de información (en mucho mayor cantidad que la mente humana). Sin embargo, ¿serán válidas o justas las decisiones que tomen por ellas mismas sin intervención humana? ¿Y qué ocurre si con la decisión de la máquina se causan daños a terceros? Y, en dicho caso, ¿quién responde por la eventual indemnización debida? ¿Deben los fabricantes informar los factores que conllevan a adoptar una determinada decisión (en relación con los sesgos algorítmicos)?

En el caso de vehículos autónomos, y los posibles daños a ocasionar, es un tema complejo y en continua evolución, ya que los vehículos autónomos son relativamente nuevos, y se ubican en proceso de desarrollo y pruebas, no existiendo a la fecha leyes y regulaciones claras que contemplen el fenómeno en todos los países, sin que esto último ciertamente obste a que el derecho deba dar una respuesta satisfactoria a la víctima.

En forma preliminar, no cabe duda alguna (al menos hoy en día) que las máquinas no se encuentran (todavía) capacitadas para reemplazar a la decisión humana, en lo que respecta a diversos lineamientos, conductas y diversas consideraciones al momento de juzgar; es por ello que se exige que detrás de cada decisión de las máquinas (utilizando IA) exista una intervención humana en algún estadio del proceso, y que permita avalar esa decisión de la IA.[9]

1. Derecho europeo. Se conocen supuestos de regulación legal en la Unión Europea por parte del Parlamento Europeo, en calidad de recomendaciones (Resoluciones 2020/2012 (INL) y 2020/2014 (INL) (Mohadeb et al., 2021, p. 263) a fin de desarrollar los principios éticos y obligaciones jurídicas ligados al desarrollo, la implantación y el uso de la IA, la robótica y otras tecnologías relacionadas.[10]

---

9 Se sostiene que "la IA tiene un potencial transformador para muchas partes de la vida, desde la medicina hasta la ley y la democracia; sin embargo, plantea profundas cuestiones éticas, sobre aspectos como la privacidad, la discriminación y el lugar de la toma de decisiones automatizada en la vida humana, que inevitablemente tenemos que afrontar tanto como individuos como sociedades… dado que la IA llegó para quedarse, debemos elevar el nivel de debate en torno a la ética de la IA y alimentar el proceso democrático más amplio entre ciudadanos y legisladores. La regulación y la política de la IA son, en última instancia, asuntos para la toma de decisiones democrática", *cf.* Pickles, Q&A with John Tasioulas, Oxford Arts Blog, 11/9/20.

10 Por medio de ello la normativa dictada por el Parlamento Europeo persigue dos cuestiones (entre otras): en

El Parlamento Europeo considera que no es necesario atribuir personalidad jurídica a los sistemas de IA, puesto que hacerlo socavaría el principio fundamental de que los seres humanos, en última instancia, deben seguir siendo responsables de los actos y omisiones de los sistemas de IA. Se persigue que siempre haya una persona responsable que ayude a dar legitimidad a la operación, proporcione una fuente clara de autoridad sobre su funcionamiento, proporcione un elemento de justificación para la decisión interna y proporcione un punto de contacto cuando los usuarios busquen algún recurso en virtud de algún agravio o daño que surja del sistema de IA.

De todos modos, la realidad demuestra que muchas veces resulta problemático identificar a la persona responsable desde un punto de vista práctico (Buyers y Barty, citados por Mohadeb et al., 2021, p. 266). La opacidad, la conectividad y la autonomía de los sistemas de IA podrían llegar a dificultar, o incluso imposibilitar en la práctica, la trazabilidad de acciones perjudiciales específicas de los sistemas de IA hasta una intervención humana específica o decisiones de diseño, y que para evitar una exoneración de responsabilidad, el Parlamento Europeo deja constancia que, de conformidad con conceptos de responsabilidad civil ampliamente aceptados, se puede recurrir a asignar responsabilidad a las diferentes personas que participan en la cadena de valor que, a su forma y en su proporción, crean, mantienen o controlan el riesgo asociado al sistema de IA.

En tal sentido, según el "Informe sobre las implicaciones de seguridad y responsabilidad de la inteligencia artificial, la Internet de las cosas y la robótica" de la Comisión Europea, la responsabilidad debería residir en el operador, sobre bases objetivas y de manera coherente con la legislación sobre responsabilidad por productos

---

primer lugar garantizar y asegurar que las personas que sufran daño serán resarcidas de los eventuales perjuicios sufridos, y a cargo del responsable de dichos daños (función resarcitoria); por el otro lado, las empresas responsables deberán cuidar y evitar causar perjuicios a los usuarios de IA, adoptando las medidas técnicas necesarias y extremando los cuidados respectivos (función preventiva), bajo apercibimiento de tener que pagar indemnizaciones altamente costosas. Se considera que las características de los sistemas de IA, así como la multitud de agentes involucrados, representan un reto importante para la eficacia de las disposiciones del marco de responsabilidad civil de la Unión Europea y de cada Estado miembro, como ser: la complejidad, la conectividad, la opacidad, la vulnerabilidad, la capacidad de ser modificados mediante actualizaciones, la capacidad de autoaprendizaje y su autonomía potencial. Las actividades, dispositivos o procesos físicos o virtuales -gobernados por sistemas de IA- pueden llegar a ser técnicamente la causa directa o indirecta de un daño o un perjuicio, **pero casi siempre son el resultado de que alguien ha construido o desplegado los sistemas o interferido en ellos.** En este sentido, las futuras leyes tendrán que respetar los siguientes principios: una IA antropocéntrica y antropogénica (o sea, sustentada en una intervención humana); seguridad, transparencia y rendición de cuentas; salvaguardias contra el sesgo y la discriminación; derecho de reparación; responsabilidad social y medioambiental; el respeto de la intimidad y protección de los datos. Además, las tecnologías de IA que presenten un riesgo elevado deben estar diseñadas para que siempre estén bajo supervisión humana. Es así que cuando se utilice una función que pudiera atentar gravemente contra los principios éticos y resultar peligrosa, las capacidades de autoaprendizaje deberán desactivarse y se deberá restaurar plenamente el control humano.

defectuosos dentro de la Unión Europea[11], la cual ha demostrado ser durante muchos años un medio eficaz para obtener una indemnización por un daño causado por un producto defectuoso, pero que, no obstante, debe ser objeto de una revisión para adaptarla al mundo actual –es decir, digital– y abordar los retos que plantean las tecnologías digitales emergentes. De esta forma, se garantizaría un elevado nivel de protección efectiva de los consumidores y de seguridad jurídica para ellos y las empresas.

En cuanto a los modelos de regímenes de responsabilidad civil derivada de los sistemas de IA, el Parlamento Europeo propone dos regímenes de acuerdo con su grado de riesgo:

a) Un régimen objetivo de responsabilidad para sistemas de alto riesgo de IA: en donde el operador no podrá eludir su responsabilidad demostrando la debida diligencia o que el daño fue causado por una actividad, un dispositivo o un proceso autónomo gobernado por su sistema de IA; la única eximente es el daño causado por fuerza mayor; y estableciendo un tope indemnizatorio máximo de 2 millones de euros en caso de fallecimiento y/o daños físicos, y de 1 millón de euros para daños morales significativos que resulten en una pérdida económica verificable o en daños a la propiedad; y la contratación obligatoria de un seguro de responsabilidad civil acorde con los montos establecidos; y

b) un régimen de responsabilidad subjetivo para sistemas de bajo riesgo de IA: en este caso, el operador estará sujeto a responsabilidad subjetiva (culpa o dolo) respecto de todo daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por el sistema de IA, y no será responsable si: 1) el sistema de IA se activó sin su conocimiento, al tiempo que se tomaron todas las medidas razonables y necesarias para evitar dicha activación fuera del control del operador; 2) se observó la diligencia debida a través de la realización de las siguientes acciones: la selección de un sistema de IA apropiado para las tareas y las capacidades adecuadas, la correcta puesta en funcionamiento del sistema de IA, el control de las actividades y el mantenimiento de la fiabilidad operativa mediante la instalación periódica de todas las actualizaciones disponibles. Además, no será responsable si el daño o perjuicio ha sido provocado por un caso de fuerza mayor. Sin embargo, se prevé una garantía para el usuario o consumidor al responsabilizarse igualmente al operador si el daño fue causado por un tercero que haya interferido en el sistema de IA al modificar su funcionamiento si dicho tercero es ilocalizable o resulte insolvente (Comisión Europea, 2020, 64).

---

11 Directiva 85/374/CEE del Consejo, del 25/7/85, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados Miembros en materia de responsabilidad por los daños causados por productos defectuosos, disponible en https://eur-lez-europa.eu/legal-content/ES/ALL/?uri=celex%3A31985L0374

En los Estados Unidos no existe legislación federal sobre responsabilidad civil en materia de IA. Sin embargo, algunos estados han regulado algunos aspectos de esta temática, en concreto sobre vehículos autónomos, condiciones para que puedan operar, requisitos de testeo y funcionamiento en la ciudad, estableciendo responsabilidades tanto para el conductor como los fabricantes por cualquier defecto en sus productos, ya sea por fallas en su tecnología o en el diseño del vehículo.

2. Derecho argentino. En la Argentina no existe una regulación específica sobre responsabilidad civil en materia de IA, existiendo diversas opiniones al respecto, ya que para algunos juristas es necesaria su reglamentación específica mientras que, para otros, puede resultar más conveniente, si resulta posible, encuadrar las situaciones que surjan con motivo del uso de la IA en las normas jurídicas ya existentes.

El Código Civil y Comercial (CCCN), y otras leyes eventualmente aplicables (Ley de Defensa del Consumidor Nº 24.240 y modif., Ley de Defensa de la Competencia Nº 27.742, Ley de Lealtad Comercial Nº 22.802, etc.), ¿son capaces de dar una respuesta satisfactoria a este fenómeno de provocación de daños a terceros por medio de utilización de artefactos que emplean IA?

Por lo pronto, si bien podría llegar a pensarse que los presupuestos de la responsabilidad civil se mantienen vigentes en tales supuestos (daño, antijuridicidad, relación causal y factor de atribución), mayores dudas se plantean en lo que respecta a los sujetos u otras cuestiones (como son el autoaprendizaje y autonomía de la IA) que difieren de los supuestos clásicos del derecho de daños.

Para ello, la doctrina sugiere aplicar los principios generales vigentes del derecho contractual, de las normas sobre propiedad intelectual, defensa del consumidor y privacidad y protección de datos personales vigentes, así como las del Código Civil y Comercial de la Nación (Repond, 2020; Fossaceca y Moreyra, 2020; Danesi, 2018a, p. 8).

En nuestro derecho una herramienta fundamental en este aspecto radica en la prevención del daño, la cual se encuentra regulada en el art. 1710 y ss. del CCCN. La tutela sustancial inhibitoria tiene como objeto directo la prevención del daño mediante una orden para impedir (en caso de amenaza de lesión) o bien para que cese su producción (si la actividad ofensiva ya se ha iniciado y es previsible su continuación o reiteración… Constituye una protección judicial de urgencia sustantiva y no cautelar y cuyos presupuestos son un comportamiento lesivo, un daño injusto y una relación de causalidad adecuada entre dicho comportamiento y el daño causado).[12]

---

12 *Cf.* Lorenzetti (1995); y Andorno (1995), receptado por la Corte Suprema de Justicia de la Nación Argentina en el *leading case* "Camacho Acosta, Máximo c/ Grafi Graf SRL y otro", LL 1997-E-652. Véanse también: Galdós (2020, pp. 305-6), Peyrano (2015) y Pizarro y Vallespinos (2018, pp. 835-6).

El mandato constitucional previsto en el art. 43 CN (en concordancia con los arts. 1.710/1.713, y 1.973 del CCCN) es claro: se debe primero evitar el daño. Es que el Código Civil y Comercial consagra de manera expresa y absolutamente amplia un deber general de prevención, que hace a la llamada responsabilidad civil preventiva.[13] Con ello, los requisitos de procedencia de la acción preventiva son (Pizarro y Vallespinos, 2018; Zavala de González, p. 211; Ossola, p. 115):

a) una acción u omisión con razonable aptitud causal para generar un peligro de daño no justificado;

b) la conducta riesgosa debe ser antijurídica;

c) razonable previsibilidad de la producción, continuidad o agravamiento del resultado nocivo, ponderada en base a estándares de causalidad adecuada;

d) amenaza de un interés no ilegítimo, patrimonial o extrapatrimonial, individual o colectivo del accionante; y

e) posibilidad material de detener el efecto lesivo.

En materia de IA, los expertos se preguntan si quien ha desarrollado una IA determinada tiene un "deber legal" de prevenir daños causados a terceros, cuando tiene conocimiento (o lo debiera tener) de que su herramienta es apta para causar daños, y que con el aporte o información a proveer por el fabricante puede evitarlos, mitigarlos o hacerlos cesar. A ello, se responde que el deber de prevención recaerá en todos aquellos sujetos que, material o jurídicamente, estén en condiciones de prevenir daños, siempre y cuando no se requiera un esfuerzo excesivo y/o extraordinario del sujeto al cual se le atribuiría responsabilidad.

Así, los propietarios de una IA que tengan aptitud para prevenir daños podrán ser legitimados pasivos de los planteos o acciones entabladas por aquellas personas que acrediten un interés razonable en la prevención del daño (*cf.* arts. 1710 y 1711, CCCN; Chamatropulos, 2017). En nuestro país se considera que la obligación en cabeza de quien desarrolla una IA determinada, además de no exigírsele un accionar anormal o extraordinario, deberá tener presente dos limitaciones de importante impacto práctico: la menor restricción posible de derechos del sujeto en cuestión y la exigencia de que lo que se le peticiona constituya el medio más idóneo para lograr el objetivo preventivo (*cf.* art. 1713, CCCN). Caso contrario, el deber de prevención no nacerá (Chamatropulos, 2017).

En nuestro ordenamiento legal a los daños causados por la IA pueden serle aplicables la responsabilidad objetiva contenida en los arts. 1757 (hecho de las cosas y actividades riesgosas), 1758 (sujetos responsables) y 1769 por los daños derivados de

---

13 Despacho unánime de la Comisión 4 de las Jornadas Nacionales de Derecho Civil, La Plata, septiembre/17. *Cf.* también Pizarro y Vallespinos, *op. cit.*, pp. 816 y 822.

los accidentes de tráfico (de eventual aplicación a los vehículos autónomos), supuestos en los cuales el dueño y el guardián de la cosa responden en forma concurrente, no pudiendo eximirse por errores en la conducción causados por la IA, tal como se concluyó en las XIX Jornadas Nacionales de Derecho Civil celebradas en septiembre de 2024 en Pilar (véase también: Danesi, 2018a).[14]

En lo que respecta a los eximentes de responsabilidad, se descarta la eventual autorización administrativa que pudiere existir, o el cumplimiento de técnicas de prevención (art. 1757 CCCN), con lo cual queda únicamente como supuesto de eximición de responsabilidad el caso fortuito o fuerza mayor (art. 1730 CCCN).

Además, en esta materia, se deberá tener especial consideración por el *software*, el cual puede ser reparado, actualizado o revisado por el productor del sistema, por componentes individuales del sistema o por terceros, de una manera que puede afectar la seguridad de estas tecnologías (Danesi, 2018a). En estos casos, las tareas mencionadas respecto al software están a cargo de un sujeto en particular que, para la doctrina, puede revestir el carácter de "guardián", definido en el art. 1758 del CCCN: "se considera guardián a quien ejerce, por sí o por terceros, el uso, la dirección y el control de la cosa, o a quien obtiene un provecho de ella", siendo el productor el sujeto responsable (conf. arts. 1757, 1758 y 1769 del CCCN), en tanto y en cuenta no acredite (para eximirse) que la cosa fue usada en contra de su voluntad expresa o presunta (art. 1758 CCCN), y de dudosa aplicación en el ámbito de la responsabilidad de defensa del consumidor o por productos defectuosos (Danesi, 2018a, p. 26).

3. Para ir sentando algunas ideas. Como se vio *ut-supra*, algunos autores proponen un régimen de responsabilidad autónomo de la IA, atribuyendo una personalidad jurídica a los robots programados con IA. De esta forma, consideran la idea de una "personalidad electrónica" (Valente, 2019, p. 24). En estos casos, los robots o "personas ciber físicas" serán capaces de desarrollar una individualidad/autonomía "propia o autónoma" a partir de su interacción independiente con el entorno, por lo que consideran estos autores que no sería justo imputar a los programadores y/o fabricantes las decisiones que tomen estas entidades con base en su propio aprendizaje (Zapata Sevilla, 2019).

Esta postura entiende que el dictado de una normativa es indispensable, al garantizar una transición digital ordenada y, al mismo tiempo, brindaría certeza jurídica a la sociedad que pudiera verse afectada por ella aún de manera indirecta (García, 2019).

Con ello, el programador sólo será responsable por los daños causados por los robots cuando se encuentren relacionados con defectos en el software, fallos o

---

14 *Cf.* https://www.casi.com.ar/videoteca/14

errores; ya que está en mano del programador la tarea de realizar una adecuada labor de determinación de los patrones de actuación y limitar en base a los derechos fundamentales y libertades humanas a la máquina[15]. En cambio, de producirse sucesos que no hubieran podido preverse, o que, previstos, fueran inevitables, no parecería correcto atribuirle la responsabilidad al programador.

4. *¿Es obligatorio en materia de producción de IA contratar un seguro?* Se propone la asignación de un seguro que pueda ser responsabilizado por dichos daños causados por la IA, siendo un problema de implementación jurídica dotar al robot de una identificación única, crear un registro e imponer un seguro obligatorio a cargo de quien o quienes, directa o indirectamente, se sirven de su actividad (Valente, 2019, pp. 22-4). [16]

En la Unión Europea se propone la creación de un seguro obligatorio (similar al de los vehículos automóviles) con cargo de los fabricantes o a los propietarios y usuarios; o fondos de compensación ante la inexistencia de seguros. Ello supondría que el fabricante, programador o usuario puedan beneficiarse de un régimen de responsabilidad limitada en caso de contribución a un fondo o suscripción de seguros. Otra propuesta es la creación de patrimonios individuales por robot o para todos los robots con el pago único por su introducción al mercado o pagos periódicos, y la creación de un número de matrícula o registro del robot que lo vincule con un fondo en particular. Esto último está vinculado a la idea de la creación de una personalidad electrónica responsable de reparar los daños que pueda causar (con un patrimonio que respalde a la misma)[17] según se vio *ut-supra*.

---

15 *Cf*. "¿Cómo se debería medir la responsabilidad legal de la IA?", disponible en https://www.syntonize.com/como-medir-responsabilidad-legal-ia/

16 Así, la Unión Europea propone permitir que el fabricante del software, su programador, el propietario y hasta el usuario puedan beneficiarse de un régimen de responsabilidad limitada si aportan a un fondo de compensación, o bien si suscriben conjuntamente un seguro que garantice la compensación de daños o perjuicios causados por un robot. *Cf*. Danesi (2018b).

17 La propia Unión Europea ha reconocido que: "En el supuesto de que un robot pueda tomar decisiones autónomas, las normas tradicionales no bastarán para generar responsabilidad jurídica por los daños ocasionados por el robot, ya que no permitirán determinar la parte que ha de hacerse cargo de la indemnización, ni exigir a dicha parte que repare el daño ocasionado (...) En materia de responsabilidad extracontractual podría no ser suficiente el marco ofrecido por la Directiva 85/374/CEE (...) que solo cubre los daños ocasionados por los defectos de fabricación de un robot a condición de que el perjudicado pueda demostrar el daño real, el defecto del producto y la relación de causa a efecto entre el defecto y el daño (responsabilidad objetiva o responsabilidad sin culpa) (...).
El marco jurídico vigente no bastaría para cubrir los daños causados por la nueva generación de robots, en la medida en que se les puede dotar de capacidades de adaptación y aprendizaje que entrañan cierto grado de imprevisibilidad en su comportamiento, ya que un robot podría aprender de forma autónoma de sus experiencias concretas e interactuar con su entorno de un modo imprevisible y propio únicamente de ese robot" (Parlamento Europeo, 2017).

II - DIVERSAS PROBLEMÁTICAS LEGALES QUE PRESENTA LA IA

Los fabricantes de vehículos autónomos[18] y los proveedores de tecnología pueden ser considerados responsables de los accidentes causados por fallas en la tecnología o en el diseño del vehículo. Sin embargo, en los casos en que los conductores humanos también estén involucrados en el accidente, la responsabilidad puede dividirse entre el conductor humano y el fabricante del vehículo autónomo.

La innovación tecnológica, y la IA en particular, genera muchos beneficios en las personas, en su confort, comunicaciones, seguridad, etc., pero al mismo tiempo puede ser muy perjudicial a diversos derechos humanos, como la privacidad, discriminación, accidentes, etc., sumado al hecho de la dificultad para encontrar un responsable a la pluralidad de sujetos intervinientes (fabricantes de software, programadores, operadores, etc.), sin perjuicio de que ello se ve agravado por el hecho de que este tipo de tecnologías requieren de manera continua la actualización del software lo que implica que puede verse comprometida la seguridad del producto original con posibles daños a las personas.

Además, los sistemas de IA –en un primer momento– son programados por una persona, pero luego la IA procesa datos, aprenden de estos y toma decisiones independientes que no necesariamente estarán relacionadas con la programación o el diseño inicial (autonomía), y ello dificulta la atribución de responsabilidad por daños porque las normas vigentes (ya sean las del Código Civil y Comercial o las de la Ley de Defensa del Consumidor) presuponen la trazabilidad del daño (atribuible al dueño o guardián, fabricante, diseñador, operador, usuario), pero en los casos más nuevos estas reglas resultarán insuficientes en la medida que no se podría identificar la parte que causó el daño, esto es, si fue por decisión autónoma de la IA o por un defecto del producto, y allí tendremos un problema de autoría del daño.

Es que en este ámbito identificar la causa de la falla de la IA será la clave para encontrar la relación de causalidad en el régimen del derecho de daños del derecho común, y también lo es para establecer el nexo entre el daño y el defecto en el régimen de la responsabilidad por productos elaborados. Se ha argumentado que a los fines de hacer la IA más explicable, y así superar esta dificultad, los diseñadores deberían revelar los códigos de los algoritmos e implementar alguna forma de registrar todos los aspectos de su funcionamiento (fenómenos de los algoritmos de caja negra), lo que permitiría reconstruir y entender las causas de su comportamiento y

---

18 Estos vehículos autónomos cuentan con un Sistema de Conducción Automatizado (ADS, por su sigla en inglés), consistente en una tecnología instalada en un vehículo motorizado que tiene la capacidad de conducir el vehículo en modo de automatización alta o completa, sin supervisión de un operador humano y posee la capacidad de llevar automáticamente al vehículo a una condición de riesgo mínimo en caso de una falla crítica del vehículo o del sistema u otro evento de emergencia.

facilitaría la atribución de responsabilidad, ya que es sumamente dificultoso rastrear el proceso completo de la operación, siendo útil recurrir a la teoría de las cargas dinámicas, merced a la cual se aligera la labor probatoria del damnificado, emplazándola en cabeza de quien se encuentre en mejores condiciones para ello. En estos casos, serán, sin duda, programadores, productores, entre otros (Melo, 2021).

La multiplicidad de nocimientos que pueden provocarse y la necesidad de precisar su causa han motivado que se exija que pese sobre los productores el deber de equipar sus sistemas con medios de grabación para registrar la información y procesamientos en cada operación tecnológica realizada, ya sea por un robot, ya sea por un algoritmo o cualquier otro producto con IA. A este sistema se lo conoce con la denominación de *logging by design*. Por medio de este sistema se podrá conocer cómo acontecieron los hechos previos al daño, de modo de conocer la influencia en el perjuicio por parte de la IA.[19]

El *logging* debe cumplir las reglas que atañen a los datos personales y secretos comerciales. Se debería permitir el acceso al damnificado, a los productores y a la compañía aseguradora. También debería gozar de sistemas de seguridad que previniesen la alteración de datos. En el caso de que los productores no cumplieran con este deber, se les asignaría una responsabilidad objetiva y deberían responder por los daños ocasionados, no solo materiales, sino también por la falta de colaboración al no equipar la tecnología con el sistema de *logging* necesario (Fossaceca y Moreyra, 2020).

Estrechamente vinculado con el denominado fenómeno de caja negra se encuentra la naturaleza imprevisible de las IA más nuevas, ya que funcionan sobre la base de aprendizaje no supervisado: tales son los supuestos de IA basados en mecanismos de *deep learning*. Esta ausencia de previsibilidad exige reflexionar sobre los presupuestos de la responsabilidad civil.

Algunos consideran que esta falta de previsibilidad también obsta a la aplicación del estatuto del consumidor con las normas sobre responsabilidad por productos elaborados en la medida que el fabricante difícilmente podría incluir información acerca de riesgos impredecibles que podría presentar el producto. Así, resultarían inaplicables a este supuesto la doctrina y la jurisprudencia sobre responsabilidad del fabricante por daños causados por defectos de información (Melo, 2021).

Los vehículos autónomos –en determinadas ocasiones– puede que se sepa cómo van a actuar (v.gr.: detenerse ante determinadas señales de tránsito o disminuir la velocidad, o evadir un determinado peligro). Sin embargo, en otras ocasiones (su-

---

19 V.gr., en el supuesto de un accidente entre vehículos automatizados, permitiría reconstruir la cadena causal y descubrir qué rodado ocasionó el choque al no responder a una señal que el otro vehículo habría mandado. *Cf*. Fossaceca y Moreyra (2020).

puestos no previstos por la máquina) habrá incertidumbre y no se va a saber con seguridad, o previsibilidad, cómo van a actuar ante determinados escenarios que plantea el tráfico.

Los conflictos pueden terminar por quedar comprendidos en: ¿qué vida salvar, o qué daño evitar?, ¿salvar la vida del usuario del vehículo o del peatón u otro usuario de la vía?, ¿quién tiene prioridad?, ¿por qué y cuándo se toma esa decisión?, y finalmente el interrogante que surge es si sería posible reducir la toma de decisiones no previstas en el tránsito a cuestiones matemáticas, siendo negativa la respuesta a esa pregunta, ya que no resulta ser suficientemente seguros los cálculos matemáticos en cuanto a previsibilidad (Martínez Mercadal, 2022).[20]

Por un lado, es cierto que estos vehículos suponen una mayor seguridad y por momentos deberían ser más predecibles que los humanos, en cuanto a respetar normas y señalización, pero la imprevisibilidad surge precisamente de la complejidad de los algoritmos y de su combinación con la experiencia adquirida; y que precisamente la mejor "decisión" según la diligencia debida del buen padre de familia puede no coincidir con la respuesta matemática (Balkin, 2015, citado por Martínez Mercadal, 2022).

En todo caso, la respuesta resarcitoria a favor de la víctima dentro del derecho de daños debe ponderar que no puede frenarse la investigación tecnológica y sí buscar otro tipo de respuestas, ya que hoy en día el ser humano es cada vez más consumi-

---

20 En el vehículo autónomo inteligente, la ciencia no ha logrado consagrar una previsibilidad cierta ante la complejidad del tránsito. Y cuanta más autonomía tenga, y mayor sea la toma de decisiones, mayor será la incertidumbre e imprevisibilidad. Los humanos ya no seremos conductores sino usuarios, lo que nos conduce a sostener que para usar un vehículo ya no se debe necesariamente saber conducir, o tener licencia habilitante o no haber consumido alcohol o estupefacientes o, ¿debe igualmente el usuario estar atento?; ¿puede el usuario detener una acción que entienda que es previsible del coche automático?; ¿debe siempre el usuario del vehículo poder tomar el control del mismo?; ¿debería la ley exigir que viaje en el vehículo un conductor con licencia habilitante cuando el auto se conduce solo?; ¿debería el usuario tener una preparación especial para tomar control del vehículo o su licencia habilitante actual ya se lo permite?; ¿cómo evaluamos estos puntos desde el análisis de la incidencia en el derecho de daños ante un accidente?; ¿cambiará un concepto importante para las leyes del tránsito como lo es el de conductor? Estos vehículos deben poder acceder a un sistema que les permita responder a tres preguntas: ¿dónde están ubicados?, ¿qué objetos están a su lado?, ¿hacia dónde es deseable, legal y seguro, realizar el próximo movimiento? Deben ser capaces de captar señales de tránsito, tanto cartelería como lumínicas, y poder desplazarse en un ambiente con otros objetos en movimientos, otros vehículos, peatones, ciclistas, y hasta obstáculos (baches, obstáculos en el camino como una reparación de la calzada o ruta) y hasta deben saber qué hacer en caso de existir otro accidente de tránsito. La tecnología desarrollada implica: a) sensores, radares, cámaras de video, para recoger información en vivo y en tiempo real de los alrededores, calcular velocidad, movimientos, ángulos, reflejos y también la incorporación de una caja negra lo que implicará una mayor información ex post en caso de siniestro, entre otra tecnología; b) mapas digitales y la posibilidad de su actualización online (lo que conlleva una eventual discordancia de información entre el tiempo real y la información almacenada, lo que también puede convertirse en una nueva tragedia); y c) sistema de coordinación computarizado. La posibilidad de combinar los dos anteriores y tomar una decisión; que en puridad es una respuesta matemática sobre dónde es deseable mover el vehículo a la próxima dirección según Surden y Williams, citados por Martínez Mercadal (2022).

dor de la innovación y desea mayores avances tecnológicos en los productos.[21]

Dentro de las personas responsables por los accidentes de automotores autónomos tenemos al propio usuario, al dueño del vehículo, al fabricante del vehículo, el fabricante de los componentes del vehículo o el software, las autoridades gubernamentales de control y seguridad vial, etc. (Gurney, 2013, citado por Martínez Mercadal, 2022).

Pero en el caso de los sistemas de vehículos autónomos y más aún los totalmente autónomos e inteligentes, el rol del usuario es bastante pasivo, por lo que surge la siguiente pregunta: ¿los fabricantes deberán responder de todos los accidentes de tránsito? Habrá casos fáciles y claros de resolver imputando responsabilidad objetiva a los fabricantes por productos defectuosos (es decir, falla de fabricación, o la utilización de un diseño que no es acorde con el estado de la ciencia o arte, o falta de información al usuario). Sin embargo, podrán existir otros casos en donde el accidente fue causado por una decisión que –de acuerdo a la fabricación, diseño e información– fue correcta, producto de un cálculo matemático de las posibilidades de la información recibida, y con ello el fabricante estaría exento de responsabilidad.

Algunos autores incluso consideran que ello va a complejizar los juicios de responsabilidad por accidentes de tránsito, ya que la víctima deberá contratar expertos matemáticos y científicos para poder descubrir el error en el algoritmo matemático que causó el accidente, aún en sistemas de responsabilidad objetiva (con fundamento en el derecho del consumidor o por productos defectuosos).

Otra teoría (Gurney, 2016) entiende que el fabricante debe ser considerado no como tal, sino como un conductor fictamente al que se le debe aplicar estándar de *conductor razonable* ("reasonable autonomus vehicle driver": literalmente, estándar de conducta razonable del conductor autónomo), y con ello evitar las discusiones sobre defecto de fabricación, diseño o información que podrían complejizar el juicio de responsabilidad civil por accidentes de tránsito.

Esta solución, que procura desojarse de los dolores de cabeza de la cuestión del producto defectuoso, también merece reproches y cuestionamientos ¿no termina complejizando aún más el accidente de tránsito ingresando la diligencia debida dentro de los algoritmos?, ¿cuál es la conducta debida por un robot o del fabricante? Los estándares de comportamiento (sea ya el buen padre de familia, el buen hombre de negocios y ahora el buen conductor autónomo) parten de la base del problema inicial planteado: la previsibilidad de conductas. Que es lo que la sociedad, o determinados sectores de ella (la familia, el mercado, o la seguridad vial) esperan de una

---

21 Expresa la Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)), 16.2.2017, P8_TA [2017]0051, que "resulta de vital importancia que el legislador pondere las consecuencias jurídicas y éticas sin obstaculizar con ello la innovación".

persona. Pero de una persona, no de un robot dotado de inteligencia artificial con mecanismos de aprendizaje y conductas o comportamientos que escapan del control humano.

Otra postura considera que a los vehículos autónomos se los debe equiparar con el régimen de los animales domésticos, y así el usuario o propietario, en su caso, son guardianes de la cosa por cuando se sirven de la misma en su provecho.[22]

La propuesta estiva por considerar a los robots como los nuevos animales, y se propone el siguiente esquema: en primer lugar, determinar si estamos ante un caso de responsabilidad del fabricante en caso de accidente en ocasión de producto defectuoso. La propuesta parte de este supuesto, pero no quiere dejar librada toda la responsabilidad a los fabricantes. Absolver al consumidor usuario y responsabilizar al fabricante sobre la base del régimen general de responsabilidad por productos (claro está con el dilema antes expuesto). Si el fabricante es responsable, la solución del accidente de tránsito queda en esos términos. Pero si no lo es, la propuesta es considerar a los robots, como los nuevos animales del siglo XXI en cuanto a la atribución de responsabilidad, imputando la misma al usuario o propietario del vehículo por el accidente causado que no obedezca a un defecto de producto, lo que en nuestro sistema nos reconduce por la responsabilidad por el hecho de las cosas. Los autores postulan que la IA termina por ser más asimilable a un animal doméstico con cierta dosis de previsibilidad; por la información cargada. Expresan que la imprevisibilidad no es total, como puede ser la de un comportamiento de un animal salvaje o feroz en nuestro sistema. Sin embargo, se vuelve a las mismas críticas realizadas al subsistema de responsabilidad por hecho de las cosas, siendo patente la responsabilidad por falta de mantenimiento o de actualización de los sistemas informáticos, pero en otros casos la incertidumbre persiste.

III - CONCLUSIÓN

De todo el desarrollo efectuado en el presente trabajo de lo que a este autor surge claro es que no existe al día de hoy una única propuesta regulatoria correcta, siendo muy novedoso el tema a nivel mundial, y más aún en nuestro derecho argen-

---

22 Artículo 1757 CCCN. Hecho de las cosas y actividades riesgosas: “Toda persona responde por el daño causado por el riesgo o vicio de las cosas, o de las actividades que sean riesgosas o peligrosas por su naturaleza, por los medios empleados o por las circunstancias de su realización. La responsabilidad es objetiva. No son eximentes la autorización administrativa para el uso de la cosa o la realización de la actividad, ni el cumplimiento de las técnicas de prevención”. Artículo 1758. Sujetos responsables: "El dueño y el guardián son responsables concurrentes del daño causado por las cosas. Se considera guardián a quien ejerce, por sí o por terceros, el uso, la dirección y el control de la cosa, o a quien obtiene un provecho de ella. El dueño y el guardián no responden si prueban que la cosa fue usada en contra de su voluntad expresa o presunta. En caso de actividad riesgosa o peligrosa responde quien la realiza, se sirve u obtiene provecho de ella, por sí o por terceros, excepto lo dispuesto por la legislación especial".

tino, siendo aconsejable y necesaria una regulación en supuestos específicos de daños derivados de IA.[23]

Particularmente me parece sumamente interesante la constitución de seguros obligatorios a cargo de los dueños y usuarios de dichos vehículos autónomos, pero deberá contar con una adecuada regulación por la autoridad de aplicación de modo de evitar los problemas existentes en materia de seguros en la Argentina, en donde se aprecian muchos casos de impunidad o víctimas sin ser indemnizadas por la insolvencia de las compañías de seguros.

Otra cuestión de la que no surge duda es que se debe proseguir con la investigación y desarrollo de encuentros académicos que aborden esta cuestión puesto que la tecnología (desde hace varias décadas) existe y avanza sumamente rápido en un mundo cada vez más consumerista. A tales efectos será necesario capacitarse en la temática y escuchar propuestas de los estudiosos y expertos en IA con el fin de poder crear normativa acorde a la tecnología en cuestión, normativa que deberá ser permeable a los cambios e innovaciones que suponen la tecnología.

La aplicación del derecho no solo puede incentivar buenas prácticas y un avance acorde y armonioso de la IA, sino también sancionar conductas inapropiadas o ilegales, y otorgando una reparación razonable y proporcionada para aquellos que han sido perjudicados por la IA (Mohadeb et al., 2021, pp. 257-8).

Por último, resultará crucial entender la verdadera naturaleza de estos fenómenos tecnológicos con IA para poder contar con una regulación acorde a ello, de modo que pueda entenderse adecuadamente el fenómeno de la manera más abarcativa, en tutela de las víctimas, pero sin que ello suponga un exceso de responsabilidad sancionatoria en contra del sindicado como responsable.

La doctrina argentina se encuentra abocada al estudio de esta temática[24], lo cual celebramos, de modo que los operadores del derecho puedan arribar a soluciones lógicas, fundadas en derecho y sobre todo justas, dando primacía a la tutela del ser humano.

REFERENCIAS

Andorno, L. O. (1995). El denominado proceso urgente (no cautelar) en el derecho argentino como instituto similar a la acción inhibitoria del Derecho italiano, JA 1995-II-887.

Caraballo, M. (2021). Inteligencia artificial, inequidad y discriminación en cajas negras. En

---

23 Así lo entienden también, por ejemplo, las Conclusiones de *lege ferenda* de las XIX Jornadas Nacionales de Derecho Civil celebradas en septiembre de 2024 en Pilar, Buenos Aires. *Cf*. https://www.austral.edu.ar/wp-content/uploads/2024/10/Conmision-3-1.pdf?x52835&x52835.

24 Como lo demuestran las XIX Jornadas Nacionales de Derecho Civil celebradas en septiembre de 2024 en Pilar, Buenos Aires, a las que se aludió.

Corvalán, Juan G. (dir.). *Tratado de inteligencia artificial*, La Ley, t. I.

Chamatropulos, D. (2017). Inteligencia artificial, prevención de daños y acceso al consumo sustentable, *La Ley*, 2017-E-1.

Chartzman Birenbaum, A. (2022). Inteligencia Artificial. El resguardo de datos personales. Los límites necesarios. Nuevos paradigmas, RDLSS 2022-23, 3, TR LALEY AR/DOC/3082/2022.

Comisión Europea. (2020). *Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica.* COM (2020) 64 Final.

Comité Económico y Social Europeo. (2017). *Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad*, 2017/C 288/01.

Corvalán, J. G. (2021). Preludio. ¿Qué hay de nuevo, viejo? Bienvenidos a la era de la inteligencia artificial. En Corvalán, J. G. (Dir.). *Tratado de inteligencia artificial*, La Ley, t. I.

Corvalán *et al.* (2021). Inteligencia artificial: Bases conceptuales para comprender la revolución de las revoluciones. En Corvalán, J. G. (Dir.). *Tratado de inteligencia artificial*, La Ley, t. I.

Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. (2018). *Inteligencia artificial para Europa.* COM (2018) 237.

Danesi, C. C. (2018a). Inteligencia artificial y responsabilidad civil: un enfoque en materia de vehículos autónomos. *Suplemento Especial LegalTech 2018*, 05/11/2018.

Danesi, C. C. (2018b). ¿Quién responde por los daños ocasionados por los robots?, *Revista de Responsabilidad Civil y Seguros*, 11.

Danesi, C. C. (2021). Sesgos algorítmicos de género con identidad iberoamericana: las técnicas de reconocimiento facial en la mira. TR LA LEY AR/DOC/1520/2021.

Fossaceca (h.), C. A. y Moreyra, P. (2020). Aproximaciones a la responsabilidad civil por la utilización de inteligencia artificial y derecho de los robots. Una mirada jurídica. RCyS2020-VIII, 20, Cita: TR LALEY AR/DOC/2254/2020.

Galdós, J. M. (2020). Comentario al art. 1711 del Código Civil y Comercial de la Nación. En Lorenzetti (Dir.), Ed. Rubinzal Culzoni, Tomo VIII.

García, Víctor Manuel (2019). Inteligencia artificial: su regulación y desafíos legales. (Primera parte). *Medium*, 18/2/19. https://medium.com/

Gurney, J. (2016). Imputing Driverhood: Applying a Reasonable Driver Standard to Accidents Caused by Autonomous Vehicles. Forthcoming, *Robot Ethics 2.0*.

Lorenzetti, R. L. (1995). La tutela civil inhibitoria. *La Ley*, 1995-C-1217.

Martínez Mercadal, J. J. (2022). El derecho privado ante la robótica y la inteligencia artificial: la prevención de la (hiper)vulnerabilidad. *La Ley Online*, TR LALEY AR/DOC/1494/2022.

Melo, V. E. (2021). Responsabilidad por daños e inteligencia artificial: ¿vino nuevo en odres viejos?, RCyS2021-III, 3, TR LALEY AR/DOC/1185/2021.

Mohadeb, S. *et al.* (2021). Inteligencia Artificial y Responsabilidad Civil. Aproximaciones a una regulación. En Danesi (Dir.). *Inteligencia Artificial, Tecnologías emergentes y Derecho*, Hammurabi.

Peyrano, J. (2015). Noticia sobre la acción preventiva. *La Ley*, 2015-F-1230.

Picasso, S. (2022). *Código Civil y Comercial de la Nación comentado*, Tomo VIII. Rubinzal-Culzoni.

Pizarro, R. D. (2013). *Responsabilidad del Estado y del funcionario público*. Tomo I. Ed. Astrea.

Pizarro, R. D. y Vallespinos, C. G. (2018). *Tratado de la Responsabilidad Civil*, Tomo I, Rubinzal Culzoni.

Repond, P. (11 de febrero de 2020). Inteligencia artificial y su marco normativo. https://abogados.com.ar/inteligencia-artificial-y-su-marco-normativo/25187

Rinessi, A. J. (2001). Lesión al crédito, Responsabilidad por daños en el tercer milenio (homenaje a Atilio Alterini). Cámara de Apelaciones en lo Civil y Comercial de Morón, Sala II, Muebles La Sorpresa de Isaac Goldfinger S.R.L. c. Sivori, Guillermo y otros, 11/09/2001.

Martínez, M. V. y Rodríguez, R. O. (2021). Deconstruyendo la inteligencia artificial. En Danesi (Dir.) *Inteligencia Artificial, Tecnologías emergentes y Derecho*, Hammurabi.

Sánchez Caparrós, M. (2021). Inteligencia artificial, sesgos y categorías sospechosas. Prevenir y mitigar la discriminación algorítmica. En Corvalán, J. G. (Dir.). *Tratado de inteligencia artificial*. Thomson Reuters La Ley, t. I.

Valente, L. (2019). La persona electrónica. *Anales*, Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional de La Plata, Nº 49. https://doi.org/10.24215/25916386e001

Zapata Sevilla, J. (2019). Inteligencia artificial y responsabilidad civil: El caso de las organizaciones descentralizadas autónomas. *Repositorio Institucional de la Universidad de Málaga*. https://hdl.handle.net/10630/18645

ISSN 3008-9484 | DOI 10.5281/zenodo.14508578 **Diálogos y Voces Judiciales** | Vol. 2, Nº 2 (diciembre de 2024): 20-33

RESPONSABILIDAD CIVIL EN EL USO DE LA INTELIGENCIA ARTIFICIAL

Civil Liability in the Use of Artificial Intelligence

Henoch Romero Boue[*]

Universidad Nacional del Comahue
henochromeroboue@gmail.com
https://orcid.org/0009-0003-4255-8985

RECIBIDO: 24/09/2024 - ACEPTADO: 21/11/2024

Resumen: La adopción de la inteligencia artificial genera nuevos retos en la responsabilidad civil debido a su autonomía, lo que complica su tratamiento legal. Este artículo propone un marco legal para abordar aspectos clave de la IA, destacando el factor de atribución objetivo como el más adecuado para evaluar la responsabilidad. Se exploran diversas cuestiones relacionadas con la responsabilidad civil, tanto en relaciones obligacionales como en el deber de no causar daño a terceros. Además, se subraya la necesidad de que los estados desarrollen un marco regulatorio más robusto que fomente la confianza en el uso de la IA, maximizando sus beneficios y reduciendo riesgos ante la seria dificultad de la autonomía inteligente.

Palabras clave: responsabilidad, supervisión, causalidad, previsibilidad, prevención

Abstract: The adoption of artificial intelligence presents new challenges in civil liability due to its autonomy, which complicates its legal treatment. This article proposes a legal framework to address key aspects of AI, highlighting the objective attribution factor as the most suitable for assessing responsibility. Various issues related to civil liability are explored, both in contractual relationships and the duty not to harm third parties. Additionally, the need for states to develop a more robust regulatory framework is emphasized, one that fosters trust in the use of AI, maximizing its benefits and reducing risks given the serious challenges of intelligent autonomy.

Keywords: responsibility, supervision, causality, predictability, prevention

El avance de la inteligencia artificial (IA) ha revolucionado sectores como la medicina, el transporte, las finanzas y el entretenimiento, impactando profundamente en la estructura de las relaciones jurídicas. Esta transformación plantea una serie de interrogantes esenciales sobre cómo la tecnología, en su contexto, tomando cada vez más decisiones y realizando tareas autónomamente, puede impactar significativamente en los principios tradicionales de la responsabilidad civil. Específicamente, en qué condiciones la IA debiera ser trabajada en materia de atribución, sea en virtud de un vínculo obligacional genérico o específico de un contracto, como fuera de aquellos, al del deber de no dañar a un tercero.

---

* Abogado, Universidad Nacional del Comahue. Especialista en Derecho Procesal Civil, Universidad de Buenos Aires. Especialista en Justicia Constitucional y Derechos Humanos (Universidad de Bolonia).

En dicho tamiz, el presente artículo explora la responsabilidad civil en su función resarcitoria derivada del uso de IA, enfocándose en los conceptos centrales como la antijuridicidad, el daño, la relación de causalidad y los factores de atribución. A su vez, aborda la función o principio de prevención del daño, que se ha vuelto indispensable en nuestros días, más aún en el contexto de los riesgos generados por el uso creciente de tecnologías avanzadas mediante su característica de autogestión. Este análisis se enmarca en la actual legislación de la Argentina y se complementa con ejemplos prácticos que ilustran los desafíos concretos de aplicar la normativa vigente en este campo tan novedoso.

I - LA ANTIJURIDICIDAD: EL ELEMENTO FUNDACIONAL DE LA RESPONSABILIDAD CIVIL EN EL CONTEXTO DE LA IA

Puede afirmarse que, en materia de responsabilidad civil, la antijuricidad es el elemento que amerita ser estudiado como punto de partida lógico de la didáctica. En efecto, es el que atiende el primer asunto del acontecimiento fáctico y esencial del campo. En particular, referida a la acción u omisión que contraviene a una norma preexistente, sea esta de origen legal o convencional, afectando un derecho o un interés jurídicamente protegido. Sumado a ello, comprende una conducta sin justificación legal para el derecho consagrado, es decir, reprochable en ese preliminar estudio contra una obligación de índole general o específica según el caso. Ya el mismo Alterini (2019, p. 68), entre otras ideas, la presentaba en términos de ilicitud o antinormatividad. En concreto, el concepto se verifica cuando la conducta lesiva vulnera un deber jurídico objetivo de conducta. Esto puede implicar tanto la violación de una obligación de resultado, en la que se espera que el deudor cumpla una prestación específica, como una obligación de medios, en la que se evalúa si se actuó con la diligencia y cuidado que el caso amerita.

Ahora bien, en el ámbito de la IA, esta categoría cobra relevancia debido al impacto de decisiones automatizadas en diversos entornos sociales y tecnológicos. Es que, en los escenarios de IA, la antijuridicidad puede surgir de múltiples modos que resultan en cierto punto inimaginables. Así, pues, se traduce en una actividad humana contraria a derecho, acometida por la implementación de sistemas de IA que vulneran derechos reconocidos. Puede surgir de tal forma la contradicción en distintos niveles, es decir, de menor o mayor raigambre; solo por mencionar la contradicción con el derecho a la igualdad, propiedad, seguridad, buena fe, etc. El modo puede configurar con inicios de conductas positivos o negativos, estos últimos tal vez más corrientes como debido a una falta de supervisión, mantenimiento o actualización de la IA, contraviniendo deberes de debida diligencia o cuidado razonable. En esencia, no debe escaparse para su comprensión la peculiaridad que caracteriza la IA, toda vez que radica en su carácter autónomo y en el hecho de que las decisio-

nes no siempre serán con acierto, o más bien calificarse de transparentes o seguras, puesto que sobre todo son aplicadas según un criterio o contexto que advierte esa misma inteligencia como tal. Esto sin dudas plantea una serie de desafíos a la hora de la identificación del agente responsable o, en el ámbito procesal, el/los legitimado/s pasivo/s.

Una nota de posible claridad en su alcance, ante este complejo escenario, puede encontrarse a partir de lo señalado por Mosset Iturraspe (2004, p. 89), quien indica que "la antijuridicidad se configura no solo por violar normas, sino también por ignorar estándares de previsión que eviten el daño". Asimismo, siguiendo esta línea, que se caracteriza por su amplio alcance en el plano de la antijuricidad, también se ha sostenido que "la prevención de los daños constituye una preocupación reciente en el escenario jurídico y se vincula en particular con ciertos derechos y bienes, tales como los derechos de la personalidad y los bienes de incidencia colectiva" (Seguí, 2009, p. 670).

Es notable identificar algunos casos prácticos inmiscuidos en la antijuricidad. Por ejemplo: una entidad financiera que, a través de la IA, rechaza de manera desproporcionada y sesgada, solicitudes de préstamos de personas con ciertas características (género, raza, edad, etc.); una clínica o profesional médico que utiliza IA para diagnósticos ágiles mediante datos inteligentes, pero que no verifica correctamente la información, causando un daño al paciente. Desde una óptica de la responsabilidad obligacional, se violarían la base de la buena fe, trato digno (de resultar un vínculo de consumo), igualdad, información, entre otros. Es que aquí el factor clave es el control del responsable, es decir, siguiendo las alusiones anteriores, quien tiene la posibilidad razonada de prever o verificar que la información proveída por la IA es efectivamente acertada.

La antijuridicidad en el contexto de la IA, entonces, resalta la necesidad de una clara comprensión sobre quién tiene la posibilidad de aplicarla o controlarla, esto es, en contraposición y su configuración, una conducta u omisión contraria a una estipulación genérica o específica en lo civil, comercial, bursátil, etc.; o bien fuera de ello violatoria del deber de no dañar a terceros. La IA es una herramienta o tecnología que debe ser percibida sobre los agentes atribuibles por su uso, implementación y especialmente de su no supervisión. Esencialmente, el principio de no dañar, inherente a la responsabilidad civil, debe ser un pilar en el desarrollo y uso de sistemas de IA, garantizando que los avances tecnológicos no comprometan los derechos fundamentales de las personas, sea de su patrimonio o dignidad como persona.

II - EL DAÑO COMO EJE DEL SISTEMA DE RESPONSABILIDAD CIVIL

El daño, sin duda, es la piedra angular sobre la cual se edifica todo el sistema de responsabilidad civil. El artículo 1737 del código Civil y Comercial de la Nación

(CCCN) define el daño como la lesión a un interés jurídicamente protegido, estableciendo que la existencia del daño es condición *sine qua non* para que surja la obligación de reparar. Esta conceptualización coloca al daño en el centro del debate sobre la aplicación de normas tradicionales a situaciones en las que la IA es responsable de causar perjuicio.

Es dable considerar que la IA, al operar de manera autónoma, puede generar tanto daños patrimoniales como extrapatrimoniales. Es así, siguiendo el caso práctico del sector bancario, los algoritmos de IA pueden decidir sobre la aprobación de préstamos de la índole que se prevea que así lo fuera. Si una IA comete errores de cálculo, esto puede generar daños patrimoniales significativos, no solo a la propia entidad financiera que adquiere los servicios de la IA, sino fundamentalmente a los propios clientes, máxime con carácter de consumidores ante la ley. Tal es así al no otorgar oportunidades financieras o la concesión de créditos a personas insolventes. Si puede pensarse que su uso es justamente inteligente, no obstante, no se escapan los errores y ajustes constantes sobre las nuevas e incesantes ocurrencias emergentes de la vida social. Del mismo modo, no se escapa a la IA en el mentado ámbito de la salud, donde un error de diagnóstico –entendido como proceso inicial y fundamental del arte de curar–, puede conllevar a notables repercusiones en el paciente. Es así que la IA, que actúa sin intervención directa humana, debe ser vista como un agente novedoso de gran utilidad, pero al mismo tiempo, con un gran potencial de fuente productora de daño, máxime en la coyuntura del desconocimiento acerca de sus posibilidades por su expansiva autonomía.

En ese marco, las tecnologías avanzadas pueden vulnerar derechos fundamentales, lo que genera la necesidad de una reparación efectiva, y, justamente, sobre lo último, nótese que este artículo no emplea el calificativo de plena, puesto que, en línea con destacados desarrollos y exposiciones doctrinarias, dicha reparación es un ideal materialmente inalcanzable, aunque de legítima aspiración (López Mesa, 2018). No obstante, es dable señalar que el objetivo resarcible debe comprender todo lo que se corresponda al caso, siempre ello en su justa medida, esencialmente que abarque la esfera patrimonial y extrapatrimonial de la víctima, más aún a su consideración de tratarse de una persona humana y su dignidad, aspecto elemental del paradigma del sistema de reparación. En tal sentido, es dable mencionar al daño moral, por cierto, muy justipreciado en el ámbito judicial, donde incluso muchas veces es prácticamente presumido, también cobra relevancia para el asunto bajo examen, puesto que, en situaciones en las que una IA infringe derechos personalísimos, como el derecho a la intimidad o a la imagen, el afectado puede y debería reclamar tal rubro. Por ejemplo, en el uso de sistemas de reconocimiento facial que fallan en identificar a una persona correctamente y la vinculan con actividades ilícitas, el daño moral y hasta psicológico, según se pruebe especialmente el último, es sumamente factible.

De manera similar, es importante destacar que cada vez más la IA, especialmente en las redes sociales (Facebook, Instagram, X, Telegram, entre otros), ofrece contenidos altamente atractivos para el usuario, al analizar y utilizar sus datos de manera precisa. Este fenómeno plantea una reflexión sobre los riesgos que implica la generación de eventos dañosos para las personas, especialmente las que volcaron información allí y es contextualizada por esa inteligencia. Efectivamente, su intervención al actuar de forma tan intrusiva, puede tener un impacto profundo en el comportamiento humano, ya que, mediante técnicas de personalización, puede influir en decisiones y pensamientos de manera constante. Así, se crea una dependencia cada vez mayor, ya que la IA profundiza en los intereses del usuario, alimentando su atracción hacia ciertos contenidos y generando patrones de consumo y comportamiento que afectan su autonomía personal.

Por tal motivo, es crucial la atención del Estado en este tipo de asuntos, fundamentalmente en la necesidad de prevenir escenarios dañosos. La adaptación ante este nuevo paradigma tecnológico implica reconocer la necesidad de estándares de previsión más elevados y una mayor diligencia por parte de los desarrolladores y usuarios de la IA.

III - RELACIÓN DE CAUSALIDAD: INMEDIACIÓN Y PREVISIBILIDAD

Otro presupuesto esencial de la responsabilidad civil lo comprende la relación de causalidad, y, en el caso de la IA, plantea uno de los mayores desafíos para cada caso. El artículo 1726 del CCCN establece la causalidad adecuada como nexo con el hecho productor del daño, lo que en la práctica se traduce en la necesaria probanza de que el daño sea consecuencia directa de la conducta antijurídica. No obstante, la autonomía de la IA introduce una complejidad adicional, ya que sus decisiones pueden involucrar a una cadena de actos intermedios que obligan a su estudio preciso para la correcta determinación del vínculo causal y, por ende, responsabilidad.

De tal modo, resulta fundamental distinguir entre causalidad inmediata y mediata, especialmente en el análisis de la responsabilidad civil cuando está involucrada la IA. Determinar si un daño vinculado a la IA era previsible depende tanto del escenario fáctico como del marco jurídico que lo rodee. En algunos casos, la relación de causalidad es relativamente sencilla de establecer, mientras que, en otros, las complejidades técnicas y jurídicas dificultan la determinación del nexo causal. Así, en el ámbito no obligacional, es dable señalar que la causalidad suele ser quizás más directa y menos controvertida. Esto responde al principio general del riesgo creado que representa el uso de la IA, especialmente en situaciones donde el daño proviene de cosas peligrosas o actividades riesgosas. Por ejemplo, si un peatón es atropellado por un vehículo autónomo, no será necesario analizar en profundidad qué causó el fallo técnico o si la IA operó conforme a sus parámetros.

Siguiendo la teoría del riesgo, el sistema judicial prioriza la reparación del daño, atribuyendo, según la legislación civil codificada y específica, la responsabilidad objetiva al propietario o guardián del vehículo, así como a la aseguradora citada en garantía. En este contexto, el marco jurídico permite una imputación simplificada basada en el deber de no dañar y la previsión razonable de las consecuencias inherentes al uso de la tecnología. En contraste, en el ámbito obligacional, la relación de causalidad se vuelve más compleja, ya que requiere analizar si el daño deriva directamente de la prestación comprometida o de una falla en los deberes accesorios. Esto cobra particular relevancia en contratos donde la IA constituye un elemento esencial de la prestación, como en sistemas médicos o financieros.

En esencia, la causalidad debe evaluarse considerando, por una parte, a la naturaleza del vínculo obligacional, es decir, si se trata de medios (debida diligencia exigible al deudor) o de resultados (obligación de alcanzar un fin u objetivo determinado). Por otro lado, debe considerarse el rol de los actores de la cadena comercial, estos son fabricantes, diseñadores, programadores, proveedores y vendedores que pueden ser responsables. De tratarse el caso de una relación de consumo, todos serán solidariamente responsables frente al consumidor dado el régimen de tutela al mismo y el carácter de orden público normativo. Sin embargo, de no resultar el caso a tal ámbito, dependerá de qué labor o aspecto de incidencia causal tiene cada uno con el daño causado. La prueba en el proceso deberá de ser justipreciada por la técnica pericial especializada en IA.

De igual manera, los responsables no solo deben prever las consecuencias directas de su actuación, sino también las mediatas, siempre que estas últimas sean razonablemente previsibles conforme al conocimiento técnico y al estándar de diligencia aplicable. La previsión adecuada y las medidas adoptadas para mitigar riesgos no solamente delimitan la responsabilidad, sino que también configuran un estándar de actuación para quienes desarrollan o implementan tecnologías de IA.

En el campo de las obligaciones contractuales, será fundamental que los sujetos del contrato sean lo más claros y precisos respecto a todos los puntos que atañen con las funciones y alcances de la IA. De tal forma, la autonomía de voluntad para el ámbito privado de los contratos guarda consigo el desafío de establecer derechos y obligaciones lógicas para la correcta eficacia contractual.

En particular en algunos sectores, la regulación de la función de la IA es un aspecto crucial. Efectivamente, se puede advertir en los servicios financieros o de salud. La automatización de los procesos que haga la IA y su impacto material deben ser previsibles, contemplando en mayor medida todos sus alcances esperados. De tal modo, piénsese en una actualización en su software que, necesaria, debe pensar en todos sus posibles eventos, sea estos de beneficios como de pérdidas. Dicha previsibilidad del daño, debería analizarse desde la plena objetividad científica y huma-

namente posible, es decir, en ese caso, si esa falla del software era un riesgo conocido y previsible para esas partes involucradas, siempre bajo el tamiz de la buena fe.

En esa dinámica, es oportuno traer el mentado apagón a nivel mundial que sufrió la empresa Microsoft a mediados de julio del 2024, donde afectó a millones de usuarios y empresas globalmente. Esta disrupción causó la interrupción de servicios clave, afectando tanto la continuidad operativa como la seguridad de los sistemas. CrowdStrike, una empresa de ciberseguridad, identificó problemas en la integración de la infraestructura de Microsoft como un factor contribuyente. En este caso, si bien la falla técnica fue inmediata, la previsibilidad de que una disrupción tecnológica masiva pudiera causar daños era un riesgo conocido.

Esta situación evidencia que los proveedores de servicios críticos, al no prever o mitigar adecuadamente tales fallos, pueden enfrentarse a una causalidad inimaginable. En suma, un ejemplo más cercano al ámbito de la justicia argentina, podría involucrar un sistema de salud público que contrata a una empresa para digitalizar la gestión de historias clínicas mediante un software especializado. Si este sistema sufre un colapso debido a una mala actualización, y esto provoca que varios pacientes no reciban el tratamiento adecuado o en el tiempo necesario, se podrían reclamar los daños resultantes. Aquí, la previsibilidad del daño es clave: si la empresa sabía o debió haber sabido que su software no estaba lo suficientemente probado para su actualización, la responsabilidad por los daños causados sería mayor.

En definitiva, quizás puedan otorgar mayor nitidez, en cierta medida, las regulaciones que razonablemente fijen o delimiten la extensión de responsabilidad, en base a los intereses jurídicos y la naturaleza de la relación, especialmente, para su interpretación válida y eficaz. En tal sentido, cabe agregar lo que señala Lorenzetti (2001) para el ámbito contractual, esto es, que "la regla de la previsibilidad determinada por los contratantes al momento de celebrar el negocio es primordial, pues, en caso contrario —esto es, si el magistrado fijara los alcances del deber de resarcir— las partes reaccionarán fijando precios más altos en cobertura de sus seguridades".

Ciertamente, se anticipan escenarios de causalidad sumamente complejos, pudiendo acontecer hasta causalidades múltiples mediante co-causación o con-causación. En el caso de la primera, será crucial identificar todas las partes involucradas y la medida en que cada una contribuyó al daño. Por ejemplo, en el caso de un accidente de tráfico involucrando un vehículo autónomo, la co-causación podría implicar tanto un fallo del sistema de IA como una acción imprudente de otro conductor. La responsabilidad podría distribuirse entre el fabricante del vehículo, el desarrollador del software y el conductor humano involucrado. En cambio, en la segunda, que refiere a varios eventos o causas independientes que contribuyen simultáneamente al daño, es decir, crean un resultado que puede ser más complejo de desentrañar, es clave cuando se utilizan distintos sistemas o algoritmos de IA, ya

que la interacción de múltiples factores, puede hacer difícil identificar y atribuir responsabilidad de manera clara.

Por consiguiente, la causalidad es un elemento sumamente interesante en la responsabilidad por la intervención de la IA, siendo el factor de la previsibilidad no una cuestión menor. Por el contrario, resulta desafiante tanto para las partes involucradas como para los tribunales que deben atender un caso con tecnología avanzada. A veces será más nítida la determinación causal con el daño y en otras no tanto. Sin embargo, en cualquier caso, el análisis técnico jurídico e informático sobre la incidencia causal de la IA en el daño, ante la premisa obligacional –general o particular– o del deber de no dañar, es la clave para la correcta resolución que positivamente se haga.

El enfoque y aplicación de un positivismo jurídico bien definido y robusto, es sin duda la respuesta para abordar esta serie de complejidades, garantizando una reparación justa y eficaz para los daños causados por la interacción de múltiples factores, tanto humanos como tecnológicos.

IV – FACTORES DE ATRIBUCIÓN EN EL ÁMBITO DE LA IA: OBJETIVIDAD Y SUBJETIVIDAD

La conceptualización de la responsabilidad civil clásicamente se distingue en factores de atribución objetivos o subjetivos. En el contexto de la IA, este punto es clave para determinar cuándo es un caso u otro y cómo se deben reparar los daños.

El artículo 1723 del CCCN establece que la responsabilidad puede ser objetiva según las circunstancias de la obligación o lo convenido por las partes, surge que el deudor debe obtener un resultado determinado. En consecuencia, si consideramos que los sistemas de IA, apartando alguna filosofía posthumanista o transhumanista, son simplemente cosas de posible causación de daño, debe ser recogido con la fuente civil directa, que siendo aludida en otros desarrollos, corresponde citarla, esta es, la del artículo 1757 de la "responsabilidad derivada de la intervención de las cosas y actividades riesgosas", es decir, sus operadores o desarrolladores podrán ser responsables bajo un criterio objetivo, sin necesidad de probar culpa.

Por otro lado, podrá apreciarse que el factor de atribución en casos de IA también puede ser subjetivo, lo que, siguiendo el artículo 1724 del CCCN, requiere demostrar que el daño se produjo por dolo o culpa (negligencia, imprudencia o impericia) por uso u omisión sobre aquella. En este sentido, pensemos el caso probable de negligencia en la falta de supervisión humana o el diseño defectuoso de los algoritmos. Es que la diligencia debida en la atención, por parte de los controles humanos, sigue siendo indispensable para evitar errores en sectores críticos, como se señaló especialmente en el sector de la salud, también no se escapa en el transporte por cualquier medio.

Lo distinguido aquí para una dirección u otra, es cotejar primero la categoría de obligación de que se trata, es decir, si es de fuente obligacional-contractual. En el caso de que efectivamente y con condiciones asequibles se previó un determinado resultado a favor de una parte, resultaría objetiva sin dudas; caso contrario, si se estipula un uso con condiciones de probabilidades a cargo del deudor, según la capacidad en el uso que ofrezca el deudor a partir de la IA, sería de medios, es decir subjetiva esa responsabilidad.

La interpretación en el ámbito contractual exige observar cuidadosamente aquello que las partes pudieron prever de manera razonable, la actuación en buena fe y sin incurrir en abusos, especialmente en relación con el uso y naturaleza de la IA. Asimismo, la verificación objetiva de si positivamente el interés del acreedor se equipara con una obligación con características que otorguen clara expectativa de resultado posible. Pareciera creerse que la IA promete cada vez más mejores resultados, lo que conlleva a proyectar a una responsabilidad objetiva por esa misma inteligencia. No obstante, dependerá ciertamente de analizar las reglas codificadas por nuestra legislación para interpretar cada aspecto del contrato en cuestión, sus sujetos contratantes, sin soslayar, en ninguna ocasión, las capacidades y realidades objetivas que ofrece la IA.

Por ende, llegado el caso al seno de la administración de justicia, será un factor importante que la judicatura, siempre que procesalmente se pudiera, se provea de auxiliares especializados en la materia donde echen mayor luz sobre los puntos debatidos y vinculados con la IA.

V - LA PREVENCIÓN DEL DAÑO EN EL USO DE LA IA EN LA JUSTICIA

El artículo 1710 del CCCN establece el deber de prevenir el daño como un principio rector en las relaciones jurídicas. Este principio tiene un fuerte impacto en el contexto de la IA, dado el potencial de los sistemas autónomos para generar riesgos y daños sin la intervención directa del ser humano. En la justicia ordinaria argentina, la acción preventiva cobra una relevancia significativa en casos donde se busca evitar la materialización de un daño inminente derivado del uso inadecuado o defectuoso de tecnologías que incorporan IA. Ese principio o deber de no dañar a otro —*alterum non laedere*—, es un concepto que se expande ampliamente en el uso de la IA, ya que estas tecnologías no solo pueden causar daños físicos, sino también afectar derechos fundamentales, como la privacidad, la integridad personal o el acceso a bienes y servicios. La acción preventiva, en este sentido, no tiene como objetivo la reparación de un daño ya causado, sino, claro está, evitar la causación del evento dañoso o su intensificación.

La teoría preventiva del daño ha sido ampliamente desarrollada en el derecho ar-

gentino antes de su cristalización en el CCCN. No solo se proyecta en obligar a prevenir daños individuales, sino que también impone una mirada del deber social como precautelar, siendo de tal forma sumamente vinculados a ello los propios riesgos de daño inherentes de las actividades de la tecnología. En ese ámbito, es determinante verificar, para la viabilidad de la tutela, la concurrencia de una contradicción entre el accionar y el ordenamiento jurídico, debiendo en tal caso resultar de un modo objetivo. Adicionalmente, debe ser previsible la producción o el agravamiento del daño, con lo cual, no resulta que se presente un daño cierto en la esfera jurídica de la víctima o accionante, sino que basta la amenaza para su procedencia.

Dicho enfoque preventivo, aplicado en aquellos casos, debe ser muy claro: la protección efectiva de los derechos implica anticiparse a los posibles riesgos mediante el uso de herramientas tecnológicas seguras y una adecuada supervisión judicial. Desde luego, los estados deben anticiparse a que, cuando una nueva tecnología se incorpore a su ámbito, sea testeada previamente a su proposición y desde ya regulada.

La globalización y la transgresión de las fronteras mediante estas tecnologías, como con el arribo en su oportunidad de internet, conlleva a concluir que la IA tendría incluso mayor impacto para la vida social, debiendo ser atendida con suma urgencia por parte de las autoridades públicas en todos sus poderes, legislativo, ejecutivo y judicial. Es que, como puede advertirse, es creciente la demanda de *chips* de IA fabricados por empresas semiconductoras, solo por mencionar algunas, NVIDIA Corp., Broadcom Inc., AMD Inc., Micron Technology Inc., cuyo margen de aplicación social es incalculable.

La tesitura actual de la tecnología, una vez más, pone sobre los estados la tarea desafiante y necesaria de brindar la mayor certeza o seguridad posible respecto de los interrogantes de la IA. Esto es, el objetivo de efectivizar o garantizar los derechos, otorgar seguridad social y jurídica que evite con mayor margen de probabilidad la causación del daño debido a la aparición de la IA. Así, es dable en la justicia que un individuo, grupo o clase, según el caso, pueda plantear una acción preventiva en casos de potenciales daños derivados por el uso de IA. Si bien se infiere que cualquier desarrollador proyecta su tecnología con la visión de mejorar con eficiencia la vida humana, ello no resulta aval suficiente para que no acontezcan nuevos problemas derivados sobre la última.

Así, recogiendo algunos ejemplos, los errores en diagnósticos médicos automatizados, donde la implementación de IA para diagnosticar enfermedades o sugerir tratamientos puede generar riesgos graves si no se supervisa adecuadamente. En efecto, un paciente que detecte inconsistencias o errores en la plataforma médica podría solicitar, mediante una acción preventiva, que se revise la implementación de la IA y que se garantice la intervención humana antes de tomar decisiones críticas sobre la salud o también en el caso de invasión a la privacidad u otros daños me-

diante el uso de drones o cámaras que operan con IA por parte de empresas de vigilancia. En estos casos, las partes afectadas podrían solicitar medidas preventivas que regulen o limiten el uso de estas tecnologías hasta que se garanticen medidas de seguridad adecuadas; entre muchos otros derivados y emergentes.

Bajo esa tesitura, en una acción preventiva en la justicia ordinaria, la parte demandante deberá acreditar que existe un riesgo inminente o una amenaza concreta de daño relacionado con el uso de IA. Por tal motivo, ese elemento de antijuricidad cobra un papel preponderante para el accionante afectado que debe exhibirla al proceso, con toda la carga probatoria, debiendo aportar elementos técnicos y pruebas que demuestren la posible afectación. Esto puede incluir informes periciales, estudios de riesgos tecnológicos, y evidencia documental sobre el funcionamiento defectuoso de los sistemas automatizados. Por su parte, quien es accionado, sea una persona humana o jurídica (empresa tecnológica o cualquier entidad) que utilice IA, tendrá la obligación de defender la legitimidad de su tecnología y, en su caso, demostrar que se han implementado las medidas preventivas necesarias para evitar cualquier daño. La carga será mayor a los últimos de encontrarse procesalmente en mejores condiciones para su acreditación, desde luego este último aspecto a decisión prudencial de la judicatura.

Ahora bien, no es menor mencionar el desafío que tiene o debiera tener el contenido y disposición de una sentencia en estos casos donde emerge un agente con gran potencial productor de daño. Especialmente, al resultar incalculable las intervenciones o usos de la IA, por ejemplo, en el marco de contratos. Si algo es positivo lo es, justamente, el derecho positivo, al prever la tutela preventiva, caracterizada por un mecanismo amplio. En este sentido, relacionado con el acto de sentencia, Pizarro y Vallespinos (2019, p. 455) señalan: "Tiene naturaleza de sentencia atípica, exhortativa u ordenatoria. A través de ella el juez realiza una actividad más creativa, que habitualmente requiere controles de implementación de lo resuelto".

En consecuencia, se colige el abanico de múltiples soluciones a fin de conducir al propósito del orden jurídico, adoptando decisiones simples o complejas. Así, solo por mencionar, se proponen las siguientes:

- *Suspensión temporal del uso de la* IA: El juez puede ordenar la suspensión del sistema de IA en cuestión hasta que se realicen las modificaciones o pruebas necesarias para garantizar su seguridad. Esto puede ser especialmente relevante en casos de vehículos semiautónomos, donde se identifiquen fallos en los sistemas de asistencia de conducción.
- *Implementación de medidas de seguridad adicionales*: En casos donde se identifiquen riesgos técnicos en la IA, el juez puede ordenar que se adopten protocolos de seguridad más estrictos, como sistemas redundantes, controles hu-

manos adicionales, o la instalación de mecanismos de monitoreo continuo, por ejemplo, en drones de vigilancia autónomos. Todas las anteriores con miras no solo a la demandada, sino también al mismo sector público para que atienda el conflicto llegado al proceso judicial.

VI - CONCLUSIÓN

La responsabilidad civil en el uso de la IA plantea interrogantes profundos sobre la adecuación de las normas tradicionales a las nuevas realidades tecnológicas. Si bien los principios generales del CCCN proporcionan un marco sólido para abordar los casos en que la IA cause daños, las características autónomas de estos sistemas exigen una evolución en los enfoques normativos y judiciales.

Es indispensable que se continúe avanzando en la creación de marcos regulatorios específicos que otorguen mayor claridad en cuanto a los criterios de causalidad, atribución y prevención del daño en el contexto de la IA. Además, la previsión y el diseño de estrategias preventivas son esenciales para minimizar los riesgos inherentes al uso de tecnologías autónomas, particularmente en sectores críticos como la salud, el transporte y los servicios financieros.

A medida que las herramientas de IA se integren más profundamente en la vida cotidiana y en la toma de decisiones, causan el desafío de si se encontrará un equilibrio entre el fomento de esta innovación tecnológica y la protección efectiva de los derechos de las personas. Este enfoque no solo garantizará la reparación adecuada de los daños, sino que además contribuirá a generar mayor confianza en las tecnologías emergentes.

De la misma manera, el uso de IA en múltiples ámbitos de la vida cotidiana plantea desafíos lógicos para el derecho civil argentino, especialmente en lo que respecta a la anticipación o más bien función preventiva de la responsabilidad en materia de daño. Sin duda la acción preventiva ofrece una herramienta vital para los ciudadanos que buscan protegerse de los riesgos que estos sistemas autónomos puedan generar, antes de que el daño ocurra. Al adaptarse a la tecnología, la justicia deberá seguir garantizando que se implementen controles adecuados para evitar daños irreversibles.

La creciente implementación de IA en Argentina, tanto en la empresa privada como en el sector público, exige una respuesta efectiva por parte del sistema judicial, que debe asegurar la correcta aplicación del principio preventivo para proteger derechos fundamentales. Al incorporar medidas preventivas adecuadas y exigir pruebas contundentes, los jueces pueden jugar un papel proactivo en la prevención de daños tecnológicos.

La prevención del daño en el contexto de la IA es fundamental para garantizar

una implementación segura y responsable de esta tecnología. En Argentina, aunque aún estamos en una etapa temprana de su desarrollo, los tribunales deben aplicar ese principio preventivo de manera efectiva en busca de mitigar los riesgos que la IA pueda generar con suma probabilidad en el futuro, imponiendo de acuerdo al sistema amplio de legitimación pasiva, su manda a quien en cuanto de ella dependa la evitación dañosa.

El rol del derecho preventivo es claro: actuar antes de que los daños se materialicen, a través de sentencias que no solo reparen, sino que también exijan medidas correctivas y anticipatorias que aseguren la seguridad futura. El desarrollo tecnológico debe ir acompañado de mecanismos legales robustos que permitan su crecimiento sin comprometer los derechos fundamentales de las personas.

Sin duda alguna, una de las mayores dificultades al abordar la responsabilidad civil en el contexto de la IA es el hecho de comprender y evaluar su autonomía en el funcionamiento. Es así que, a diferencia de las tecnologías tradicionales, los sistemas de IA operan con un grado de independencia que les permite tomar decisiones sin intervención humana directa. Esta autonomía plantea muchos interrogantes sobre la previsibilidad de sus acciones y sobre la asignación de responsabilidad cuando las decisiones resultantes causan daño.

Será esencial reconocer que, en ciertos casos, la IA actúa basándose en algoritmos que pueden tomar decisiones fuera del control explícito del programador o del usuario, lo que complica la identificación y en qué medida el agente será responsable. Este fenómeno exige un enfoque jurídico razonado, que no solo contemple la acción directa de los humanos involucrados en la creación y uso de la IA, sino que también abarque los riesgos inherentes a los sistemas autónomos, cuyo comportamiento, aunque diseñado bajo ciertos parámetros, puede evolucionar de maneras impredecibles.

REFERENCIAS

Alterini, A. A. (2018). *Responsabilidad civil.* Abeledo Perrot.

Código Civil y Comercial de la Nación Argentina. Ley 26.994. Disponible en: https://www.argentina.gob.ar/normativa/nacional/ley-26994-235975

López Mesa, M. J. (2018). El mito de la reparación plena. *El Dial: Suplemento de Derecho Económico*, 1-1.

Lorenzetti, R. L. (2001). Resarcimiento del daño contractual: confianza, información, previsibilidad. *Jurisprudencia Argentina*, pp. 1207-1215.

Mosset Iturraspe, J. (2004). *Responsabilidad por daños*. Rubinzal-Culzoni.

Ossola, Federico A. (2016). *Responsabilidad civil*. Abeledo Perrot.

Pizarro, R. D. y Vallespinos, C. G. (2014). *Manual de responsabilidad civil* (Tomo 1), Ru-

binzal-Culzoni Editores.

Rivera, J. C. (2019). *Instituciones de Derecho Civil*. Abeledo Perrot.

Seguí, A. (2009). *Prevención de los daños y tutela inhibitoria en el derecho del consumo*. En Picasso, S. y Vázquez Ferreyra, R. A. (Dirs.). *Ley de Defensa del Consumidor: Comentada y Anotada* (Tomo II), La Ley.

ISSN 3008-9484 | DOI 10.5281/zenodo.14508965 **Diálogos y Voces Judiciales** | Vol. 2, Nº 2 (diciembre de 2024): 34-49

LAS DAO Y EL DERECHO: DESCENTRALIZACIÓN EN EL NUEVO ORDEN JURÍDICO

DAOs and the Law: Decentralization in the New Legal Order

R. Sebastián Cabana[*] *y M. Cecilia Hansen*[**]

Universidad Nacional del Córdoba
rscabana2000@hotmail.com / ceciliahansenunc@gmail.com

RECIBIDO: 10/10/2024 - ACEPTADO: 11/11/2024

Resumen: La inteligencia artificial y tecnologías emergentes como *blockchain* han irrumpido en áreas clave del derecho. En este contexto, las Organizaciones Autónomas Descentralizadas (DAO) se posicionan como protagonistas de un modelo organizacional sin precedentes. Basadas en contratos inteligentes y gobernadas colectivamente, las DAO prescinden de una autoridad central, lo que abre interrogantes fundamentales sobre su interacción con el derecho vigente. Este trabajo aborda las complejidades jurídicas que plantean las DAO, analizando cómo encajan en marcos normativos tradicionales y si es necesaria una legislación específica para regular su existencia y funcionamiento.

Palabras clave: DAO, contratos inteligentes, cadena de bloques, token, inteligencia artificial

Abstract: Artificial intelligence and emerging technologies like blockchain have disrupted key areas of law. In this context, Decentralized Autonomous Organizations position themselves as protagonists of an unprecedented organizational model. Based on smart contracts and collectively governed, DAOs dispense with a central authority, raising fundamental questions about their interaction with existing law. This paper addresses the legal complexities posed by DAOs, analyzing how they fit into traditional regulatory frameworks and whether specific legislation is needed to regulate their existence and operation.

Keywords: DAOs, smart contracts, blockchain, token, artificial intelligence

La inteligencia artificial (IA) ha dejado de ser una mera herramienta tecnológica para convertirse en un fenómeno transformador que cuestiona estructuras y paradigmas en diversos ámbitos del conocimiento. Noel Yuval Harari (2024), por ejemplo, advierte sobre la capacidad autónoma de la IA al describirla no solo como un instrumento, sino como un agente independiente capaz de tomar decisiones, lo que pone en crisis la centralidad humana en el proceso de creación y control: "cualquier tecnología previa tenía un poder ingente, pero ese poder estaba en manos de los seres humanos. La bomba atómica no podía decidir nada ni inventar un arma nueva; la

* Abogado (Universidad Nacional de Córdoba), Juez de Primera Instancia en lo Civil y Comercial, Poder Judicial de Jujuy.

** Abogada (Universidad Nacional de Córdoba), especialista en Derecho Procesal (Universidad Católica de Santiago del Estero). Secretaria de Primera Instancia en lo Civil y Comercial, Poder Judicial de Jujuy.

IA es distinta: puede tomar decisiones por sí misma". En igual tesitura se ha pronunciado Geoffrey Hinton, destacado pionero en la materia, galardonado con el Premio Nobel de Física este año: "no tenemos experiencia sobre lo que es tener cosas más inteligentes que nosotros"[1] . Hinton enfatiza la necesidad de actuar con cautela ante un futuro incierto donde coexistir con entidades más inteligentes que los humanos plantea desafíos inéditos.

El ámbito legal no escapa a esta transformación. La IA y tecnologías emergentes como *blockchain* han irrumpido en áreas clave del derecho, desde la protección de datos hasta el derecho contractual y societario. En este contexto, las Organizaciones Autónomas Descentralizadas (DAO, por sus siglas en inglés) se posicionan como protagonistas de un modelo organizacional sin precedentes. Basadas en contratos inteligentes y gobernadas colectivamente, las DAO prescinden de una autoridad central, lo que abre interrogantes fundamentales sobre su interacción con el derecho vigente.

Este trabajo aborda las complejidades jurídicas que plantean las DAO, analizando cómo encajan en marcos normativos tradicionales y si es necesaria una legislación específica para regular su existencia y funcionamiento. En la primea sección se describe brevemente el contexto actual, señalando los principales hitos en el camino hacia la descentralización. En la segunda, se desarrollan las notas esenciales de dos tecnologías emergentes –*blockchain* y *smart contracts*–, que convergen en las DAO. La tercera sección explica qué son las DAO y, en la cuarta, se propone una clasificación de estas organizaciones, además de analizar sus implicancias legales a través de tres casos. Por último, se ofrece una perspectiva legal para repensar las estructuras jurídicas locales en relación con estas transformaciones. En las conclusiones sugerimos que no conviene encasillar a las DAO en un modelo rígido. A la luz de las reflexiones de la Comisión Europea en 2020, que anticipaban posibles vacíos legales frente a estas innovaciones, resulta útil pensar cómo el derecho puede adaptarse a esta nueva era de descentralización y tecnología, entendiendo que las DAO no pueden pensarse divorciadas del mundo jurídico.

I - CONTEXTO: HITOS EN EL CAMINO DE LA DESCENTRALIZACIÓN

No hay duda de que nos encontramos transitando un mundo distinto al que conocíamos, donde coexisten seis generaciones que han pasado por adaptaciones tecnológicas disímiles; desde la generación "silenciosa" preexistente a la Segunda Guerra Mundial, cuyo contacto con la tecnología se reducía a escuchar el programa de radio a una misma hora y discar periódicamente un teléfono, a la generación "T" o

---

1 BBC Mundo, 8 de octubre de 2024. *Cf*. https://www.bbc.com/mundo/articles/c07njpdypn50

"Alpha" que no concibe prescindir de la hiperconectividad y la utilización de aplicaciones a cada instante, siendo parte del escenario el metaverso y el empleo de placas de video GPU para una mejor experiencia inmersiva *gamer*. En este contexto, la materia prima son los datos y no un recurso natural en particular, motivo por el cual el esquema de acción de las empresas se basa en una gobernanza de datos de sus usuarios reduciendo las pérdidas y logrando un acercamiento más preciso a sus necesidades.

Bajo esta línea y haciendo un poco de retrospección en el tiempo, cabe mencionar que desde la primera conexión de veintitrés computadoras a internet por el Departamento de Defensa de los Estados Unidos (ARPANET), el cual envió el primer correo electrónico allá por 1971, hemos visto evolucionar a la web desde algo parecido a las páginas amarillas y el consiguiente surgimiento de las "puntocom" y su posterior extinción con la burbuja del 2001 y la crisis de las mismas, para luego ver emerger la web 2.0 y la utilización de internet para relacionarnos, escribir y ver videos (Facebook, YouTube, Twitter, etcétera).

Más aquí en el tiempo, otro hito histórico se produjo en el 2007 con la denominada crisis de las *subprime* en EE.UU., más comúnmente denominada como la crisis de las hipotecas, que tuvo su inicio en el endeudamiento de un sinnúmero de particulares a consecuencia de las "hipotecas basura", lo que llevó a generar una gran recesión a escala global, poniendo en jaque a las principales economías desarrolladas.

Como contrapartida, una persona o grupo de personas –lo que hasta la fecha se desconoce– bajo el seudónimo de Satoshi Nakamoto, en reacción al sistema financiero y bancario tradicional, que en no pocas ocasiones hizo posible su sostenimiento en base a prácticas que importaban que muchos de sus más transcendentales protagonistas nunca quebrasen siendo rescatados incluso por los propios estados (por ejemplo, Merrill Lynch, Freddie Mac y Fannie Mae o ING, entre muchos otros), publicó el famoso *Whitepaper* en Halloween de 2008. La propuesta consistía en contar con un dinero que no requiera de bancos, pero que a su vez no pueda ser vulnerado: viendo la luz el Protocolo Bitcoin.

Ese documento implicó un salto cualitativo en la evolución de internet, surgiendo la famosa Web 3. A su vez, esto generó el surgimiento de un nuevo paradigma, el de la "democracia de los datos"; dado que los mismos no se albergan en data centers únicos de propiedad de grandes empresas, siendo posibles víctimas de algún *ramsomware*; sino en las redes descentralizadas de registros distribuidos (DLTs), donde los datos están atomizados entre un sinfín de computadoras conectadas a la red. Dichas redes pueden ser: públicas (Bitcoin, Ethereum), privadas o híbridas, conforme su acceso y objeto final.

Para ser más precisos, cabe destacar que esta nueva tecnología se caracteriza porque el dato (que es algo preciado, por ser un valor dinerario o un dato sensible)

pasa a estar albergado en una representación digital inviolable, trazable, auditable, denominada *token*, que se reduce a una seguidilla de números y letras. Estas transacciones entre los usuarios quedan registradas en la red (de acceso público, privado o híbridas), en la cual se puede constatar su carácter de única y de quién proviene, ello a consecuencia de que posee una identificación personal e inalterable.

Con posterioridad a *bitcoin* surgen los *smart contracts* o contratos inteligentes, los cuales se tratan de programas informáticos que se ejecutan automáticamente cuando se cumplen ciertas condiciones predefinidas. Fueron propuestos por primera vez por Nick Szabo en la década de 1990, pero su implementación práctica se popularizó a partir de 2015 con la creación de Ethereum por Vitálik Buterin.

Un contrato inteligente se compone de un código que define reglas y consecuencias estrictas de un acuerdo similar a un contrato tradicional, pero que se ejecuta en la *blockchain* (literalmente, "cadena de bloque").

Además, los contratos inteligentes están habilitando nuevas formas de interacción y modelos de negocio en diversos sectores. En finanzas se encuentran revolucionando la forma en que se realizan préstamos, seguros y pagos. En la cadena de suministro están mejorando la trazabilidad y la eficiencia. Incluso en la gobernanza permiten la creación de organizaciones autónomas descentralizadas (DAO), donde las decisiones se toman a través de contratos inteligentes ejecutados por la comunidad, todos temas que pasamos a tratar en particular.

II – PRELIMINAR: *BLOCKCHAIN* Y *SMART CONTRACTS*

Para un correcto entendimiento de las tecnologías bajo estudio resulta necesario circunscribir en sus notas más características a dos tecnologías emergentes que convergen para así poder dar origen a una DAO, ellas son las *blockchain* o cadenas de bloque y los *smart contracts* o contratos inteligentes mencionados en el parágrafo anterior.

El nombre de "cadena de bloques" representa la manera en la que se almacena la información. Así como los libros tienen capítulos, este "libro mayor" tiene bloques. Estos bloques suelen almacenar información de transacciones con un token, que puede tener valor o no en algún tipo de mercado. Las transacciones se van añadiendo a la cadena de manera constante por lo que el orden es importante. Es por ello por lo que, cuando se escribe un bloque, éste se encripta para crear un *hash*[2] y se escribe ese hash en el bloque siguiente, de ahí que sea una cadena. La blockchain es, pues, un libro mayor en el que se almacenan por orden cronológico todas las tran-

2 Un hash es "la cadena de caracteres de longitud fija que resulta del procesamiento de un archivo digital representada en un algoritmo que crea un valor único". *Cf*. Delle Donne (2020, pp. 232-242).

sacciones de una moneda o token. Los usuarios únicamente necesitan un número de cuenta dentro de esa cadena para recibir tokens en su cuenta y poder enviarlos luego. Los intervinientes dentro de las cadenas son los usuarios, aquellos que dan valor al token, según su oferta y demanda; y los nodos, aquellos que almacenan toda la información de la cadena, que verifican que cuando haya una transacción, la cuenta exista, tenga fondos, etcétera, y que compiten entre ellos para encontrar el hash para ser recompensados con la creación de nuevos tokens (Marín Pérez, 2022, p. 17).

Siguiendo a Heredia Querro, podemos circunscribir las notas características de las blockchain en la descentralización y los protocolos de consenso. Con respecto a la descentralización, la blockchain se basa en una red de computadoras conectadas *peer-to-peer*, donde cada nodo representa un usuario, con una copia exacta de la blockchain. Esta estructura elimina la necesidad de un servidor central y otorga a cada nodo la responsabilidad de mantener el registro, haciendo extremadamente difícil que un ataque externo logre modificar la información almacenada, ya que para alterar la cadena de bloques se requeriría modificar todas las copias distribuidas en cada nodo de la red.

La descentralización, entonces, no solo favorece la seguridad del sistema, sino también su independencia frente a terceros intermediarios, permitiendo la publicación y distribución de datos sin pasar por plataformas centralizadas. Además, el anonimato de los usuarios se garantiza mediante el uso de llaves públicas y privadas, lo cual protege la privacidad mientras mantiene la integridad y transparencia del sistema. Los mecanismos de consenso en blockchain son procesos que permiten a todos los participantes de la red ponerse de acuerdo sobre cuáles transacciones son válidas, sin depender de una entidad central. Este tipo de consenso es esencial para que la blockchain funcione de manera segura y transparente, resolviendo problemas clásicos de los sistemas distribuidos, como el riesgo de doble gasto (es decir, que alguien intente gastar dos veces los mismos activos digitales) o ataques como el *Sybil Attack* (en el cual un atacante crea múltiples identidades falsas para influir en la red). En términos simples, un mecanismo de consenso asegura que todos los nodos de la red coincidan en que las transacciones que se están agregando son correctas y no fraudulentas (Heredia Querro, 2022, pp. 65-77).

En cuanto a los contratos inteligentes[3], para una correcta aproximación, los podemos circunscribir a un programa de computación, el cual puede operar sobre tecnologías de registro distribuido o de otro tipo, cuya función principal es ejecutar los términos expresados en su código. Es decir, a través de los contratos inteligentes

3 El término comenzó a ser utilizado por el criptógrafo Nick Szabo a mediados de la década de los noventa, quien lo ha definido como "un conjunto de promesas especificadas en formato digital, incluyendo los protocolos por medio de los cuales las partes ejecutan dichas promesas". *Cf*. Szabo (1996).

las partes incorporan las cláusulas de un acuerdo en el código de programación del software para que este las ejecute automáticamente ante el cumplimiento de las condiciones correspondientes (Ordóñez, 2020, p. 118).

Sobre sus ventajas, con acierto se ha sostenido que, a diferencia de lo que ocurre con el contrato tradicional, en el contrato inteligente las partes tienen certeza de cuál será la resolución de su conflicto, puesto que en su ejecución no hay participación humana y, por tanto, se prescinde de subjetividades. Si bien es cierto que esa característica puede ser vista como una ventaja o desventaja, no hay duda de que le otorga a este tipo de contratos cierta autonomía y certidumbre que no se advierte en sus pares celebrados de forma tradicional. Por lo demás, no podemos desconocer que recurrir a la Justicia para resolver una disputa en materia contractual suele ser un mecanismo costoso, lento y muchas veces insatisfactorio, por lo que la autonomía de los contratos inteligentes también contribuye en ese aspecto. La otra ventaja que suele atribuirse a los contratos inteligentes es que son seguros. Ello obedece a que el acuerdo de voluntades queda registrado, no en un papel que puede adulterarse o en una computadora que puede hackearse, sino en múltiples equipos que tienen, a su vez, acceso a toda la información, pero de manera encriptada. Ello hace que sea mínima, por no decir inexistente, la posibilidad de que el acuerdo sufra alteraciones, dado que cualquier modificación debería reescribirse simultáneamente en toda la cadena de bloques, a la vista de todos los nodos que componen la red, lo que representaría una dificultad extrema que no es posible de superar con la tecnología que existe en la actualidad (Danesi, 2022, p. 122).

III – ¿QUÉ SON LAS DAO?

Ahora bien, yendo al tema que nos ocupa, a esta altura nos encontramos en condiciones de proponer una definición acerca de las Organizaciones Autónomas Descentralizadas (DAO). En dicho cometido podemos decir, siguiendo a Gravanago, que una DAO es "una entidad autónoma, impulsada por código, que existe en una blockchain. Está diseñada para operar bajo reglas predefinidas y transparentes, que se ejecutan mediante contratos inteligentes. Dichos contratos son programas informáticos que se ejecutan automáticamente cuando se cumplen ciertas condiciones y son los que permiten la toma de decisiones dentro de la DAO sin intervención humana" (Gravanago, 2023). Las DAO buscan que las comunidades alcancen sus objetivos al tiempo que disminuyen la necesidad de que intermediarios gestionen la gobernanza y operaciones derivadas. Los tokens DAO permiten a los titulares votar sobre los cambios en la organización. El uso de cadenas de bloques y activos digitales genera confianza en terceros y proporciona un medio de recompensar a los contribuyentes. Al descentralizar la gobernanza a través de varias partes interesadas y

la divulgación de información operativa y financiera, las DAO pueden reducir la desinformación y las asimetrías de poder (Foro Económico Mundial, 2023, pp. 4-5).

Si tuviéramos que resumir las características de las DAO, diríamos que son entes con tintes empresariales y colectivos cuyos miembros toman decisiones democráticamente, pero careciendo de un órgano de administración o directorio como un CEO. Sumado a esto, sus miembros son completos extraños, dispersos por el mundo, cuyo contacto ha surgido de interacciones en redes sociales como Twitter o Discord, en donde se ha "cocinado" el proyecto que motiva su surgimiento y consiguiente inversión. El primer paso para crear una DAO es la publicación de una propuesta, que es elaborada por los fundadores en un documento fundamental, el "*Whitepaper* de la DAO". Este documento presenta el concepto original del proyecto, junto con otros datos como información técnica, organizativa y de inversión. Los fundadores también ponen a disposición el código de blockchain y el contrato inteligente para promover la colaboración con otros desarrolladores interesados. Luego, la etapa financiera inicial comienza a través de las ofertas iniciales de monedas (ICO, por su sigla en inglés). Los poseedores de criptomonedas que invierten en DAO se convierten en miembros y reciben tokens DAO que se traducen en derechos en la organización, como votar y discutir propuestas. Al final de la etapa de financiación, la DAO comienza a funcionar (Mateus y Sarkar, 2023).

Las DAO se desenvuelven de manera democrática, atento a que sus miembros adoptan en su seno decisiones dentro del marco de la automaticidad de sus reglas operativas dadas por el *smart contract* base, de lo que se deriva que no existe persona o grupo de ellas que ejerzan el rol para la toma de decisiones como lo es de ordinario para otro tipo de entes colectivos. La transparencia y la democracia son pilares fundamentales en el funcionamiento de las DAO. Estas estructuras descentralizadas utilizan la tecnología blockchain para garantizar un registro fiable y transparente de todas las transacciones y decisiones que se toman dentro de la organización[4], es decir, cada una de las transacciones y las reglas de administración de la DAO se registran y mantienen en la cadena de bloques, lo que da fiabilidad en cuanto a su carácter de inalterable, con las consabidas ventajas que ello acarrea, en especial a consideración de que sus contribuyentes (inversores de criptomonedas) pueden tener residencia en cualquier sitio del globo.

IV - CLASES DE DAO

Resulta propicio adentrarnos en una suerte de clasificación de las DAO entre algorítmicas y participativas. Las primeras se caracterizan por tener algoritmos fijos

4 *Cf*. *Estrategias de Inversión*: DAO.

que no admiten modificaciones ulteriores por parte de los inversores; mientras que en las DAO participativas los protocolos permiten nuevas propuestas y la votación de ellas por parte de los titulares de tokens, o de alguna categoría de ellos (Duprat, 2022, p. 580).

Tal situación implica que en la etapa de toma de decisiones en las DAO algorítmicas no exista intervención humana y esta sea definida por el protocolo algorítmico diseñado previamente a extender los tokens a los inversores; mientras que en las participativas los tenedores de tokens serán los que definan esta etapa, habilitados por el propio protocolo pudiendo modificarlo e inclusive cambiar la estructura de diseño de las DAO.

Existen consideraciones a favor y en contra de la gobernanza por algoritmos. En tanto de la vereda de los que están a favor se sostiene que permite lograr un pie de igualdad entre sus participantes, un acceso sencillo y económico al momento de votar y facilidad al contar con toda la información sin estar sujetos a que se publique la orden del día. Sin embargo, del lado de los detractores se considera que no es real que los participantes puedan votar libremente al estar condicionados por el protocolo, el cual, al haber sido creado con anterioridad, no tiene capacidad de adaptación a las situaciones futuras.

Sin embargo, la ausencia de un sujeto definido cuya tarea principal sea la toma de decisiones, lejos de desincentivar su uso, constituye el ser que las informa y genera el crecimiento exponencial de su empleo para encarar bajo tal ropaje digital las más diversas actividades[5] como, por ejemplo: filantropía, financiación de los más variados proyectos[6], gobernanza y decisiones comunitarias[7], solidaridad o la adquisición de bienes[8], algunos de gran importancia en cuanto a su valor.

En tal entendimiento, podemos concluir que las DAO constituyen una moderna herramienta que permite emplearse para alcanzar los más variados fines, los que de antemano signan su forma e incluso su posibilidad de supervivencia y éxito desde la óptica de su realización. Esto no resulta un pensamiento abstracto, todo lo contrario, el objeto al que esté direccionada va a determinar que, en no pocos casos, la

---

5 *Cf.* https://deepdao.io/organizations

6 AntidoteDAO posee como misión financiar directamente la investigación del cáncer, haciéndola más democrática, transparente y colaborativa en todo su proceso. *Cf.* https://daocentral.com/dao/antidote

7 Como es el caso de Aragon que se fundó en el 2016 con el objetivo de poner al alcance de sus usuarios una herramienta para que estos puedan experimentar con la gobernanza a la velocidad de un software, como una opción para abordar las crisis sociales emergentes y, paradójicamente, los fracasos de la democracia tradicional. *Cf.* https://aragon.org/

8 Pleasr se encuentra constituido por un colectivo de artistas y amantes del arte que invierten en arte digital a través de una DAO, en la que los miembros acuerdan las piezas que creen que representan ideas y causas importantes, y cada miembro posee una parte de la creciente colección (Mateus y Sarkar, *op. cit.*).

DAO se vea compelida a adoptar cierta forma dentro de un marco jurídico determinado que le permita el desarrollo y consecución ulterior de su objetivo, premisa que no debe ser pasada por alto y que será materia de análisis. En dicha misión, nos detendremos en tres arquetipos de DAO y sus implicancias, los cuales fueron elegidos por su relevancia en la temática y porque denotan la envergadura comercial/legal del asunto, para luego realizar una sinopsis del encuadre jurídico de las DAO y así finalizar con una breve conclusión.

a) CityDAO

Como primer ejemplo traemos el caso de Wyoming, siendo este el primer lugar de los Estados Unidos en donde, allá por el 2021, se reguló a las DAO que poseyeran la intención de funcionar dentro de dicho estado mediante la Ley N.° 16 del 2022[9] en donde se modificó la ley de corporaciones local (sociedades) para otorgarle un marco legal a aquellas DAO que se encontraran administradas de manera algorítmica a las que se las subsumía dentro de las llamadas *limited liability company* (LLC), las que para un correcto entendimiento local son equiparables a nuestras sociedades de responsabilidad limitadas (SRL) con el consabido efecto de otorgarles personalidad jurídica y limitación de responsabilidad a sus miembros, tema no menor, para lo cual cada DAO debe tener un agente registrado en Wyoming y el agente debe establecer una dirección física y mantener un registro de los nombres y direcciones de los directores de la entidad o personas que desempeñen una función similar (Ruane y McAfee, 2022).

La mentada situación fue el disparador para que en el mismo año un grupo de 6.000 inversores de los más variados lugares como Alemania, Estados Unidos, Irlanda y Canadá, adoptando el carácter de fundadores, se uniesen para crear a la que llaman ciudad del futuro o CityDAO en uso de la cadena de bloques de Ethereum, para lo cual fue necesaria la tokenización de la tierra, y así lograr la descentralización de la propiedad de los activos. La primera inversión bajo dicho formato fue de alrededor de 7 millones de dólares lo que permitió la compra por CityDAO de un inmueble de un poco más de dieciséis hectáreas (40 acres). Los ciudadanos de CityDAO obtuvieron a cambio un token no fungible (NFT) que es un activo digital sin que ello implique una participación directa en la propiedad del terreno en el mundo real. El NFT representa estrictamente los derechos de gobernanza (proponer y votar sobre actividades). Los miembros pueden votar sobre lo que debe hacer la DAO, pero no tienen un retorno directo de esas actividades en forma de ganancias anticipadas (Ruane y McAfee, 2022).

---

9 *Cf.* https://www.wyoleg.gov/Legislation/2022/SF0068

b) bZx DAO

Otro caso paradigmático fue el del bZx DAO, no en cuanto a lo novedoso de su constitución o funcionamiento, sino por las implicancias legales que se produjeron a consecuencia de las resultas de la contienda judicial que tuvo como pretensión inicial el retorno de los fondos invertidos en criptomonedas equivalentes a 1,7 millones de dólares, monto que fue parte de total de 55 millones de dólares robados por el actuar de un hacker mediante el empleo de una técnica de *phishing*, lo que permitió que por una negligencia se develе la clave de las cuentas manejadas por Polygon y Binance Smart Chain pertenecientes a la DAO.

La causa se caratuló "Sarcuni vs bZx DAO"[10] y la demanda se promovió en contra de la DAO bZx y su continuadora la DAO Ooki, los titulares de tokens, sus creadores y diseñadores del protocolo bZx, sus cofundadores y controlantes, dos LLC inversoras en el protocolo bZx y una LLC operadora de la plataforma de trading Fulcrum. La acción intentada pretendió que todos los demandados fueran condenados, ya no en virtud de su responsabilidad individual en la prevención y evitación del fraude y consecuente perjuicio, sino por ser considerados socios de una general *partnership* (sociedad con un régimen similar a nuestras antiguas sociedades de hecho). El 27 de marzo de 2023 el juez del Distrito Sur de California, Larry Alan Burns, dictó sentencia preliminar sobre la mencionada cuestión –que constituía un caso de *first impression*, es decir, que carece de precedentes conforme al principio de *stare decisis* del sistema anglosajón–, haciendo lugar a la demanda en forma parcial. Resolvió que la bZx DAO y su sucesora, Ooki DAO, debían ser subsumidas como una general "partnership" y que los inversores titulares de tokens de la DAO debían ser considerados sus socios y responder, consecuentemente, en forma conjunta, solidaria e ilimitada por sus deudas (Duprat, 2023).

c) El caso argentino: Decentraland

Para un correcto entendimiento del precedente local debemos introducirnos en el denominado "metaverso", concepto que combina a dos grandes tipos de elementos, los cuales predominan en todo el universo virtual. Primero los elementos base que ya conocíamos desde hace tiempo y sobre los cuales se montarán los avances tecnológicos y técnicos propios del metaverso –se trata de internet, la inteligencia artificial, y la tecnología del blockchain, cimientos de todo el ecosistema–; luego, los elementos centrales, grupo integrado por la lógica descentralización, matices de inmersión, una economía nativa digital e identidad mediante avatares (Danesi, 2022,

---

10 "Sarcuni v. bZx DAO", 2023 U.S. Dist. LEXIS 52245, United States District Court for the Southern District of California, 27-3-2023, Filed Case No.: 22-cv-618-LAB-DEB, TR LALEY S/JUR/1/2023.

p. 28). Así, el metaverso se define como una red de mundos en línea inmersivos que pueden experimentarse mediante realidad virtual o realidad aumentada, en los que los usuarios interactúan entre sí y adquieren bienes, servicios e incluso propiedades enteras, elementos algunos de los cuales solo existen en el mundo en línea. El metaverso es una visión futurista de una internet inmersiva y virtual, donde la gente puede conectarse, crear, socializar e incluso experimentar mundos virtuales[11].

Por su parte, Argentina posee la cualidad de ser un país de vanguardia en el surgimiento de *apps* o aplicaciones y unicornios de gran relevancia, sobrepasando sus límites geográficos, incluso los regionales. Dentro de este panorama pujante tecnoempresarial, en febrero de 2020 los *developers* nacionales Esteban Ordano y Ari Meilich crearon Decentraland[12], un mundo virtual de código abierto, construido sobre una red de blockchain (Etherium), que lo que propone a sus usuarios es la participación en eventos como conciertos, desfiles o simplemente explorar las extravagancias del mismo pudiendo interactuar mediante sus *avatars*. En tal sentido, cabe agregar que famosos, cantantes y personalidades de gran exposición participan en el metaverso de Decentraland incrementando el interés del resto de los usuarios por ser parte de este.

Así las cosas, Decentraland tiene su propia moneda virtual llamada "Mana", a través de la cual se puede comprar tierra virtual y a partir de esto conseguir un token que permite participar de las decisiones de la DAO que rige el funcionamiento de este ecosistema. Para tener noción de la envergadura de los que hablamos nos detenemos en su criptomoneda oficial "Mana" la que, a la fecha de realización de este trabajo, posee una cotización de mercado de 0.27849 dólares por unidad. Cabe mencionar que el máximo histórico que ha alcanzado esta divisa digital es de 5.902317 dólares por unidad, encontrándose Decentraland en el lugar #110 de popularidad en el mercado digital[13], lo que hace que, según Coinbase[14], posea una capitalización de mercado total de más de 545 millones de dólares.

V - PERSPECTIVA LEGAL

Visualizando los supuestos traídos a colación desde una óptica local, como punto de partida, no compartimos la solución dada por el magistrado interviniente en los autos "Sarcuni vs bZx DAO", toda vez que el hacer extensiva la responsabilidad a

---

11 *Cf.* https://www.nationalgeographicla.com/ciencia/2023/02/que-es-el-metaverso

12 *Cf.* https://www.decentraland.org/

13 Según una nota publicada el 4/10/2024 en *Infobae*.

14 *Cf.* https://www.coinbase.com/es-la

todos sus miembros mediante el empleo de la figura de la *partnership* implicó quitarle a la DAO la cualidad que las hace atractivas a los inversores. Peor aún, desincentiva su implementación, siendo que subsumir dentro de un formato societario tradicional en su tipología más extrema, a manera de sanción, constituye un precedente negativo y que no se corresponde con un novísimo formato de negocio que ha demostrado sus notorios beneficios en el campo financiero y del *e-commerce* en general. En el punto coincidimos con Duprat al concluir, a la luz del antecede jurisprudencial en estudio, que, en definitiva, para regular los efectos de un negocio novedoso y distinto se aplicó una estructura societaria existente y diseñada para otras realidades. Es evidente que cuesta entender y asimilar el fenómeno del comercio de activos financieros de carácter digital a través de entidades descentralizadas, con las estructuras jurídicas y mentales actuales (Duprat, 2022, p. 580).

Ahora bien, esa renovación o repensar las estructuras jurídicas actuales por las que pugna el citado doctrinario puede encontrar –en alguna medida– solución en el precedente de Wyoming, como un claro ejemplo de adecuación de las estructuras societarias a la nueva realidad que proponen las DAO, al otorgarle la posibilidad de adoptar el formato de una *limited liability company* (LLC) acomodando en uso de tal conducto a una veterana figura corporativa o societaria a los requerimientos de la modernidad, alcanzando así una solución que acarrea, previa observación de los requisitos de la Ley N.º 16 del 2022, la limitación de responsabilidad de sus miembros, lo cual constituye el paradigma de los negocios asociativos de índole comercial, al menos durante los dos últimos siglos y lo que va del presente. Y, la mayor prueba del acogimiento por parte de los inversores de la solución propiciada por Wyoming surge de los propios hechos, con la materialización del proyecto CityDAO, el cual posee basamento real con la adquisición de tierras, hecho que obligadamente condiciona como una necesidad irrefrenable el adoptar un formato legal local (LLC). A manera de ensayo, el procedente en cuestión puede catalogarse de exitoso, siendo que desde lo operativo se encuentra en expansión, solo basta referenciar que en febrero del pasado 2023 CityDAO anunció que otorgaría el primer contrato de arrendamiento NFT del mundo para un terreno en Blanca, Colorado, a alguien con una idea interesante sobre cómo utilizar el terreno. La propuesta será "visada por los ciudadanos de CityDAO, quienes, democráticamente, votarán al ganador, a quien se le otorgará un arrendamiento gratuito del terreno".[15]

Empero, lo expresado da firmeza a la premisa antes expresada acerca de que el objeto al que esté direccionada una DAO en particular va a determinar que se vea compelida a adoptar cierta forma dentro de un marco jurídico que le permita alcanzar el objetivo propuesto para el que fue creada. A manera de ejemplo y trasladando

---

15 *Cf.* https://daotimes.com/the-story-of-citydao-explain-through-timeline/. La traducción nos pertenece.

el caso de CityDAO bajo parámetros locales, en el supuesto de que se pretenda adquirir una fracción de tierras en nuestro país, incluso de una extensión más que considerable, nada obsta a que adquiera en observancia a las exigencias legales de localía una tipología societaria dentro del marco general estatuido por la Ley General de Sociedades N.º 19.550 (LGS) para así lograr la inscripción del inmueble de que se trate a nombre de la misma ya en su formato societario, incluso podría tratarse de un ente de los contenidos por la Sección IV de la LGS, es decir aquellos no constituidos con sujeción a uno de los tipos previstos en la citada norma, sin que tal cuestión sea óbice para la adquisición de un bien inmueble de carácter registrable y sin que a derivación de tal flexibilidad pueda inferirse necesariamente la pérdida de la mentada limitación de la responsabilidad, ello a derivación de lo normado por los arts. 22, 24 y concordantes de la LGS.

Sin embargo, la alternativa recién descripta no constituye la única opción con viabilidad para el caso de que CityDAO ponga el pie en nuestras tierras o que Decentraland pretenda trasvasar parte de su metaverso a bienes tangibles como lo es un inmueble. También podría echarse mano al tan conocido contrato de fideicomiso, tarea que fue realizada en el plano doctrinario por los Dres. Santamaría (2022), quienes al hacerse la pregunta de si es posible en el ámbito local "tokenizar" las posiciones contractuales en un contrato de fideicomiso usando DLTs (blockchain), con sobrada calidad y conocimiento en la materia respondieron a dicho interrogante de la siguiente manera:

> "En la República Argentina, *prima facie*, podemos afirmar que, amén de cuál sea la DLTs que se vaya a utilizar, ya sea pública, privada permisionada o pública permisionada, tales como *Blockchain*, *Ethereum* o *Lacchain*, sí resulta posible tokenizar las posiciones contractuales en un contrato de fideicomiso. Todo ello en virtud de lo establecido en nuestro Código Civil y Comercial de la Nación que, en los arts. 1667, 1669 y 1671 referentes al contenido y la forma del contrato de fideicomiso, estipulan que debe (i) identificar al beneficiario, o al menos contener "la manera de determinarlo" a través de datos que permitan su identificación futura; (ii) individualizar al fideicomisario o hacer constar los datos que permitan su individualización a futuro; (iii) permitir la cesión del derecho del beneficiario por actos entre vivos o por causa de muerte, excepto por una cláusula en contrario inserta en el contrato; (iv) celebrarse por escrito e inscribirse en el Registro Público. Como podemos observar, no habría ningún obstáculo legal que impida que, mediante la utilización de DLTs con wallets criptográficas que cumplan normas vigentes de KYC-AML-CTF y que transaccionen contra una DLT pública, privada o híbrida, se pueda obtener la identificación y autenticación del beneficiario de un fideicomiso ordinario no financiero, e incluso la registración de la cesión de su derecho beneficiario. En otras palabras, es posible gestionar que dentro del mismo contrato la figura del beneficiario o fideicomisario sea representada por los "tenedores de los tokens", optimizando y permitiendo una mayor flexibilidad transaccional referida a dichos *tokens*" (Santamaría y Santamaría, 2022, p. 11).

En síntesis, compartimos lo expresado por los citados autores acerca de las posibilidades y beneficios de utilizar a un contrato de fideicomiso como vehículo para una DAO en particular.

Para finalizar, nos resulta de interés la propuesta consistente en lograr una integración de las DAO y las asociaciones civiles (Gravanago, 2023) bajo la premisa de que la transparencia y la rendición de cuentas en su gobernanza son puntos fundamentales y en común. Para lo cual, en resumidas cuentas, se argumenta acerca de las bondades de implementar el funcionamiento de las DAO en las asociaciones civiles lo que permitiría múltiples beneficios como: crear estatutos híbridos con tecnología de blockchain que logren automatizar el cumplimiento de ciertas reglas de manera confiable; la posibilidad de fortalecer la gestión y el liderazgo en las asociaciones civiles mediante la participación de una autoridad central, como la junta de directivos o líderes designados; la implementación de *smart contracts* que aseguren la transparencia poniendo a disposición el estado financiero con absoluta precisión, etcétera. A tal fin, se resalta la importancia de reconocer las anotaciones en blockchain como documentos digitales, lo que simplificaría la gestión documental y permitiría la creación de estatutos híbridos que aprovechen la tecnología blockchain.

VI - CONCLUSIONES

Llegados a este punto, se torna imposible tapar el sol con la mano y desconocer el hecho de que las DAO son parte de nuestra realidad y que en varios aspectos funcionan de maravilla pudiendo, por ejemplo, agilizar y simplificar cuestiones que muchas veces en el mundo empresarial se tornan de alta complejidad como la deliberación en decisiones asamblearias y el contacto con el orden del día y su previa publicidad.

Bajo tal contexto, consideramos que encasillar a las DAO por completo en un modelo estanco conlleva el serio riesgo de quitarles la calidad de flexibles y descentralizadas siendo tales caracteres las que las tornan atractivas.

En tal sentido, quizás podría percibirse como una postura que arrastra cierta comodidad el adoptar la tesitura de la amplia avenida del medio, a consecuencia de no inclinarnos de manera terminante en relación con un formato legal o tipología societaria establecida de antemano. Sin embargo, ello dista de lo real, siendo que tal concepción encuentra su razón en el hecho de que la envestidura jurídica a adoptarse dependerá del objeto al que en particular la DAO se direccione, el cual signa desde su génesis su elección.

A manera de síntesis, optar entre un formato u otro se centra, desde un inicio, en el objeto societario o del fideicomiso, es decir, el fin perseguido el que constituye, en definitiva, la razón por la cual se conglomeran a los *tokenholders*.

Estamos convencidos de que las DAO no pueden pensarse divorciadas del mundo jurídico. Cuestiones tan simples y usuales como abrir cuentas de banco, contratar empleados, firmar un contrato de locación o la prestación de servicios de cualquier índole hacen necesaria la adopción por parte de la DAO de un ropaje institucional con recepción normativa, sea una sociedad, un fideicomiso o una asociación civil, etcétera. Incluso, más allá del giro ordinario que implican las actividades mencionadas para cualquier ente, existen cuestiones que son trascendentales para quienes poseen la intención de ser parte de una DAO, las que vienen de la mano de asegurar la responsabilidad limitada a la participación en el negocio y la necesaria escisión entre la DAO y el sujeto que la integra. Entender lo contrario, implicaría dejar a las DAO, pese a su existencia digital, afuera del orden natural de las cosas, es decir del mundo analógico, que a la fecha sigue siendo nuestra única realidad.

REFERENCIAS

Danesi, C. C. (Dir.) (2022). *Inteligencia artificial, tecnologías emergentes y derecho. Reflexiones interdisciplinarias* (Tomo 2), Hammurabi.

Delle Donne, C. P. (2020). La extracción de prueba electrónica de teléfonos celulares y la garantía de defensa en juicio. *La Ley*, 12/02/2020, AR/DOC/89/2020.

Duprat, D. A. J. (2022). Las DAOs (Decentralized Autonomous Organizations) y el régimen societario. *La Ley*, 2022-D, 17/08/2022.

Duprat, D. A. J. (2023). ¿Mataron a las DAOs? Las DAOs y su naturaleza societaria. Noticias sobre el fallo 'Sarcuni v. bZx DAO'. *La Ley*, 7, TR AR/DOC/1543/2023, 10/07/2023.

Foro Económico Mundial (2023), *Decentralized Autonomous Organization Toolkit*. https://www.weforum.org/publications/decentralized-autonomous-organization-toolkit/

Gravanago, R. (2023). DAOs y asociaciones civiles. *La Ley*, Año 87, N° 225, 2023-F, 30/11/2023.

Harari, Y. N. (16 de septiembre de 2024). Existe un potencial totalitario en la inteligencia artificial, *La Nación. Suplemento de Cultura*.

Heredia Querro, S. (2022). Smart Contracts: Qué son, para qué sirven y para qué no servirán. SSRN. https://ssrn.com/abstract=3875645

Marín Pérez, C. (2022). Tecnología de blockchain: origen, funcionamiento y usos. Trabajo de Fin de Grado, Facultad de Economía y Empresa, Universidad de Zaragoza. https://zaguan.unizar.es/record/111139#

Mateus, S. y Sarkar, S. (2 de enero de 2023). Can Decentralized Autonomous Organizations (DAOs) Revolutionize Healthcare?, *California Management Review*.

Ordóñez, C. J. (2022). *Derecho y Tecnología*, Hammurabi.

Ruane, J. y McAfee, A. (10 de mayo de 2022). What a DAO Can -and Can't- Do. *Harvard Business Review*.

Santamaría, G. L. y Santamaría, M. M. (29 de diciembre de 2022). Fideicomiso, *blockchain*, tokenización de participaciones y DAOs. Su viabilidad como vehículo jurídico en Latino-

américa ('Being Tokenized'). Año LXXXVI, Nº 265, *La Ley* 2022-F.

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets, *Extropy*, #16. https://docslib.org/doc/246577/smart-contracts.building-blocks-for-digital-markets

ISSN 3008-9484 | DOI 10.5281/zenodo.14509292 **Diálogos y Voces Judiciales** | Vol. 2, N° 2 (diciembre de 2024): 50-61

DERECHOS DEL NIÑO E INTELIGENCIA ARTIFICIAL: UN ANÁLISIS EN CLAVE CONSTITUCIONAL

Children's Rights and Artificial Intelligence: A Constitutional Analysis

María Paula Carril[*]

Universidad Católica de Santiago del Estero
mpaulacarril@gmail.com
https://orcid.org/0009-0003-6970-4508

RECIBIDO: 15/11/2024 - ACEPTADO: 27/11/2024

Resumen: Argentina asumió obligaciones en el plano internacional al suscribir tratados que consagran el derecho de niñas, niños y adolescentes (NNA) a participar y ser oídos en los procesos donde sus intereses se encuentran involucrados. Hoy, la incorporación de la IA en procesos en que estén involucrados derechos de NNA constituye un desafío en clave convencional. El Art. 76 de la Constitución de la Provincia de Jujuy incorporó expresamente la IA en la Reforma del año 2023. Una primera aproximación nos invita a explorar las ventajas y desafíos de utilizar IA en el sistema judicial, particularmente en casos que involucran a NNA, así como las medidas necesarias para asegurar que estas tecnologías respeten y protejan sus derechos, evitando sesgos y asegurando la transparencia y equidad en las decisiones judiciales.

Palabras clave: inteligencia artificial, acceso a la justicia, protección de derechos del niño, proceso judicial

Abstract: Argentina has assumed international obligations by signing treaties that enshrine the right of children to participate and be heard in processes where their interests are involved. Today, the incorporation of AI in processes involving chilren's rights presents a challenge within a constitucional framework. Article 76 of the Constitution of the Province of Jujuy explicitly incorporated AI in the Constitutional Reform of 2023. An initial approach invites us to explore the advantages and challenges of using AI in the judicial system, particularly in cases involving children, as well as the necessary measures to ensure that these technologies respect and protect their rights, avoiding biases and ensuring transparency and fairness in judicial decisions.

Keywords: artificial intelligence, access to justice, child protection, judicial process

La inteligencia artificial (IA) viene irrumpiendo abruptamente en nuestras vidas, a pasos agigantados y en un incesante devenir que parece marcar el puntapié de una era nueva, en un sinfín de aspectos aún desconocidos para el ser humano. Sin embargo, su uso todavía se encuentra transitando una etapa de pleno desarrollo, en la que los grandes avances realizados en el campo –combinados con su enorme capacidad disruptiva– han generado amplios debates y diálogos interdisciplinarios res-

* Abogada por la Universidad Católica de Santiago del Estero. Especialista en Derecho Procesal (UCSE-UNR). Secretaria del Poder Judicial de la Provincia de Jujuy.

pecto a su impacto tanto efectivo como perjudicial.

El fenómeno jurídico que se nos interpone en el horizonte resulta amplio y variado, y se gesta en el marco de una vasta confluencia entre relaciones jurídicas que son impactadas por los cambios tecnológicos y las que no. El universo jurídico no escapa a las transformaciones tecnológicas, y se encuentra profundamente infundido por los cambios que se producen en las relaciones interpersonales, sus modalidades y formas de comunicación.

El indiscutido impacto de las nuevas tecnologías, y en particular de la IA, es un invaluable fenómeno que se posiciona para quedarse entre nosotros y que, en ese impetuoso devenir que va trazando, origina una inasequible cantidad de externalidades que, todas ellas, ponen en jaque viejas estructuras y demandan repensar las nuevas formas y modalidades en que se podrá compaginar un punto de encuentro respetuoso, serio, y razonado entre el acceso a la justicia y la protección de los derechos de los niños en el uso de la IA en el marco de los procesos judiciales.

El presente artículo propone abordar referencias sobre el marco normativo del derecho al acceso a la justicia de niñas, niños y adolescentes (NNA) y pensar en la incorporación de la IA en procesos judiciales en que se involucren derechos de NNA como un desafío en clave convencional; analizar el Art. 76 de la Constitución de la Provincia de Jujuy que incorporó expresamente la IA o no humana en la Reforma Constitucional del año 2023; hipotetizar cómo las herramientas de IA pueden facilitar el acceso a la justicia a los NNA y explorar –como una primera aproximación– las ventajas y desafíos de utilizar IA en el sistema judicial, particularmente en casos que involucran a NNA, así como las medidas necesarias para asegurar que estas tecnologías respeten y protejan los derechos de los mismos; y, por último, ensayar posibles enfoques sobre los que puede pensarse su implementación.

I - ACCESO A LA JUSTICIA DE NNA A 30 AÑOS DE LA REFORMA CONSTITUCIONAL

La incorporación de la IA en los procesos judiciales es un hecho que inevitablemente hemos comenzado a transitar. Cuando en esos procesos judiciales se involucran, discuten, debaten, y deciden cuestiones que directa o indirectamente afectan (de manera positiva o negativa) derechos de NNA, la cuestión toma un matiz diferente y particular. Es que, proteger los derechos de los NNA y concretar en el caso particular el respeto y la vigencia del interés superior del niño como principio o premisa conductora de toda decisión judicial, es una obligación en clave constitucional y convencional.

Decimos que es ésta la piedra angular desde la que debe pensarse la razonable in-

corporación a los procesos judiciales de este fenómeno que constituye la IA. Hoy, creemos que no es errado pensar en que esa paulatina incorporación nos posiciona como operadores jurídicos frente a un enorme desafío en clave convencional. La IA se nos aparece como una herramienta de adecuada respuesta al mandato constitucional que traduce la operatividad de normas relativas a derechos humanos, que han sido consagradas con jerarquía constitucional a partir de la reforma del año 1994.

Nuestro país asumió obligaciones en el plano internacional al suscribir tratados que consagran el derecho de NNA a participar y ser oídos en los procesos donde sus intereses se encuentran involucrados.

El artículo 12 de la Convención de los Derechos del Niño (CDN) establece que "los Estados Parte garantizarán al niño que esté en condiciones de formarse un juicio propio el derecho de expresar su opinión libremente en todos los asuntos que afectan al niño, teniéndose debidamente en cuenta las opiniones del niño, en función de la edad y madurez del niño".

La Observación General Nro. 12 del Comité de los Derechos del Niño (2009) puntualiza que los procesos de escucha de NNA deben ser transparentes, informativos, voluntarios, respetuosos, pertinentes, adaptados a los niños, incluyentes, apoyados en la formación, seguros y atentos al riesgo y responsables. El documento refiere a que el proceso de escucha, o –como lo llama Radcliffe (s.f.)– de participación, debe ser adaptado a los niños, y se concentra en que los ambientes y los métodos de trabajo deben ajustarse a la capacidad de los niños. Se debe prepararlos para dicha actividad, generar confianza con quienes participarán de este proceso y no olvidar el hecho de que los niños necesitarán diferentes niveles de apoyo y formas de participación, acordes con su edad y la evolución de sus facultades.

El Consejo de Derechos Humanos de las Naciones Unidas emitió los "Principios y Directrices de Acceso a la Justicia para las Personas en Situación de Vulnerabilidad" (2016), que proporcionan directrices específicas para asegurar que las personas en situación de vulnerabilidad, incluyendo a los menores, tengan un acceso efectivo a la justicia.

También es atinado remitir a otros instrumentos internacionales que son de aplicación en la materia: la "Recomendación sobre la Ética de la Inteligencia Artificial" (2021), emitida por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), que incluyen la equidad, la transparencia, la inclusividad y la protección de datos, y promueven la inclusión y participación de los niños y otras poblaciones vulnerables en el desarrollo y uso de la IA; las "Recomendaciones del Comité de los Derechos del Niño sobre la Era Digital" (2021), emitidas por el Comité de los Derechos del Niño de las Naciones Unidas, que aborda cómo los derechos de los niños se aplican en el contexto digital (esto incluye la protección contra la explotación y el abuso, el derecho a la privacidad y la participación en la

toma de decisiones que los afectan); y las "Directrices sobre los Niños y la Inteligencia Artificial" (2020), emitidas por el Consejo de Europa, que proporcionan un marco para proteger a los niños en el uso de tecnologías de IA, destacando la necesidad de diseñar sistemas que respeten los derechos del niño y promuevan su bienestar.

Los diferentes Instrumentos Internacionales de Derechos Humanos que fueron incorporados al ordenamiento jurídico argentino con jerarquía constitucional como consecuencia del proceso de constitucionalización del derecho internacional, y los efectos que los procesos de internacionalización de los derechos humanos, constitucionalización y convencionalización tuvieron en la normativa privatista, generaron las bases para el dictado de la norma de fondo y de las de forma que –en esa construcción hermenéutica del juez para el caso particular– deben dar respuesta a una realidad empírica que requiere una adecuación al paradigma de Derechos Humanos.

La incorporación al Código Civil y Comercial del Título VIII "Procesos de Familia" plasmó nuevas directrices y reglas aplicables a los procesos de familia y principios que se direccionan a consagrar el real acceso a la justicia de los niños.

El artículo 706 contempla los principios que deben regir los procesos de familia: tutela judicial efectiva, inmediación, buena fe y lealtad procesal, oficiosidad, oralidad y acceso limitado al expediente. Además, incorpora las siguientes reglas: a) las normas que rigen el procedimiento deben ser aplicadas de modo de facilitar el acceso a la justicia, especialmente tratándose de personas vulnerables, y la resolución pacífica de los conflictos; b) los jueces ante los cuales tramitan estas causas deben ser especializados y contar con apoyo multidisciplinario; y c) la decisión que se dicte en un proceso en que están involucrados niñas, niños o adolescentes, debe tener en cuenta el interés superior de esas personas.

El art. 707, por su parte, consagra el reconocimiento de la facultad que le asiste a los niños como sujetos de derecho, y en su condición de tales, de participar en el proceso. Así, dispone: "Las personas mayores con capacidad restringida y los niños, niñas y adolescentes tienen derecho a ser oídos en todos los procesos que los afectan directamente. Su opinión debe ser tenida en cuenta y valorada según su grado de discernimiento y la cuestión debatida en el proceso".

Las premisas de las que parten los diferentes Instrumentos Internacionales con jerarquía constitucional, y la idea que se abre de un ordenamiento jurídico constitucional convencional, permiten dirigir la mirada y la perspectiva desde la cual deben pensarse, regularse e interpretarse las normas, sin soslayar la realidad social que pretenden abordar, y la consideración de las particularidades de cada caso. Esa visión, que importa un diálogo constante y en retroalimentación entre derecho, ciencia, y cultura, demanda inexcusablemente considerar los cambios y adelantos que

nos acercan la IA y las Tecnologías de la Información y la Comunicación (TIC).

Como bien lo retrata Medina (2021): "Es imprescindible pensar al niño, al adolescente y a cada integrante de su familia, como sujeto de derecho y como objeto de intervención. Sólo así se podrá escuchar algo de su experiencia, al brindarles el lugar para ser protagonistas de su propia historia y ofrecerles un sostén para acompañar su deber. Ello tendrá que ver también con correrse de un lugar de omnisapientes donde se detentaría algún saber acerca de lo que cada uno de esos sujetos necesitan. Así que quienes también trabajan en esta problemática necesitan del trabajo con otros, del aporte de otros, para posibilitar la formación de un dispositivo de atención flexible y articulado que posibilite la producción de los recursos adecuados para dar alguna respuesta eficaz".

II - LA CONSAGRACIÓN CONSTITUCIONAL DE LA IA EN JUJUY

El Art. 76 de la Constitución de la Provincia de Jujuy incorporó expresamente la inteligencia artificial o no humana en la Reforma Constitucional del año 2023:

> "ARTÍCULO 76.- INTELIGENCIA ARTIFICIAL O NO HUMANA 1. Esta Constitución reconoce el derecho de toda persona a utilizar sistemas de inteligencia artificial o no humana, basados en métodos computarizados de algoritmos, datos y modelos que imitan el comportamiento humano y automatizan procesos complejos, así como otros futuros desarrollos que surjan en este campo.
> 2. La ley sujetará estos sistemas a los principios de legalidad, transparencia, responsabilidad, privacidad y protección de datos, seguridad, no discriminación y rendición de cuentas, garantizando el acceso a la justicia en caso de vulneración de derechos y consagrando la acción de solicitud de revisión humana cuando sea necesario.
> 3. El Estado fomentará la investigación y el desarrollo de estos sistemas para fines que modernicen, agilicen y mejoren la prestación de servicios públicos en beneficio de la población, promoviendo la colaboración a estos efectos entre los sectores público y privado.
> 4. El Estado fomentará la educación y el debate público sobre los desafíos éticos y jurídicos que plantean estos sistemas, incluyendo sus efectos sobre la transformación del mundo laboral.
> 5. En caso de conflicto de derechos a partir del uso de estos sistemas, se aplicará el principio de primacía de los derechos humanos y de las libertades y garantías constitucionales a favor de las personas".

La incorporación al texto constitucional de la IA no es una cuestión menor y constituye una novedad su inclusión. Celebramos por nuestra parte la consagración legislativa que necesariamente debe traducirse en un serio compromiso del Estado provincial para concretar los mandatos constitucionales que los convencio-

nales constituyentes han querido consagrar.

No es caprichoso señalar que el reconocimiento del uso de la IA no se agota con esa declaración *stricto sensu*. Demanda más que el reconocimiento de las tecnologías y sistemas de IA que ya conviven entre nosotros, que el Estado asuma la garantía, frente a su uso, de que todo otro derecho no sea vulnerado. Este es el sentido, teleológicamente hablando, en el que, en el marco de una interpretación consecuencialista[1], entendemos debe interpretarse la norma constitucional.

Jorge Llambías (1973, p. 98) enseña que "...el resultado de la interpretación es un elemento de la hermenéutica de enorme valor...cuando legítimamente sea dable extraer dos o más significaciones, entonces sí será ineludible optar por interpretación que reporte el mejor resultado, o sea, el más justo y conforme a las exigencias de la materia social sometida al imperio de la norma en discusión...".

Ya lo hemos señalado antes (Carril, 2019, pp. 113-121), y cabe traer a colación de nuevo esa opinión respecto a que toda interpretación es una tarea que debe efectuarse bajo el prisma que impone el principio de razonabilidad, que –como dice Linares (1970, p. 107)– se traduce en la elección de la alternativa más racional, justa y equitativa de todas las posibles para obtener el fin deseado; y que debe, necesariamente, juzgarse no en abstracto sino en el caso concreto, teniendo presente a su vez el contexto histórico, ideológico, sociológico y fáctico.

El texto establece que la ley sujetará los sistemas de IA a los principios que señala en el apartado 2. Y en los siguientes apartados marca directrices de fomento para futuras políticas legislativas. En el apartado 5 refiere al principio de primacía de los derechos humanos y de las libertades y garantías constitucionales a favor de las personas, en caso de conflicto de derechos. Si bien, esa conclusión resulta una derivación lógica del sistema constitucional convencional, esencial y particularmente aplicable en materia de derechos humanos[2], no es errada –pero sí quizás innecesaria– su expresa mención.

Tenemos entonces para nosotros que el texto constitucional reconoce expresamente el uso de sistemas de inteligencia artificial o no humana, basados en métodos computarizados de algoritmos, datos y modelos que imitan el comportamiento humano y automatizan procesos complejos, así como otros futuros desarrollos que

---

1 Como lo enseña Horacio Rosatti (2010, pp. 87-89), atendiendo a la jerarquía de la norma constitucional, en su interpretación, resulta recomendable asumir un criterio contextual –y no abstracto– de los hechos a ponderar; y consecuencialista, de modo que no se desentienda de las consecuencias que conlleva, una consideración sistémica del ordenamiento y no perder de vista los objetivos centrales del mandato constitucional.

2 En la estructura kelseniana de la norma, acostumbramos a situar en el vértice piramidal a la Constitución Nacional, y por debajo de ese estamento a las restantes normas. A partir de la reforma del año 1994, el constituyente ha impreso un nuevo sentido menos rígido en la interpretación de la jerarquía de las normas. Es la misma Constitución que –en ese carácter de norma primaria y fundante de todo el ordenamiento jurídico– equipara sus normas a otras de carácter internacional que refieren a derechos humanos. La Constitución es

surjan en este campo. La previsión constitucional no sólo focaliza la utilización de los actuales y ya conocidos sistemas de IA, sino que deja en una suerte de cláusula abierta ya sentado el reconocimiento de futuros desarrollos en ese campo. En ese aspecto, resulta impensado, o al menos difícil, aunar consensos frente a eventos cuyas fronteras aún no se avizoran.

No obstante, y siendo que la IA ha tocado la puerta en nuestras vidas, de manera transversal en casi todos los escenarios posibles e imaginables, el proceso judicial no se encuentra exento de los cambios cuyo camino ya ha comenzado a transitarse, y en lo que nos atañe, aún importa un campo desconocido la confluencia entre el acceso a la justicia y la protección de los derechos de los niños en el uso de la IA en el marco de los procesos judiciales.

III - ACCESO A LA JUSTICIA Y PROTECCIÓN DE DERECHOS DEL NIÑO

En palabras de Casiano Highton (2020), vivimos en un devenir constante y ese fenómeno va reuniendo todo un conjunto de hechos aparentemente simples pero que todos juntos producen un cambio que trasciende lo ordinario y termina generando un cambio de época y un cambio de paradigma.

Un amplio campo de investigación se despliega a medida que nos permitimos hipotetizar cómo las herramientas de IA pueden facilitar el acceso a la justicia a los NNA en Argentina, y en particular en la provincia de Jujuy. Una primera aproximación nos invita a explorar las ventajas y desafíos de utilizar IA en el sistema judicial, particularmente en casos que involucran a NNA, así como las medidas necesarias para asegurar que estas tecnologías respeten y protejan los derechos de los mismos, evitando sesgos y asegurando la transparencia y equidad en las decisiones judiciales.

Como dice Schwab: "la nueva revolución digital está evolucionando a un ritmo exponencial, más que lineal. Este es el resultado del mundo polifacético y profundamente interconectado en que vivimos, y del hecho de que la nueva tecnología engendra, a su vez, tecnología más nueva y más poderosa se basa en la revolución digital y combina múltiples tecnologías que están llevando a cambios de paradigma sin precedentes en la economía, los negocios, la sociedad y las personas. No solo está cambiando el 'qué' y el 'cómo' hacer las cosas, sino el 'quiénes somos'" (Schwab, 2016).

La implementación del uso de técnicas y sistemas de IA en procesos en que los intereses de NNA se vean involucrados, necesariamente deberá transitar una gradual, paulatina, sistematizada e integral evaluación de las políticas y regulaciones

---

suprema en el sentido de que realiza repartos de jerarquía: incorpora con idéntica jerarquía a la suya normas internacionales (como sucede con la vigencia del art. 75 inc. 22); y en algunos casos –incluso–, resigna ese primer plano para que otra norma internacional cobre vigencia en el caso concreto.

necesarias para propender a la utilización segura y efectiva de IA en nuestro sistema judicial, con un particular enfoque en la protección de los derechos que asisten a los NNA.

El universo que estos temas ofrecen, sintetiza una amplia gama de aspectos legales, éticos y prácticos para explorar, y pueden contribuir significativamente a la comprensión y mejora de la intersección entre la IA y los derechos de los menores en el proceso judicial.

La protección de los derechos de los NNA en el uso de IA en el sistema judicial es crucial para asegurar que las decisiones automatizadas no perjudiquen a los niños y adolescentes. Es importante garantizar que las herramientas de IA sean justas, transparentes, seguras y libres de sesgos, y que respeten los derechos humanos fundamentales de los niños.

Condensar los diferentes aspectos que deberán tenerse en cuenta en relación a los posibles enfoques que la tarea demandará, resulta un enorme y comprometido desafío al que habrá que dar respuesta, y que despertará debates éticos y morales que confluirán en una indudable y necesaria discusión abierta y plural, que requerirá de inusitada prudencia para construir un orden normativo adecuado, que recepte la cuestión fáctica insoslayable pero en un marco de respeto y garantía de los derechos de los NNA en la utilización de sistemas de IA en el marco de los procesos judiciales.

IV – POSIBLES ENFOQUES PARA EL USO DE IA EN EL ACCESO A LA JUSTICIA Y LA PROTECCIÓN DE LOS DERECHOS DE NNA EN EL PROCESO JUDICIAL

Las aproximaciones son aún (como casi todo en este campo en particular) primeras afirmaciones que no buscan agotarse en sí mismas, y que pretenden ser un punto basal pero abierto al diálogo, y un manto permeable de nuevas ideas que seguramente irán surgiendo y a las que habrá que adecuar incluso con los futuros desarrollos que surjan en materia de IA, que busque satisfacer mecanismos de respuesta en la adecuación a las particulares circunstancias de cada caso en la tarea exegética del juez, sopese los intereses en juego, y evite vacíos normativos que afecten la resolución de casos en los que se encuentren involucrados intereses de NNA.

Nos permitimos apuntar algunas ideas sobre el contenido en el que pensamos se puede comenzar a idear la implementación del uso de IA en el acceso a la justicia y la protección de los derechos de NNA en el proceso judicial:

1. Evaluación de sesgos algorítmicos:
   - *Marco regulatorio para auditorías de equidad*: Proponer la sanción de una ley que exija auditorías regulares de los algoritmos utilizados en el sistema ju-

dicial, específicamente para detectar y corregir sesgos que puedan afectar a los menores. Esta normativa debería establecer estándares claros para la evaluación de la equidad.

- *Obligación de transparencia algorítmica*: Incorporar en la legislación la obligación de los desarrolladores de IA de publicar las metodologías y datos utilizados para entrenar sus algoritmos. Esto permitiría una evaluación independiente y pública de posibles sesgos.

2. Garantía de derechos procesales:
   - *Derecho a la información*: Incluir en las leyes procesales locales el derecho de los NNA y sus representantes legales a tener acceso completo a la información sobre la modalidad y forma en que se toman las decisiones algorítmicas en sus casos, asegurando así la transparencia y el debido proceso.
   - *Mecanismos de impugnación*: Establecer en el marco legal procedimientos claros y accesibles para que los NNA y sus representantes puedan recurrir e impugnar decisiones basadas en el uso de técnicas y sistemas de IA. Esto incluiría la obligación de una revisión humana de todas las decisiones algorítmicas impugnadas o recurridas. De esa manera, creemos que se concreta el mandato constitucional del apartado 2. del Art. 76 de la Constitución de la Provincia.
   - *Abordaje interdisciplinario*: Como dice Radcliffe (s.f.), recurrir al auxilio de la interdisciplina, pero no solo pensada desde el aporte de instrumentos y/o soluciones tecnológicas, sino como aquella herramienta que permitirá abordar el sujeto desde diversas perspectivas. Una base que encontrará la forma de participación que mejor resguarde su interés superior y garantice el ejercicio de su capacidad jurídica.
3. Protección de la privacidad y seguridad de los datos:
   - *Regulación de la privacidad de datos*: Fortalecer las leyes de protección de datos, para asegurar que los datos personales de los NNA sean tratados, procesados, almacenados y utilizados con el más alto nivel de protección. Esto deberá incluir requisitos estrictos para el cifrado en extremo y la anonimización de datos.
   - *Consentimiento informado*: Establecer requisitos legales claros para el consentimiento informado de los NNA y sus tutores antes de la recopilación y uso de sus datos en sistemas de IA.
4. Desarrollo de IA ética:
   - *Normas éticas obligatorias*: Incorporar en la legislación principios éticos obligatorios para el desarrollo de IA y su utilización en el marco de los procesos judiciales, tales como la equidad, la no discriminación y la promoción del bienestar de los NNA en orden a la protección de su interés superior. Las

leyes deberán exigir la inclusión de estos principios desde el diseño inicial de las herramientas de IA.

- *Participación de expertos en derechos del niño*: Crear una comisión asesora permanente integrada por expertos en derechos del niño para supervisar el desarrollo y la implementación de IA en el sistema judicial.

5. Capacitación y sensibilización:
   - *Formación jurídica continua*: Establecer programas de capacitación y formación continua, regular y obligatoria para jueces, abogados, defensores de NNA, funcionarios, agentes del Poder Judicial de la Provincia y auxiliares de la justicia, sobre el uso de IA en el sistema judicial enfocado en la protección de los derechos de NNA.
   - *Sensibilización en derechos del niño*: Promover campañas de sensibilización dirigidas a NNA, familias, profesionales del derecho y operadores jurídicos sobre los derechos de los niños en el contexto del uso de IA en el sistema judicial.
6. Monitoreo y evaluación continua:
   - *Comisión de supervisión independiente*: Crear una comisión independiente, con mandato legal, para monitorear y evaluar continuamente el uso de IA en el sistema judicial, que estará facultada para formular recomendaciones, cambios y mejoras en las políticas y prácticas judiciales para su implementación, y que deberá publicar informes periódicos sobre el impacto de la IA en los derechos de NNA para asegurar la protección continua y mejorada de estos derechos.

Implementar estos enfoques permitirá garantizar que la integración de la IA al proceso judicial en el que se encuentren involucrados derechos e intereses de NNA no solo mejore la eficiencia y el acceso a la justicia, sino que también respete y proteja los derechos de los niños en su uso e implementación.

V - CONCLUSIONES

Es necesario y primordial asumir que los tiempos actuales demandan garantizar un tratamiento especial al desarrollo tecnológico, su uso y su vinculación con el acceso a la justicia y la protección de los derechos de NNA en el proceso judicial. De tal manera, es imperioso comenzar a delinear los enfoques sobre los que puede pensarse su implementación, como un punto de partida que busque satisfacer mecanismos de respuesta en la adecuación de las particulares circunstancias de cada caso en la tarea exegética del juez, sopese los intereses en juego, y evite vacíos normativos que afecten la resolución de casos en los que se encuentren involucrados intereses de NNA.

A treinta años de la Reforma Constitucional de 1994, los derechos humanos han conquistado terrenos antes impensados por el constituyente. La clave de esa conquista decididamente la han constituido los cambios de paradigmas, la irrupción en el derecho interno del derecho internacional de los derechos humanos y la constitucionalización del derecho internacional.

La inevitable incorporación de la IA en los procesos en que se decidan derechos que involucren a NNA es un desafío en clave convencional, que sintetiza un compromiso asumido por el Estado Argentino en materia de obligaciones contraídas en el ámbito internacional en el marco de tratados de derechos humanos que, con la reforma del año 1994, el constituyente ha equiparado con la misma jerarquía normativa a nuestra Carta Magna.

De la mano de la Convención de los Derechos del Niño, el respeto por el interés superior del niño se forjó como una obligación constitucional que, necesariamente requiere consagrarse como un eje transversal en la hermenéutica de cada caso particular, en la interpretación de la norma y en el juego de principios y demás fuentes del derecho, como un estándar obligado e infranqueable. De allí que, la incorporación de la IA a los procesos en que se decidan y discutan derechos de NNA debe, necesariamente, pensarse en clave convencional.

La importancia de la tarea radica en que la injerencia, incorporación y uso de los sistemas de IA no solo constituye una innegable realidad, sino un mandato constitucional consagrado expresamente en Jujuy. El uso de la IA irá aumentando de cara al futuro porque los avances en el campo se presentan a pasos agigantados y la utilización de las tecnologías en los procesos en los que se involucren intereses de NNA estará cada vez más asociada al uso de sistemas y tecnologías intrincadas que incluso aún no conocemos.

Resulta difícil aunar consensos frente a un evento cuyas fronteras aún no se avizoran. Sin embargo, es posible ensayar primigeniamente líneas generales sobre la implementación de la IA en los procesos judiciales y su necesaria vinculación con la protección de los derechos de los NNA.

El desafío que hoy afronta el Derecho es pensar en formas diversas de regular una realidad esencialmente mutable sobre bases suficientemente dinámicas, que puedan servirse también de la propia tecnología, para ir adecuándose y acompañando esa evolución. Es que, si las normas procesales no se actualizan y se adaptan a las situaciones actuales, terminan regulando supuestos de hecho obsoletos y dejan de cumplir justamente su función normativa.

Es justo que los NNA, como personas humanas esencialmente vulnerables que son, sean el epicentro de la regulación y que sus derechos –en ese irrefrenable camino de uso e implementación de las nuevas tecnologías–, no sean mera utopía, sino una verdadera realidad asequible.

REFERENCIAS

Carril, M. P. (2019). La denominada “irrecurribilidad” en las decisiones del Jurado de Enjuiciamiento. Comentarios en torno al fallo 'Brusa' de la Corte Suprema de Justicia de la Nación. *Revista Omnia*, 2(2), 113-121. https://revistas.ucasal.edu.ar/index.php/RO/article/view/253

Consejo de Europa (2022). *Directrices sobre los Niños y la Inteligencia Artificial*. Disponibles en: https://learning-corner.learning.europa.eu/learning-materiales/use-artificial-intelligence-ai-and-data-teaching-and-learning_es

Medina, M. L. (2021). La interdisciplina como herramienta para el análisis sociojurídico. Niños privados de cuidados parentales. En Rey Galindo, M. J. (Dir.) Silva, M. C. del H. y Acuña, M. N. (Coord.). *Derecho de las familias, temas de fondo y forma. La incidencia de la interdisciplina*. ConTexto.

Highton, C. (2020). Los Daños derivados de la Inteligencia Artificial y del impacto de las nuevas tecnologías. Trabajo Final Integrador, Maestría en Derecho Civil Patrimonial. Disponible en: https://repositorio.uca.edu.ar/bitstream/123456789/10922/1/danos-derivados-inteligencia-artificial.pdf

Linares, J. F. (1970). *Razonabilidad de las Leyes*. Astrea.

Llambías, J. (1973). *Tratado de derecho Civil Parte General* (Tomo 1). Abeledo Perrot.

Observación General Nro. 12 del Comité de los Derechos del Niño. Disponible en: https://acnur.org/fileadmin/Documentos/BDL/2011/7532.pdf

Observación General Nro. 25 del Comité de los Derechos del Niño. Disponible en: https://www.plataformadeinfancia.org/wp-content/uploads/2021/09/observacion-general-25-relativa-a-los-derechos-de-los-ninos-en-relacion-con-el-entorno-digital.pdf

Organización de las Naciones Unidas. *Convención de los Derechos del Niño*. Disponible en: http://servicios.infoleg.gob.ar/infolegInterner/anexos/o-4999/249/norma.htm

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), *Recomendación sobre la Ética de la Inteligencia Artificial.* Disponible en: https://www.unesco.org /es/artificial-intelligence/recommendation-ethics

Radcliffe, M. S. (s.f.). La aplicación de nuevas tecnologías al derecho de niñas, niños y adolescentes a participar y ser oídos. Disponible en: https://www.argentina.gob.ar/andis/la-aplicacion-de-nuevas-tecnologias-al-derecho-de-ninas-ninos-y-adolescentes-particular-y-ser

Rosatti, H. (2010). *Tratado de Derecho Constitucional*. Tomo I. Rubinzal Culzoni.

Schwab, K. (2016). *La Cuarta Revolución Industrial*. Ed. Debate.

ISSN 3008-9484 | DOI 10.5281/zenodo.14509465 **Diálogos y Voces Judiciales** | Vol. 2, Nº 2 (diciembre de 2024): 62-82

LA REGULACIÓN DE LA IA: LA PROTECCIÓN DE DATOS Y LA PRIVACIDAD COMO DERECHOS HUMANOS

Regulating AI: Data Protection and Privacy as Human Rights

Rosa Merlín Rodríguez [*]

Universidad Nacional Autónoma de México
rmerlin@politicas.unam.mx
https://orcid.org/0009-0005-0191-4060

RECIBIDO: 14/10/2024 - ACEPTADO: 11/11/2024

Resumen: La inteligencia artificial tiene un gran potencial para mejorar el acceso a la información, pero también presenta riesgos significativos que requieren una regulación adecuada para su uso ético. La responsabilidad de asegurar un uso ético de la IA recae tanto en los Estados, que deben crear marcos legales adecuados, como en las empresas, que deben priorizar los derechos humanos. Es esencial gestionar eficazmente los datos personales para prevenir abusos. Por lo tanto, tanto los Estados como otros actores deben garantizar la privacidad y la no discriminación, implementando regulaciones que protejan los derechos humanos. Este artículo sugiere que adoptar un enfoque que integre los derechos humanos en el desarrollo de la IA promoverá un ecosistema tecnológico más responsable y sostenible.

Palabras clave: inteligencia artificial, derechos humanos: protección de datos, privacidad, regulaciones.

Abstract: Artificial intelligence has great potential to improve access to information, but it also presents significant risks that require adequate regulation for its ethical use. The responsibility for ensuring the ethical use of AI lies with both states, which must create appropriate legal frameworks, and companies, which must prioritize human rights. It is essential to effectively manage personal data to prevent abuse. Therefore, both states and other actors must ensure privacy and nondiscrimination by implementing regulations that protect human rights. This article suggests that adopting an approach that integrates human rights into the development of AI will promote a more responsible and sustainable technological ecosystem.

Keywords: artificial intelligence, human rights, data protection, privacy, regulations.

En un entorno globalizado e interconectado, la utilización masiva de datos que se gestionan desde aplicaciones electrónicas, plataformas en la nube, dispositivos del Internet de las Cosas y la inteligencia artificial (IA) presentan desafíos significativos en la regulación y manejo de la información. Aunque la IA tiene un gran potencial para resolver diversos problemas, su utilización sin principios éticos bien definidos puede representar riesgos importantes para los derechos humanos.

* Lic. en Derecho (Universidad Nacional Autónoma de México), Doctora en Derecho y Gobernanza Global (Universidad de Salamanca). Académica de la Facultad de Ciencias Políticas y Sociales de la UNAM.

> Las nuevas tecnologías generativas son una paradoja del progreso que pueden brindar soluciones a situaciones complejas pero que conllevan un alto riesgo de socavar la dignidad y las garantías fundamentales, advierte el responsable de velar por esos derechos, abogando por regulaciones que también promuevan conductas empresariales responsables y rendición de cuentas (Naciones Unidas, 2023).

En respuesta a esto, organizaciones internacionales como las Naciones Unidas, el Consejo de Europa y la Unión Europea están trabajando en marcos normativos para reducir estos riesgos. Un avance clave ha sido la "Recomendación sobre la Ética de la IA" (2021) de la Organización de las Naciones Unidas para la Educación la Ciencia y la Cultura (UNESCO), que establece pautas éticas aplicables en todas las fases del desarrollo de la IA. No obstante, aunque las resoluciones recientes del Consejo de Derechos Humanos de la ONU destacan riesgos importantes, aún faltan medidas concretas para prohibir o regular aquellas aplicaciones de IA que no cumplan con los estándares de derechos humanos. Esto resalta la urgencia de incorporar los derechos humanos en cada etapa del proceso de la IA, a través de mecanismos de gestión de riesgos efectivos impulsados por gobiernos y empresas.

El respeto, la protección y la promoción de los derechos humanos, las libertades fundamentales y la dignidad humana son esenciales en todo el ciclo de vida de los sistemas de IA. La dignidad inviolable de cada persona, independientemente de su raza, género, religión o condición social, es la base de los derechos humanos. Ningún ser humano o comunidad debe sufrir daños por el uso de IA, y estos sistemas deben mejorar la calidad de vida sin vulnerar los derechos o la dignidad. Además, en las interacciones con la IA, especialmente con personas vulnerables, su dignidad y derechos deben ser siempre respetados (UNESCO, 2021, p.18).

El uso indebido de la IA puede poner en riesgo derechos fundamentales como la libertad de expresión, la privacidad, la igualdad y la protección de datos. La IA presenta desafíos como oportunidades en el ámbito de los derechos humanos, lo que ha motivado su inclusión en diversas propuestas regulatorias internacionales. Es fundamental que el reconocimiento de los riesgos éticos y preocupaciones asociados con esta no frene la innovación. En lugar de ello, se debe fomentar una investigación responsable que no solo impulse el desarrollo tecnológico, sino que también garantice que este avance esté alineado con los derechos humanos, las libertades fundamentales y los principios éticos.

La UNESCO (2021, p. 5) subraya que la IA debe ser desarrollada y aplicada de forma que respete y promueva la dignidad humana, la privacidad, la igualdad y otros derechos. No se trata solo de identificar los riesgos, sino de convertir esas preocupaciones en oportunidades para garantizar que ésta mejore la vida de las personas sin violar sus derechos. Esta visión ética no solo puede proteger los derechos funda-

mentales, sino también abrir nuevas posibilidades para crear tecnologías más inclusivas, responsables y seguras.

Así, la clave radica en encontrar un equilibrio en el desarrollo de la IA y el respeto de los derechos humanos, fomentando un ecosistema tecnológico que priorice la dignidad y los valores éticos. Esto a fin de que la innovación genere un impacto positivo y duradero. No obstante, uno de los principales desafíos es definir con precisión lo que significa aplicar un enfoque de derechos humanos en este contexto. Este estudio busca arrojar luz sobre esa cuestión, subrayando el rol fundamental de los Estados en la creación de marcos legales y normativos para los sistemas de IA que promuevan la responsabilidad de las empresas.

El objetivo de este artículo es revisar las implicaciones de la IA y su regulación en el contexto de la privacidad y la protección de datos personales. Uno de los puntos más preocupantes es el uso de sistemas de IA que gestionan datos personales, ya que esto puede acarrear riesgos significativos, como el tratamiento inadecuado de la información y fallos de seguridad. Estas preocupaciones pueden afectar derechos fundamentales, incluidos el derecho a la vida, la no discriminación, la salud y la privacidad.

Los Estados tienen la capacidad de establecer normativas y políticas para regular el uso y acceso a tecnologías digitales y datos en línea, ajustándolas según sus intereses y valores nacionales: "Es necesario que las nuevas tecnologías proporcionen nuevos medios para promover, defender y ejercer los derechos humanos, y no para vulnerarlos" (UNESCO, 2021, p. 19).

A pesar de que existen marcos normativos tanto a nivel local como internacional para proteger los datos personales, el desafío principal radica en la necesidad de desarrollar mecanismos eficaces que aseguren la protección de los derechos humanos. Es crucial evaluar si el marco legal actual es suficiente para equilibrar la innovación tecnológica con la dignidad humana. Este análisis no solo busca identificar las limitaciones de la regulación existente, sino también proponer estrategias que integren los derechos humanos en el desarrollo de tecnologías de IA, fomentando un enfoque que priorice la seguridad y la ética en la gestión de datos personales.

En consecuencia, en la primera parte de este artículo se aborda la IA desde un punto de vista jurídico. En la segunda, se analizan los precedentes más notables de regulación de la IA. La tercera parte profundiza en aspectos fundamentales como son la protección de datos y la privacidad entendidas como derechos humanos. En la cuarta parte se desarrollan estas cuestiones desde el caso mexicano, repasando las leyes introducidas en los últimos años en materia de protección de datos, incluyendo la creación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). A pesar de estos avances, existen aún en México desafíos importantes. Este trabajo sugiere en las reflexiones finales la nece-

sidad de implementar un modelo de gobernanza coordinado con actores internacionales a fin de establecer un ecosistema digital más seguro y confiable para todas las personas.

I - LA IA: SU COMPRENSIÓN JURÍDICA

La comprensión jurídica de la IA está íntimamente relacionada con los desafíos éticos, sociales y técnicos que plantea su desarrollo. La IA ha permitido la automatización de decisiones en diversos ámbitos, lo que ofrece enormes oportunidades para mejorar servicios e industrias. Sin embargo, también genera importantes interrogantes sobre la responsabilidad, la ética y los derechos humanos. Cabe señalar que la IA no es de aparición reciente; sus orígenes se remontan a los años cincuenta cuando Alan Turing sentó las bases teóricas, y posteriormente se crearon los primeros programas "inteligentes", capaces de resolver problemas.

En los últimos veinte años, la IA, y más específicamente el aprendizaje automático, ha sido esencial en tecnologías digitales como los motores de búsqueda, los algoritmos de recomendación, los drones, los vehículos autónomos y los sistemas de reconocimiento facial. A medida que nuevas formas de IA generativa como *chatbots* y generadores de imágenes avanzados han ganado popularidad, han resurgido antiguos debates y surgido nuevos. Estos modelos tienen el potencial de generar cambios sociales significativos, superando a otras tecnologías de IA debido a su versatilidad, accesibilidad y capacidad para transformar sectores enteros. Sin embargo, también han provocado tanto entusiasmo como preocupación (De Souza Dias y Sagoo, 2024).

Woods (2023) define la inteligencia artificial como el uso de computadoras para tomar decisiones racionales que podrían haber sido tomadas por seres humanos. Mientras que, para De Souza Dias y Sagoo (2024), la IA es una tecnología global que trasciende fronteras y afecta significativamente tanto la vida individual como el tejido social a nivel mundial, influyendo en áreas como la calificación crediticia, las redes sociales, el desarrollo de armamento y la configuración del entorno informativo global.

Dado el avance de la IA, es fundamental contar con plataformas en la nube que permitan entornos separados para desarrollar y entrenar modelos de IA, garantizando al mismo tiempo la seguridad, el cumplimiento normativo y un rendimiento eficiente, incluso en momentos de alta demanda (Juri, 2023).

En este contexto, los derechos digitales adquieren una relevancia crítica. Los derechos humanos, especialmente en lo que respecta a la privacidad y la protección de datos, deben constituir el eje de cualquier regulación relacionada con la IA. Europa, a través del Reglamento General de Protección de Datos (RGPD), ha liderado es-

ta protección, destacando la importancia de equilibrar el progreso tecnológico con la protección de los derechos individuales.

La propuesta de incorporar los derechos digitales en constituciones nacionales, como sugiere Barrio (2023) para España, refuerza la idea de que estos derechos en el entorno digital son una extensión natural de los derechos humanos tradicionales. Sin embargo, sigue siendo un reto crear un marco normativo flexible y robusto que se mantenga al ritmo del avance tecnológico. Este desafío es especialmente notable a nivel global, donde el acceso y uso de la tecnología varía considerablemente entre países, lo que dificulta la creación de normas universales.

II – REGULACIÓN DE LA IA

La convergencia entre la IA y la protección de datos plantea un reto significativo, dado el delicado equilibrio entre el avance tecnológico y las exigencias regulatorias. Si bien la IA puede revolucionar diversas industrias y elevar el bienestar social, su uso a gran escala conlleva riesgos importantes para la privacidad y los derechos humanos. Para asegurar un desarrollo ético y sostenible, es imprescindible mantener un balance entre la innovación y la salvaguarda de los datos, lo que requiere la implementación de un marco normativo robusto que fomente el progreso sin comprometer los derechos individuales.

La transformación digital ha impactado profundamente los principios de la regulación jurídica, incluyendo los derechos humanos (Bieliakov *et al.,* 2023). Aunque la noción de "derechos humanos digitales" no es nueva en Europa, está ganando reconocimiento tanto nacional como internacional. Estos derechos, centrados en las libertades y derechos en internet, han sido respaldados por documentos como la "Resolución sobre la promoción, protección y realización de los derechos humanos en internet".[1]

Si bien los derechos digitales están emergiendo como una extensión natural de los derechos humanos establecidos en la Declaración Universal de Derechos Humanos, su reconocimiento global aún está en una etapa inicial y enfrenta varios desafíos como la rápida transformación de la tecnología que presenta dificultades para desarrollar normas claras y adaptables frente a los cambios constantes. Las diferencias en el acceso y uso de la tecnología entre países y grupos sociales complican la implementación universal de los derechos digitales y, a su vez, los derechos digi-

---

1 *Cf*. "Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo", Consejo de Derechos Humanos, Asamblea General de Naciones Unidas, 38º período de sesiones, 18 de junio a 6 de julio de 2018, disponible en: https://ap.ohchr.org/documents/S/HRC/d_res_des/A_HRC_38_L10.pdf

tales pueden entrar en conflicto con otros derechos fundamentales como la libertad de expresión.

La convergencia entre la IA y leyes estrictas de privacidad, como el RGPD y marcos similares a nivel global, subraya la urgencia de desarrollar estrategias integrales y adaptativas para abordar estos desafíos de manera efectiva. Esto con el fin de salvaguardar los derechos de privacidad individual mientras permiten el progreso tecnológico. Con la proliferación de aplicaciones de IA en áreas como la atención médica personalizada y los sistemas de conducción autónoma, es fundamental integrar de manera efectiva los principios de protección de datos en todas las etapas del desarrollo de la IA (Yanamala y Suryadevara, 2023, p. 295).

La Unión Europea ha liderado la regulación de los derechos digitales con normativas como el RGPD, la cual ha experimentado diversas modificaciones, reflejadas en la actualización de la Ley Orgánica de Protección de Datos (LOPD), que ahora es la Ley Orgánica 3/2018. Esta ley busca la protección de los derechos digitales y autores como Barrio (2023) proponen una futura reforma constitucional para incluir estos derechos, por ejemplo, en la Constitución Española.

El activismo del Tribunal de Justicia de la UE, impulsado por la implementación de la Carta de los Derechos Fundamentales de la UE, fue clave para establecer un enfoque centrado en las personas y en la protección de sus derechos y libertades fundamentales en el ámbito digital. Este proceso normativo sigue en desarrollo bajo la actual Comisión Europea, que ha propuesto diversas iniciativas legales para crear un marco regulador más coherente y unificado. Sin embargo, aunque se priorizan los derechos individuales, estos esfuerzos presentan inconsistencias y ambigüedades que deben resolverse si la UE quiere lograr un marco jurídico común que asegure un entorno digital seguro, transparente y democrático (Pérez de las Heras, 2022).

La UE ha sido proactiva en la regulación de tecnologías digitales basada en valores y principios de derechos humanos y democracia. Desde el inicio ha abordado las implicaciones sociales y éticas de estas tecnologías, especialmente en cuanto a privacidad y seguridad.

Como parte de esta estrategia, se han aprobado directivas y reglamentos que impactan en el uso del mercado digital europeo y han surgido nuevos bienes jurídicos protegidos por la revolución digital. En una década, la Comisión Europea y el Parlamento han emitido más de 30 normativas que afectan las operaciones comerciales en línea (Hidalgo, 2020).

La estrategia digital europea que incorpora como uno de sus ejes clave a la Ley de Servicios Digitales y la Ley de Mercados Digitales. La Ley de Servicios Digitales se enfoca en garantizar un entorno digital más seguro para usuarios y empresas, protegiendo los derechos fundamentales en línea. Los principales temas que aborda incluyen la lucha contra el comercio e intercambio de bienes, servicios y conte-

nidos ilegales en la web, así como el control de los sistemas algorítmicos que facilitan la difusión de desinformación[2].

La segunda, define criterios para reconocer a las grandes plataformas en línea como "guardianes de acceso", centrándose en su influencia sistémica. Entre sus beneficios se encuentran la creación de un entorno más justo para las empresas que dependen de estas plataformas, la apertura de nuevas oportunidades para emprendedores y empresas tecnológicas emergentes, una mayor variedad de servicios y opciones para los consumidores, así como precios más competitivos. Aunque los guardianes de acceso podrán continuar innovando, no podrán emplear prácticas injustas que afecten a las empresas y usuarios que dependen de ellos[3].

El mercado único digital busca suprimir las barreras nacionales en las transacciones electrónicas, fundamentado en el principio del mercado común que favorece el libre movimiento de mercancías, personas, servicios y capitales en la Unión Europea. La Estrategia Europa 2020 subrayó el papel esencial de las tecnologías de la información y la comunicación (TIC) para alcanzar los objetivos de la Unión. Asimismo, el mercado único digital se considera una prioridad central en la Agenda para Europa 2019-2024, impulsada por la presidencia de la Comisión[4].

La creación de un mercado único digital en Europa ha promovido la armonización de normas y el desarrollo de una legislación integral para el comercio electrónico y los servicios digitales.

También la Agenda Digital para Europa de 2010 subrayó la importancia de las TIC para cumplir los objetivos de la Unión. En 2015, la Estrategia para el Mercado Único Digital impulsó el acceso a bienes y servicios digitales, el desarrollo de redes eficientes y el fortalecimiento de la economía digital. La estrategia de 2020 se enfocó en tecnologías que beneficien a las personas y fomenten una sociedad competitiva y democrática. En 2021, la Brújula Digital fijó objetivos en competencias, gobierno, empresas e infraestructuras digitales para el año 2030.

Es así que la Agenda Digital para Europa 2020-2030 busca fortalecer la soberanía digital y asegurar un entorno digital seguro, competitivo y sostenible. Basada en el Tratado de Funcionamiento de la Unión Europea (TFUE), la agenda se enfoca en

---

2 *Cf.* Reglamento de Ejecución (UE) 2023/1201 de la Comisión de 21 de junio de 2023 relativo a las disposiciones detalladas para la tramitación de determinados procedimientos por parte de la Comisión con arreglo al Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo: Ley de Servicios Digitales, DOUE. núm. 159, de 22 de junio de 2023, Recuperada de: https://www.boe.es/buscar/doc.php?id=DOUE-L-2023-80876

3 *Cf.* Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo de 14 de septiembre de 2022 sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales), DOUE, núm. 265, de 12 de octubre de 2022, Recuperada de: https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81470

4 *Cf.* Base jurídica de La ubicuidad del mercado único digital, Parlamento Europeo, Recuperada de: https://www.europarl.europa.eu/factsheets/es/street/43/la-ubicuidad-del-mercado-unico-digital

empoderar a ciudadanos y empresas, fomentar el crecimiento digital y asegurar el cumplimiento de principios éticos en las tecnologías emergentes, como la IA, entre los cuales destacan los siguientes logros (Petit, Wala, *et. al*, 2024):

1. *Conectividad y telecomunicaciones*: se han eliminado los costos de itinerancia, mejorado la conectividad de banda ancha y reforzado la protección de datos y ciberseguridad. Esto garantiza un acceso equitativo a servicios digitales.
2. *Competitividad digital*: se adoptaron normativas como el Reglamento de Servicios Digitales y el Reglamento de Mercados Digitales, que promueven la competencia leal y definen responsabilidades claras para las plataformas en línea, especialmente en lo que respecta a la eliminación de contenidos dañinos.
3. *Inteligencia Artificial*: La Ley de Inteligencia Artificial de 2024 regula su uso, limitando la biometría y prohibiendo prácticas abusivas como la puntuación ciudadana. También se presentó una directiva para asegurar la responsabilidad civil en el uso de IA.
4. *Transformación empresarial y educativa*: Europa pretende que el 80% de los adultos adquiera competencias digitales básicas, aumentando la contratación de especialistas en TIC y promoviendo el uso de IA, la computación en la nube y los macrodatos en empresas.
5. *Infraestructura y tecnologías emergentes*: se promueve la conectividad 5G, el desarrollo de semiconductores y la creación de supercomputadoras, con una inversión significativa a través del Programa Europa Digital (7.500 millones EUR) para proyectos de IA, ciberseguridad y competencias digitales.
6. *Protección de datos y privacidad*: El RGPD sigue siendo un pilar en la protección de la privacidad, mientras que nuevas normativas sobre el uso de datos no personales buscan equilibrar la innovación con la seguridad.
7. *Servicios públicos digitales*: se impulsa la administración electrónica y la interoperabilidad de servicios públicos, con iniciativas para garantizar el acceso en línea a servicios esenciales y establecer un marco de identidad digital europea.

En conjunto, esta agenda refuerza la posición de Europa como líder en la gobernanza digital global, promoviendo la innovación tecnológica, la sostenibilidad y los derechos de los ciudadanos.

El pasado 13 de marzo de 2024, el Parlamento de la Unión Europea aprobó el Reglamento de Inteligencia Artificial (RIA), diseñado para proteger los derechos fundamentales y la seguridad, al tiempo que fomenta la innovación. Este reglamento busca establecer un marco jurídico uniforme para el desarrollo, comercialización y uso de sistemas de IA en la Unión, promoviendo una IA centrada en el ser humano, confiable y alineada con los valores de la UE.

El reglamento también garantiza la libre circulación de productos y servicios basados en IA, clasifica los sistemas según su nivel de riesgo e impone obligaciones para operadores dentro y fuera de la UE. Excluye sistemas de IA con fines militares o de seguridad nacional (Parlamento Europeo, 2024b).

Es indudable que el marco normativo de la UE tiene como objetivo fomentar una IA ética, orientada hacia el ser humano y fiable. Al crear un marco jurídico coherente, se garantiza que los sistemas de IA funcionen de manera responsable, en concordancia con los valores democráticos, evitando la fragmentación entre los Estados miembros y asegurando la libre circulación de productos y servicios.

Este reglamento clasifica los sistemas de IA de acuerdo con su nivel de riesgo y prohíbe ciertas prácticas que podrían comprometer la privacidad y los derechos fundamentales, resaltando la importancia de una regulación dinámica que fomente la innovación sin poner en peligro la protección de datos. La exclusión de sistemas de IA destinados a fines militares pone de manifiesto la complejidad que conlleva la regulación en este ámbito, mientras que la adopción de este reglamento establece un precedente que puede servir de modelo a seguir a nivel global en la intersección de la tecnología y los derechos humanos.

Sin embargo, Rafael de Asís Roig (2024, p. 28) identifica cuatro problemas clave en la intersección entre derechos y tecnologías emergentes, con un enfoque particular en la IA: en primer lugar, se plantea la nueva ética, cuestionando si el discurso de los derechos es realmente adecuado para enfrentar los retos tecnológicos, aunque no se pone en duda su universalidad. Segundo, se menciona la insuficiencia del discurso, destacando que el marco actual de derechos podría no ser suficiente para abordar los desafíos que presentan las nuevas tecnologías, lo que resalta la necesidad de establecer nuevos derechos, como los digitales y los "neuroderechos". Tercero, enfatiza la prioridad de la ética, argumentando que esta debe guiar las discusiones sobre derechos y tecnología. Finalmente, se observa la ausencia de un enfoque de derechos en la regulación tecnológica, subrayando la importancia de integrar la perspectiva de derechos humanos en las políticas relacionadas. Por lo que es fundamental revisar y ampliar el marco de derechos existentes, especialmente en el ámbito de los derechos digitales.

El Consejo de Derechos Humanos, en la resolución A/HRC/20/L.13[5], afirma que los derechos de las personas deben protegerse también en internet, destacando la necesidad de garantizar los mismos derechos que en el mundo *offline*. En especial, subraya la libertad de expresión y el acceso a la información, asegurando que internet siga siendo un espacio abierto y seguro para el ejercicio de los derechos humanos a nivel global.

---

5 A/HRC/20/L.13, "Promoción, protección y disfrute de los derechos humanos en Internet", Consejo de Derechos Humanos 20º período de sesiones, 29 de junio de 2012, Recuperado de: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_hrc_20_L13.pdf

III – LA PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD FRENTE A LA IA

El derecho a la privacidad es esencial para el ejercicio de los derechos humanos en ambos ámbitos, físico y digital. Este derecho constituye un pilar fundamental de las sociedades democráticas y es crucial para el ejercicio de libertades como la expresión, la asociación y reunión, así como para el acceso a derechos económicos y sociales. Su violación puede tener efectos desproporcionados en ciertos grupos, intensificando la desigualdad y la discriminación (ACNUDH, 2024).

El artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos prohíben las injerencias arbitrarias o ilegales en la vida privada, la familia, el domicilio o la correspondencia, así como ataques al honor y la reputación de las personas. Ambos instrumentos garantizan el derecho a la protección legal contra tales injerencias. Aunque el derecho a la privacidad no es absoluto en el marco de los derechos humanos internacionales, cualquier intervención debe estar justificada por la ley y someterse a un examen riguroso de necesidad y proporcionalidad.

Si bien la privacidad es un elemento fundamental de la dignidad humana y requiere protección legal, el derecho a la privacidad se centra en la capacidad de una persona para mantener ciertos aspectos de su vida alejados del escrutinio público.

La privacidad se define como el aspecto más íntimo de la vida de una persona, incluyendo sus sentimientos, pensamientos, emociones, vida familiar y relaciones personales. El derecho a la privacidad capacita a los individuos para decidir sobre su espacio privado y regular la intromisión de terceros, incluidos los Estados, permitiendo así la distinción entre lo que debe ser público y lo que debe permanecer privado. Sin embargo, estos conceptos han evolucionado debido al avance tecnológico, que ha permitido una mayor exposición de aspectos que antes se consideraban exclusivamente privados. En este contexto, es crucial reflexionar sobre la importancia de preservar la privacidad, especialmente en la era de la IA (Mendoza, 2022).

Se debe tener presente que la falta de una adecuada protección de la privacidad en la era de la IA puede afectar la democracia y la libertad individual, así como amenazar libertades personales y minar la confianza en las instituciones. La IA facilita la recolección masiva de datos, lo que permite el acceso a aspectos íntimos de la vida de las personas y plantea dilemas éticos sobre su uso. Sin olvidar que el papel de las empresas tecnológicas en la economía digital puede poner en riesgo el papel de los Estados en la protección de derechos fundamentales.

De tal forma que la protección de la privacidad en la era de la IA es fundamental por varias razones: en primer lugar, porque la privacidad es crucial para la preservación de la democracia y la libertad; en segundo lugar, porque las tecnologías modernas permiten la recolección y procesamiento masivo de datos en tiempo real, lo que

revela aspectos íntimos de las personas; y en tercer lugar, porque el creciente poder de las corporaciones en la economía digital puede reducir el rol de los Estados en la salvaguarda de derechos fundamentales, como la privacidad (Mendoza, 2022).

Por ello, es vital establecer marcos regulatorios sólidos que garanticen la privacidad como un derecho inviolable y salvaguarden el bienestar humano ante los intereses comerciales.

La protección de datos personales es crucial en un entorno en el que los sistemas de IA son capaces de recolectar y procesar grandes cantidades de información. Como se ha mencionado anteriormente, el artículo 12 de la Declaración Universal de Derechos Humanos reconoce el derecho a la no injerencia en la vida privada, lo cual establece un fundamento esencial para la evolución de las normativas y la inclusión de diversas figuras jurídicas que defienden la privacidad.

Las crecientes inquietudes sobre el uso de la IA destacan la necesidad de establecer regulaciones efectivas que protejan la privacidad de los individuos. La presencia de algoritmos sesgados y sistemas de vigilancia inapropiados representa importantes desafíos, ya que pueden amenazar la integridad de la información personal y violar los derechos de las personas. Por lo tanto, es fundamental crear marcos regulatorios que aseguren no solo la protección de los datos personales, sino también la justicia y la transparencia en la aplicación de tecnologías emergentes.

La protección de datos personales y la privacidad son temas críticos que requieren atención a nivel internacional, especialmente en el contexto de la IA. Las resoluciones adoptadas en diversas conferencias internacionales resaltan la importancia de establecer un marco normativo que garantice estos derechos como parte integral de los derechos humanos. Esta necesidad se hace evidente en diferentes foros, donde se ha discutido la urgencia de contar con regulaciones efectivas para salvaguardar la privacidad en un mundo cada vez más digitalizado.

La 27ª Conferencia en Montreux enfatizó la necesidad de que los derechos a la protección de datos y la privacidad sean reconocidos como derechos humanos exigibles a través de un instrumento jurídicamente vinculante por parte de la ONU. Esta declaración es fundamental, ya que establece un precedente que impulsa a los países a adoptar legislaciones que garanticen estos derechos. Asimismo, la 28ª Conferencia en Montreal instó a mejorar la cooperación internacional en la protección de datos y la privacidad, subrayando que un enfoque global es esencial para abordar los desafíos que plantea un mundo interconectado (OEA, 2013).

En cuanto a la necesidad de establecer estándares comunes, la 30ª Conferencia en Estrasburgo y la 31ª Conferencia en Madrid adoptaron estándares internacionales sobre protección de datos y privacidad. Estas normas son cruciales para guiar el tratamiento de la información personal, asegurando que se respeten los derechos de los individuos en diversos contextos. Además, la 32ª Conferencia en Jerusalén

instó a los gobiernos a desarrollar una convención internacional vinculante, lo que resalta la importancia de contar con un marco legal sólido que proteja los derechos de privacidad y datos personales en un entorno digital sin fronteras (OEA, 2013).

Finalmente, la 35ª Conferencia Internacional reafirmó la necesidad de un enfoque equilibrado que no solo proteja los derechos humanos, sino que también mejore la transparencia en el procesamiento de datos. Esta transparencia es vital para asegurar la integridad de las redes y evitar comprometer la libertad de expresión y los intereses económicos. En conjunto, estas conferencias reflejan un consenso creciente sobre la importancia de proteger la privacidad y los datos personales en la era de la IA (OEA, 2013).

En consecuencia, es necesaria la creación de estándares normativos globales que funcionen como leyes modelo e incentiven la cooperación entre países en un contexto de transacciones y flujos de datos internacionales, donde se privilegie el respeto a los derechos humanos.

IV - LA PROTECCIÓN DE DATOS PERSONALES Y PRIVACIDAD EN MÉXICO

Los datos personales se comparan con el "nuevo petróleo" de la era de la información, debido a su potencial para generar valor económico en una época donde la información es un recurso clave. Los datos personales se definen como cualquier información que puede identificar o hacer identificable a una persona física, y son fundamentales para definir la identidad, la privacidad y la seguridad de los individuos (INAI, s.f.). En un mundo cada vez interconectado por internet donde la digitalización y las plataformas electrónicas son fundamentales, la gestión y protección de estos datos se vuelve esencial para preservar la dignidad y la seguridad de las personas.

Esto subraya la relevancia de salvaguardar y administrar de forma adecuada los datos personales, ya que su uso conlleva repercusiones tanto económicas como éticas, siendo esencial para el crecimiento de la economía digital. Actualmente, los datos personales cuentan con un valor económico, equiparable a ciertos activos intangibles, tales como el *software* o el valor comercial de los nombres de dominio. Esto ha llevado a considerarlos como el petróleo de la sociedad de la información y del conocimiento (Mendoza, 2022, p.269).

Los derechos a la protección de datos personales y a la privacidad son dos derechos humanos reconocidos por la Constitución Política de los Estados Unidos Mexicanos. El primero está destinado a salvaguardar el control que las personas tienen sobre el uso de sus datos personales, mientras que el segundo busca proteger su privacidad o vida privada. A estos derechos se añade el derecho al secreto de las comunicaciones, ya que, con frecuencia, los usuarios de redes sociales y otros servi-

cios digitales se conectan mediante plataformas de mensajería electrónica, correo electrónico u otros servicios disponibles para su uso (Recio Gayo, 2022, p.19).

La protección de datos personales en México ha avanzado a través de diversas reformas legislativas. En 2002, la Ley Federal de Transparencia introdujo principios sobre la protección de datos en el ámbito gubernamental. En 2009, una enmienda constitucional reconoció la protección de datos personales como un derecho fundamental, lo que llevó a la promulgación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares en 2010 y su reglamento en 2011. En 2014, se creó el INAI, el cual supervisa el cumplimiento de estas leyes, imponiendo sanciones cuando se violan los derechos de los titulares de datos. Posteriormente, en 2017, la Ley General de Protección de Datos Personales en Posesión de Entidades Gubernamentales reguló el manejo de datos por parte de autoridades gubernamentales.

Esta normativa exige el respeto a los principios legales e internacionales, garantizando una protección integral de los datos personales en todos los contextos, fortaleciendo el derecho a la privacidad en el entorno digital. Como se puede observar, México ha creado un robusto marco legal para proteger los datos personales, asegurado por el artículo 16, segundo párrafo de la Constitución:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros (Cámara de Diputados, 2024a).

Así, se establecen normas para la recolección, uso, almacenamiento, divulgación y transferencia de datos personales, con el objetivo de asegurar tanto la privacidad como la autodeterminación de los individuos (Morales y Flores, 2023, p.210).

Estas normas se rigen a través de los principios ARCO (Acceso, Rectificación, Cancelación y Oposición) que permiten a las personas controlar el uso de sus datos personales en posesión de entidades públicas a nivel federal, estatal o municipal. El término ARCO corresponde a las siglas que identifican cada uno de estos derechos ejercibles por el titular:

1. *Derecho de Acceso*: Cada persona tiene el derecho de solicitar y obtener información sobre los datos personales que están en poder de una entidad. Esto incluye conocer qué datos se tienen, cómo se utilizan y con qué fines.
2. *Derecho de Rectificación*: Las personas pueden pedir que se corrijan o modifiquen datos personales que sean incorrectos, incompletos o desactualizados. Este derecho asegura que la información sobre una persona sea precisa y actual.

3. *Derecho de Cancelación*: Los individuos tienen la facultad de solicitar la eliminación de sus datos personales de una base de datos. Este derecho permite que la información sea suprimida cuando ya no sea necesaria para los fines para los que fue recolectada.

4. *Derecho de Oposición*: Las personas pueden oponerse al tratamiento de sus datos personales en ciertos casos, especialmente cuando se considera que el tratamiento no es legítimo o que afecta negativamente a sus derechos. Esto puede incluir la oposición a la utilización de datos para fines específicos, como marketing.

El ejercicio de los derechos ARCO es exclusivo del titular de los datos, su representante legal o un representante autorizado, y debe realizarse mediante procedimientos gratuitos ofrecidos por la entidad pública correspondiente. Estos derechos se enfocan en proteger los datos personales cuyo tratamiento ha sido autorizado por el titular, a diferencia del derecho al olvido, que abarca cualquier información personal, aunque con restricciones, especialmente cuando entra en conflicto con otros derechos, como la libertad de expresión.

En cuanto a la posibilidad de que organizaciones sin fines de lucro presenten recursos en nombre de los titulares de datos o busquen una reparación colectiva, la ley no contempla esta opción. Solo los titulares de los datos o sus representantes legales pueden buscar reparaciones por infracciones (Data Protection Laws and Regulations Mexico, 2024).

La protección de los datos personales está estrechamente relacionada con el derecho a la privacidad, el cual es reconocido en el artículo 16 de la Constitución mexicana en los párrafos 1 y 12, en donde no está permitido intromisiones en la vida de las personas, en su familia, domicilios o documentos, tampoco en sus comunicaciones privadas, a menos que sea requerido por autoridad competente conforme a la ley:

> Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.
> Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley (Cámara de Diputados, 1917).

El derecho a la privacidad en México revela un marco legal en constante evolución, adaptado para enfrentar los desafíos de la era digital. La Ley Federal de Protección de Datos Personales en Posesión de Particulares establece principios clave

como legalidad, consentimiento, información, calidad y seguridad para la gestión de datos personales por entidades privadas, protegiendo así la privacidad individual y garantizando un manejo adecuado de la información. Complementando esta ley, la Ley General de Protección de Datos Personales en Posesión de Entidades Gubernamentales extiende estos principios al sector público, asegurando una protección uniforme a nivel nacional. Además, a través del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) antes IFAI[6], en cuya reforma constitucional de 2014 se le dota de autonomía constitucional con el objetivo de crear un sistema de coordinación entre la federación y las entidades federativas (Carreón, 2023, p.150); juega un papel esencial en la supervisión y aplicación de estas leyes, promoviendo la cultura de protección de datos y resolviendo reclamaciones para mantener los derechos digitales robustos y efectivos.

Varios instrumentos internacionales abordan los derechos vinculados a la privacidad entre los que se destacan el artículo 12 de la Declaración Universal de Derechos Humanos de 1948, el artículo 11 de la Convención Americana de Derechos Humanos de 1966, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos 1966, el artículo 8 del Convenio Europeo de Derechos Humanos 1950, y la Carta de los Derechos Fundamentales de la Unión Europea 2000.

Cuadro A.
Instrumentos internacionales relacionados con la privacidad

Instrumento Internacional	Artículo Relacionado
Declaración Universal de los Derechos Humanos	Artículo 12: protege la privacidad contra injerencias arbitrarias.
Pacto Internacional de Derechos Civiles y Políticos	Artículo 17: protege la privacidad y la correspondencia contra injerencias arbitrarias.
Convención Americana de Derechos Humanos	Artículo 11: garantiza la protección de la vida privada y la honra personal.
Convenios de la OIT sobre derechos fundamentales de los trabajadores	Si bien no se encuentra un artículo directo sobre la protección de la vida privada, abordan derechos laborales y condiciones dignas.
Convención Americana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Convención de Belem Do Para)	Si bien no se especifica un artículo directo sobre la protección de la vida privada, aborda aspectos relacionados que se vinculan a la violencia de género.

6 IFAI, el entonces Instituto Federal de Acceso a la Información Pública, en 2015 se convirtió en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Convención Interamericana para la Eliminación de todas las Formas de Discriminación de las Personas con Discapacidad	Si bien no se encuentra un artículo directo sobre la protección de la vida privada, aborda derechos y no discriminación que indirectamente pueden relacionarse con la privacidad.
Convenio Europeo de Derechos Humanos (1950)	El Artículo 8 salvaguarda el derecho a la privacidad al asegurar que ninguna entidad gubernamental pueda intervenir en la vida privada, familiar, domicilio o correspondencia de un individuo, salvo que dicha intervención sea conforme a la ley, necesaria y proporcionada en el contexto de una sociedad democrática.
Carta de los Derechos Fundamentales de la Unión Europea (2000)	El Artículo 7 garantiza el derecho a la privacidad al afirmar que cada persona tiene el derecho a que se respete su vida privada, familiar, domicilio y comunicaciones. Esto refuerza la protección de la privacidad dentro del marco legal de la Unión Europea.

Fuente: elaboración propia, con apoyo en ChatGPT.

Como observamos en el cuadro, se muestran los instrumentos jurídicos internacionales y regionales en donde tratan la protección de la privacidad y también se señalan algunos otros que pueden tener una conexión indirecta con dicho derecho (si bien no hacen énfasis en la era digital, se extiende su protección a ésta).

Por ejemplo, la Convención de Belém do Pará aborda la protección de los derechos de las mujeres frente a la violencia, y aunque no se encuentre explícitamente el derecho a la privacidad lo protege dada su vinculación con éste.

El artículo 3 establece que toda mujer tiene derecho a una vida libre de violencia, tanto en el ámbito público como en el privado. Este artículo pone de relieve la importancia de la privacidad como un aspecto esencial en la protección de las mujeres contra la violencia, garantizando que puedan vivir sin el temor a invasiones en su esfera personal y sin que sus vidas privadas sean objeto de abuso (OEA, 1994).

El artículo 4 señala que toda mujer tiene derecho al reconocimiento, goce, ejercicio y protección de todos los derechos humanos y libertades consagradas por los instrumentos regionales e internacionales sobre derechos humanos. Este artículo refuerza que el derecho a la privacidad es un componente fundamental de los derechos humanos universales, estableciendo una base sólida para su protección en el contexto de la violencia de género (OEA, 1994).

El artículo 10 exige que los Estados Partes informen a la Comisión Interamericana de Mujeres sobre las medidas adoptadas para prevenir y erradicar la violencia contra las mujeres, así como sobre las dificultades encontradas en la implementación de estas medidas. Este requerimiento implica un compromiso con la protec-

ción de estas medidas. Este requerimiento implica un compromiso con la protección de la privacidad de las mujeres afectadas, garantizando que la información sobre sus experiencias y datos personales se maneje con confidencialidad y respeto (OEA, 1994).

La Convención de Belém do Pará resalta la importancia del derecho a la privacidad en la protección de las mujeres contra la violencia mediante algunos artículos importantes. Este derecho es esencial no solo para salvaguardar la vida privada de las mujeres, sino también para garantizar que puedan ejercer plenamente sus derechos humanos sin enfrentar invasiones o violaciones de su intimidad, lo cual aplica al ámbito del ciberespacio. Al proteger la privacidad, se asegura un entorno en el que las mujeres puedan vivir libres de violencia y abuso, y en el que sus derechos y libertades fundamentales estén debidamente resguardados. La integración del derecho a la privacidad en la Convención contribuye a una efectiva de la protección de los derechos digitales y de privacidad en el contexto de la violencia de género.

La privacidad en internet abarca una amplia gama de cuestiones, desde el manejo de datos personales con fines publicitarios hasta la vigilancia electrónica, y su interrelación con otros derechos humanos, como la libertad de expresión. Esta preocupación también se extiende a las redes sociales y servicios digitales, donde los usuarios deben actuar con precaución para protegerse contra acciones ilícitas, como el robo de identidad o fraudes.

La digitalización ha permitido la recolección extensa de datos, que abarca desde la actividad en internet hasta la información en redes sociales, generando riesgos considerables para la privacidad.

En las redes sociales, de acuerdo con Recio Gayo (2022, pp. 47-51), la persona usuaria es la titular de sus datos personales y, en muchos casos, también la responsable de su tratamiento. No obstante, existen otros actores, como los proveedores de la red social (SRS), proveedores de aplicaciones y socios, que también pueden asumir esta responsabilidad. Estos actores gestionan y deciden sobre el uso de los datos personales, especialmente para fines comerciales y publicitarios. Además, los socios pueden analizar o combinar estos datos con otros obtenidos a través de servicios digitales, lo que subraya la importancia de que los usuarios revisen las políticas de privacidad para identificar a los responsables del tratamiento de sus datos. A diferencia de los responsables, los encargados del tratamiento solo procesan datos para prestar un servicio, sin utilizarlos para fines propios.

Es crucial que los usuarios conozcan las plataformas que utilizan, incluyendo la identidad de las empresas que las gestionan, el tipo de datos que recopilan, sus usos y sus prácticas de manejo de datos. Utilizar responsablemente las redes sociales y servicios digitales, limitando la información personal compartida y manteniéndose alerta frente a posibles usos indebidos, es esencial para proteger la privacidad y los

derechos asociados.

El INAI ha publicado diversas recomendaciones orientadas a proteger a la población frente a ciberdelitos, tales como el fraude, el robo de identidad y el ciberacoso, poniendo un enfoque especial en la seguridad de los menores y el uso responsable de las redes sociales. Asimismo, en 2022, presentó directrices para el manejo de datos personales en sistemas de IA, resaltando la importancia de estas tecnologías por su capacidad para recolectar, analizar y compartir datos personales. Estas recomendaciones están diseñadas para fomentar un uso ético y adecuado de la información personal tanto en el ámbito público como privado.

Si bien México ha logrado avances en ciberseguridad y desarrollo digital, aún enfrenta desafíos importantes en su capacidad para responder a riesgos cibernéticos y fomentar el desarrollo digital. De acuerdo con indicadores de 2024 se observa que:

· México ocupa el puesto #42 del *National Cyber Security Index*, el cual mide la capacidad de los países para prevenir, manejar y responder a los ciberataques, por lo que es urgente que el gobierno implemente medidas de ciberseguridad más sólidas para enfrentar los riesgos en constante aumento (NCSI, 2024).

· En el *Global Cybersecurity Index* ocupa el lugar #52, destacando brechas en infraestructura, capacidades legales y técnicas, así como en cooperación internacional.

· El #62 en el *E-Government Development Index*, lo cual refleja la necesidad de avanzar en la digitalización y accesibilidad de los servicios gubernamentales.

· *Network Readiness Index* también en el lugar #62, México enfrenta retos en infraestructura tecnológica y habilidades digitales.

A pesar de las propuestas legislativas en materia de ciberseguridad, las posiciones que ocupa México en estos índices indican que aún hay áreas importantes que necesitan mejorar. Por lo que debe concentrar sus esfuerzos en optimizar su capacidad para enfrentar las ciberamenazas y promover servicios más seguros en internet. Es esencial que esto se refuerce con políticas y regulaciones adecuadas para salvaguardar los derechos digitales en un contexto digital cada vez más expuesto a ciberataques. Sobre todo, que la cultura de la prevención de riesgos sea un pilar que el Estado mexicano incorpore dentro de sus ciberestrategias.

V - REFLEXIÓN FINAL

El impulso acelerado de la IA en diversos sectores ha aumentado las inquietudes sobre la protección de datos y la privacidad. Asimismo, los retos éticos asociados con la implementación de la IA, tales como el sesgo algorítmico y la escasez de transpa-

rencia, han emergido como aspectos cruciales que necesitan ser abordados.

La protección de datos personales en la era de la IA no sólo es un imperativo moral y ético, sino es esencial para salvaguardar los derechos humanos. En un mundo digitalizado, es crucial que los derechos a la privacidad y la protección de datos se integren plenamente en la protección de la dignidad y libertad de las personas. Su implementación en diversas áreas de nuestra vida cotidiana genera serios desafíos, como el riesgo de sesgos algorítmicos y vigilancia excesiva, lo que hace necesaria la creación de regulaciones claras que prevengan el uso indebido de la información personal.

Además, en un entorno tecnológico en constante cambio, es vital que las regulaciones se adapten a las nuevas realidades para garantizar que los derechos de los ciudadanos se protejan de manera efectiva. Por lo tanto, la protección de datos y la privacidad deben reforzarse mediante un marco legal robusto y cooperativo a nivel internacional y nacional. Solo así podremos asegurar que la tecnología actúe como una herramienta de empoderamiento en lugar de un mecanismo de control.

Aunque existen propuestas de ley sobre ciberseguridad y de la IA, los índices internacionales revelan que aún persisten áreas críticas que requieren atención. En México no existen leyes que regulen estas materias. Es esencial que el Estado establezca un enfoque preventivo y de riesgos para hacer frente a las ciberamenazas. Por lo que se requiere de un modelo de gobernanza coordinado con actores internacionales a fin de establecer un ecosistema digital más seguro y confiable para la ciudadanía.

REFERENCIAS

Asís, R. de. (2024). De nuevo sobre Inteligencia Artificial y derechos humanos. *Derechos y Libertades: Revista de Filosofía del Derecho y Derechos Humanos*, (51), 25-40. https://doi.org/10.20318/dyl.2024.8582

ACNUDH (2024). *Normas internacionales relativas a la privacidad digital*. https://www.ohchr.org/es/privacy-in-the-digital-age/international-standards-relating-digital-privacy

Bieliakov, K., Tykhomyrov, O., Radovetska, L. y Kostenko, O. (2023). Digital Rights in the Human Rights System. *InterEULawEast: Journal for the International and European Law, Economics and Market Integrations*, 10(1). https://hrcak.srce.hr/305542

Botero Marino, C. (2012). Libertad de expresión e internet, Relatoría Especial para la Libertad de Expresión Comisión Interamericana de Derechos Humanos, OEA. https://oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

Cámara de Diputados (1917). *Constitución Política de los Estados Unidos Mexicanos*. https://diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Carreón, C. (2023). La protección de la legislación mexicana en materia de Internet en un contexto de trabajo híbrido. En Hernández, F. (Coord.). *Esquemas de trabajo híbrido y nuevos escenarios internacionales en las bibliotecas jurídicas*. Instituto de Investigaciones Jurídicas, UNAM. https://archivos.juridicas.unam.mx/www/bjv/libros/15/7210/37.pdf

Data Protection Laws of The World (2024). México. https://dlapiperdataprotection.com/index.html?t=law&c=MX

De Souza, T. y Sagoo, R. (2024). AI Governance in the Age of Uncertainty: International Law as a Starting Point. *Just Security*. https://www.justsecurity.org/90903/ai-governance-in-the-age-of-uncertainty-international-law-as-a-starting-point/

Hidalgo, A. (2020), "Derecho digital en la unión europea, Techlaw y mercado único digital en la década 2010-2020", *Comares Editorial*, España. Disponible en: https://biblioteca.utc.mx/cgi-bin/koha/opac-detail.pl?biblionumber=436845.

Mendoza Enríquez, O. A. (2021). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, 15(48), pp.179-207- https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-214720210000200179.

Morales y Flores (2023). Mexico. En *Privacy, Data Protection and Cybersecurity* (Chapter 12), Edition 10, *Law Business Research Ltd*. https://www.santamarinasteta.mx/wp-content/uploads/2023/11/Mexico-1.pdf.

Naciones Unidas (2023). La inteligencia artificial requiere una gobernanza basada en los derechos humanos. Noticias. https://news.un.org/es/story/2023/11/1526062.

NCSI (2024). *Mexico. National Cyber Security Index*. https://ncsi.ega.ee/country/mx/42.

Organización de Estados Americanos (2013). Resolución La Protección de Datos y la Privacidad deben asegurarse mediante el Derecho Internacional. https://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_conferencias_varsovia_2013_resol_proteccion_datos.pdf

Parlamento Europeo (2024a). La Eurocámara aprueba una ley histórica para regular la inteligencia artificial, 13/03, Unión Europea. https://www.europarl.europa.eu/news/es/press-room/20240308IPR19015/la-eurocamara-aprueba-una-ley-historica-para-regular-la-inteligencia-artificial.

Parlamento Europeo (2024b). *Reglamento de Inteligencia Artificial*, Texto Aprobado, Unión Europea. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf

Pérez de las Heras, B. (2023). El Acuerdo de Libre Comercio entre la Unión Europea y Nueva Zelanda: promoviendo una agenda climática global. *Araucaria*, 25(54). https://revistascientificas.us.es/index.php/araucaria/article/view/23417

Petit A., Wala Z., et. al. (2024). "Una Agenda Digital para Europa". Parlamento Europeo. Disponible en: https://www.europarl.europa.eu/factsheets/es/sheet/64/una-agenda-digital-para-europa

Recio Gayo, M. (2022). *La privacidad en las redes sociales*. INAI. México.

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

Woods, A. K. (2023). Digital Sovereignty+Artificial Intelligence. En Anupam Chander, and Haochen Sun (Eds.). *Data Sovereignty: From the Digital Silk Road to the Return of the State*, New York, 2023; online edn, Oxford Academic, 14 Dic. 2023, *Oxford Academic*. https://academic.oup.com/book/55328/chapter/428796733.

Yanamala, A. y Suryadevara, S. (2023). Advances in Data Protection and Artificial Intelligence: Trends and Challenges. *International Journal of Advanced Engineering Technologies and Innovations*, Vol. 1(01), pp. 294-319. https://ijaeti.com/index.php/Journal/article/view/392.

ISSN 3008-9484 | DOI 10.5281/zenodo.14509560 **Diálogos y Voces Judiciales** | Vol. 2, Nº 2 (diciembre de 2024): 83-99

EL PRINCIPIO DE TRANSPARENCIA Y LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL EN COLOMBIA

The Principle of Transparency and the Regulation of Artificial Intelligence in Colombia

Juana Gabriela Peña González, Juan Esteban Rojas Barbosa, Lai Shin Wong Hernández, Sara Isabel Ruiz Barahona y Valery Isabel Camacho Ríos[*]

Universidad Nacional de Colombia
srodriguezard@unal.edu.co

RECIBIDO: 24/10/2024 - ACEPTADO: 15/11/2024

Resumen: Aunque la IA ofrece grandes oportunidades, también presenta retos significativos, especialmente en la protección de derechos fundamentales como la privacidad y la equidad. Este artículo examina la importancia del principio de transparencia, central en los estándares de la Unión Europea, para la regulación inminente de la inteligencia artificial en Colombia, destacándolo como esencial para un desarrollo ético y justo de esta tecnología. Se compara el progreso regulatorio de la Unión Europea entre 2020-2024 y se propone adoptar la transparencia como pilar central en la legislación colombiana, promoviendo así la confianza pública y la adaptación tecnológica.

Palabras clave: inteligencia artificial, transparencia, regulación, derechos fundamentales, Unión Europea, Colombia

Abstract: Although AI offers great opportunities, it also presents significant challenges, especially in protecting fundamental rights such as privacy and equity. This article examines the importance of the principle of transparency, central to the standards of the European Union, for the imminent regulation of artificial intelligence in Colombia, highlighting it as essential for the ethical and fair development of this technology. It compares the regulatory progress of the European Union between 2020-2024 and proposes adopting transparency as a central pillar in Colombian legislation, thus promoting public trust and technological adaptation.

Keywords: artificial intelligence, transparency, regulation, fundamental rights, European Union, Colombia

La inteligencia artificial (IA) ha emergido como una de las tecnologías más transformadoras de nuestro tiempo, caracterizada por su capacidad para procesar grandes volúmenes de datos y manifestar comportamientos inteligentes. Este tipo de sistemas no solo analiza su entorno, sino que actúa de manera autónoma para alcanzar objetivos específicos, imitando el razonamiento humano en la toma de decisiones, la resolución de problemas y el aprendizaje (Comisión Europea, 2018). Sin

* Estudiantes avanzados de Derecho de la Universidad Nacional de Colombia (UNAL). El presente trabajo fue supervisado por el Dr. Santiago Rodríguez Ardila, abogado defensor de Derechos Humanos y profesor de la UNAL. https://orcid.org/0009-0006-9733-5174

embargo, la IA no es la única innovación que conecta el mundo físico con el digital. Otras tecnologías disruptivas, como la robótica avanzada, la biotecnología, la impresión 3D y la computación cuántica, también están transformando industrias enteras y cambiando profundamente la sociedad.

Este conjunto de avances ha sido denominado por Klaus Schwab, fundador del Foro Económico Mundial, como la Cuarta Revolución Industrial, una era marcada no solo por la velocidad con la que se desarrollan estas innovaciones, sino por su profundo impacto en todas las esferas de la vida (Schwab, 2016). A diferencia de las revoluciones industriales anteriores, impulsadas por la mecanización, la automatización y la electrificación, esta nueva fase se distingue por la capacidad de las tecnologías para procesar grandes cantidades de datos a una velocidad nunca antes vista, generando oportunidades, pero también desafíos significativos para su regulación y control.

A nivel global, la IA presenta desafíos complejos y diversos ya que plantea disrupciones en derechos fundamentales como la privacidad, la seguridad y la equidad. Siendo claro que uno de los principales retos es la protección de los datos personales. Los sistemas de IA dependen del procesamiento de enormes cantidades de datos, que incluyen datos personales, para desarrollar su capacidad de análisis y toma de decisiones. Aunque el Reglamento General de Protección de Datos (GDPR) en Europa ha establecido un marco normativo para regular el uso de la información, el rápido avance tecnológico frecuentemente supera las capacidades regulatorias vigentes. Además, muchos países aún no han implementado una regulación adecuada, lo que genera vacíos legales especialmente cuando los datos personales cruzan fronteras internacionales.

Por otro lado, existe un gran reto en materia de transparencia y explicabilidad en el funcionamiento de los sistemas de IA y sus algoritmos. La falta de claridad en los procesos que siguen estas tecnologías no solo dificulta su supervisión, sino que también compromete derechos fundamentales, como la protección contra la discriminación o el acceso a la justicia, lo que subraya aún más la necesidad de una regulación robusta y adaptativa. Esto último debido a que esta tecnología funciona a través de aprendizaje automático (*Machine Learning*) y puede degenerar en las llamadas "cajas negras", esto es, situaciones en las cuales los desarrolladores no comprenden la forma en que la IA toma determinada decisión (Corvalán, 2017). Estas dificultades afectan directamente a los usuarios, pues respecto al aprendizaje se vuelve aún más complicado dar una explicación sobre el funcionamiento de la IA.

Teniendo en consideración estos retos, resulta evidente que la ausencia de una regulación adecuada no solo pone en riesgo la vulneración de derechos a nivel individual, sino que también puede tener repercusiones a mayor escala, afectando a grupos sociales más amplios. La regulación de esta tecnología tiene como objetivo

evitar contradicciones frente a su rápido desarrollo y promover su integración de manera efectiva y profunda en las instituciones. En este sentido, las políticas de protección de datos resultan esenciales para restringir la recolección y el uso indebido de información, poniendo especial énfasis en los riesgos que implica la ausencia de controles adecuados, como las posibles violaciones graves a los principios de no discriminación, equidad, libertad de expresión, el derecho al trabajo, entre otros. Es fundamental garantizar que las innovaciones tecnológicas se alineen con los principios de dignidad humana, justicia, igualdad y transparencia, asegurando un desarrollo ético y responsable de la IA.

En este contexto, el presente artículo busca responder, conforme a los estándares establecidos por la Unión Europea respecto a la regulación de la IA entre 2020 y 2024, por qué el principio de transparencia debería ser angular en su regulación en Colombia.

El desarrollo de los sistemas de IA ofrece grandes oportunidades. Sin embargo, también han generado una creciente desconfianza que parte del desconocimiento sobre su funcionamiento. De ese modo, la transparencia se erige como un principio fundamental para fomentar la confianza pública y garantizar que la implementación de la IA en Colombia se haga de manera ética y justa.

Por lo tanto, la relevancia de este estudio radica en la necesidad de reducir la incertidumbre y desconfianza que rodea a las tecnologías de IA, principalmente en lo que respecta a la toma de decisiones automatizadas que afectan directamente los derechos fundamentales de las personas a través de una adecuada legislación. Este proyecto no solo aborda el vacío regulatorio en Colombia, sino que también propone el principio de transparencia como un elemento esencial para asegurar que las nuevas tecnologías sean seguras, responsables y aceptadas por la sociedad. El estudio adopta un enfoque comparativo con los estándares europeos, cuya avanzada regulación de IA puede ofrecer valiosas lecciones para la legislación colombiana.

La estructura del artículo comienza por un análisis general de la Cuarta Revolución Industrial y la IA, para exponer el contexto de la revolución tecnológica y sus implicaciones en la regulación normativa. A continuación, se desarrolla el principio de transparencia en la regulación de IA, explorando sus fundamentos y alcances, para luego hacer un examen de los estándares internacionales en la regulación de IA tomando como referencia el caso de la Unión Europea entre 2020 y 2024. Después, se detalla el desarrollo normativo que ha tenido la IA en Colombia, para destacar desafíos y oportunidades en la creación de un marco regulatorio. Posteriormente, se realiza una comparación entre los estándares europeos y la propuesta regulatoria colombiana, lo que ofrecerá una visión crítica sobre las posibles adaptaciones de dichos estándares al contexto local. Finalmente, el artículo plantea una serie de recomendaciones para la adopción de un marco regulatorio adecuado en el país, tenien-

do como eje fundamental el principio de transparencia.

I - EL PRINCIPIO DE TRANSPARENCIA EN LA REGULACIÓN DE LA IA

El principio de transparencia se erige como un eje central en el desarrollo y regulación de la IA, debido a su capacidad para generar confianza pública, garantizar la rendición de cuentas y proteger los derechos fundamentales. La transparencia implica la existencia de políticas claras y accesibles para los usuarios, y la educación sobre el funcionamiento y las limitaciones de los sistemas de IA (Ruiz, 2022). En este sentido, es esencial que existan mecanismos efectivos de supervisión y responsabilidad para que, tanto los desarrolladores como los usuarios y las autoridades reguladoras, puedan entender y evaluar cómo se hace la toma de decisiones automatizadas.

Este principio exige que los procesos y decisiones de la IA sean comprensibles y accesibles, no solo para rastrear y explicar cómo se llega a una decisión, sino para permitir una evaluación crítica de su equidad, evitando posibles sesgos y discriminación (Araya, 2021). En el contexto de los desafíos éticos y sociales que plantea la IA, el principio de transparencia aborda los aspectos más relevantes, teniendo un impacto directo en las dimensiones socioeconómicas y en la confianza de los usuarios hacia las innovaciones tecnológicas. Asimismo, la transparencia juega un papel fundamental en contrarrestar la desinformación en torno al desarrollo de la IA.

En comparación con otras tecnologías emergentes, la IA tiene un impacto de mayor envergadura, dada su complejidad, lo que ha fomentado percepciones contradictorias o falsas sobre su uso. Implementar políticas claras y accesibles que acompañen su despliegue facilita un mayor uso responsable de esta tecnología, y también fomenta un aprendizaje más rápido por parte de los usuarios, lo que fortalece la interacción entre la IA, la sociedad y los derechos que deben salvaguardarse en este proceso de evolución tecnológica (Carvajal, 2021).

II - LOS ESTÁNDARES DE LA UNIÓN EUROPEA (2020-2024)

La regulación de la IA en la UE ha sido propiciada desde el año 2020, año en el cual la UE empezó a abordar los retos de la IA con la "Estrategia Europea de Inteligencia Artificial", la cual se planteó como marco de referencia para el periodo 2020-2025. Esta estrategia se propone orientar los planes sectoriales, nacionales y regionales en esta materia, en línea con las políticas desarrolladas por la UE, e impulsar la transformación de los diferentes sectores económicos mediante la cooperación público-privada.

Bajo este marco, la Comisión Europea presentó el "Libro Blanco sobre la inteli-

gencia artificial: un enfoque europeo de la excelencia y de la confianza"[1], el cual se estableció como la primera y principal propuesta para una regulación adecuada de la IA. El Libro Blanco establece opciones políticas de cómo lograr el doble objetivo de promover la adopción de la IA y abordar los riesgos asociados en el uso de dicha tecnología. Asimismo, tenía como objetivo explicar el desarrollo de un ecosistema de confianza al proponer un marco legal para una IA confiable, basado en los valores y derechos fundamentales de la UE, para darle a los usuarios la confianza en adoptar soluciones basadas en IA, al tiempo que alienta a las empresas a desarrollarlas.

El Parlamento Europeo también planteó un debate sobre la transición digital. Dentro de sus conclusiones se resaltó que debían asegurarse una mejor coordinación, así como más redes y sinergias entre los centros europeos de investigación basada en la excelencia, logrando que se proporcione una definición clara y objetiva de los sistemas de IA de alto riesgo.

El 21 de octubre de 2021, la Comisión Europea dio el siguiente paso y publicó una propuesta de "Reglamento para la armonización de las normas en materia de inteligencia artificial" y un plan coordinado que incluyó una serie de acciones conjuntas para la Comisión y los Estados miembros. Con éste, se buscó mejorar la confianza en la IA y fomentar el desarrollo y la actualización de la tecnología de IA, siguiendo un enfoque basado en los riesgos y establecer un marco jurídico horizontal y uniforme para la IA encaminado a garantizar la seguridad jurídica. En efecto, la propuesta de Reglamento ha sido un elemento clave de la política de la UE que apunta a consolidar el desarrollo y la adopción, en todo el mercado común, de una IA segura que respete los derechos fundamentales.

El avance del proceso legislativo durante los años 2022 y 2023 estuvo marcado por una serie de debates. El 6 de diciembre del 2022 el Consejo Europeo adoptó su posición sobre el Reglamento de IA, mencionando que este nuevo reglamento debía estar encaminado a garantizar que los sistemas de IA introducidos y posteriormente utilizados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos humanos, así como los valores de la Unión Europea. Al cabo de ciertas discusiones, el Consejo y el Parlamento Europeo alcanzaron un acuerdo provisional sobre el reglamento el 9 de diciembre de 2023.

Finalmente, el 21 de mayo de 2024 el Consejo adoptó el "Reglamento de Inteligencia Artificial"[2], un acto legislativo innovador que armoniza las normas sobre IA y a-

---

1 El Libro Blanco destaca la necesidad de reforzar las capacidades industriales y tecnológicas, con la correspondiente adaptación normativa de coordinación y de gobierno, que impulse este crecimiento de las capacidades de manera ética y fiable, alineado con la postura de la UE, así como con el correspondiente marco de seguridad y responsabilidad civil.

2 Presentado por el Consejo Europeo como "la primera norma jurídica del mundo sobre IA", el Reglamento de Inteligencia Artificial clasifica las aplicaciones de IA en tres categorías de riesgo. La primera prohíbe las apli-

dopta un enfoque basado en el riesgo. Como se lee en los fundamentos, "cuanto mayor sea el riesgo de causar daños a la sociedad, más estrictas serán las normas". Por ello, sus objetivos son fomentar el desarrollo y la adopción de sistemas de IA seguros y fiables en todo el mercado único de la UE por parte de agentes públicos y privados, garantizando el respeto de los derechos fundamentales de los ciudadanos de la UE, y estimular la inversión y la innovación en IA en Europa.

Si bien la Comisión ha planteado que el enfoque basado en el riesgo es la base de un conjunto proporcionado y eficaz de normas vinculantes, señaló asimismo la importancia de las "Directrices éticas para una IA fiable"[3], de 2019, las cuales han sido elaboradas por el Grupo Independiente de Expertos de Alto Nivel sobre IA creado por la Comisión. Este Grupo Independiente desarrolló siete principios éticos que tiene por objeto garantizar la fiabilidad y el fundamento ético de la IA. Estos principios son:

1. *Acción y supervisión humana*: se entiende que los sistemas de IA se desarrollan y utilizan como herramientas al servicio de las personas, que respeta la dignidad humana, y que funciona de manera que puede ser controlada y vigilada por los seres humanos.
2. *Solidez técnica y seguridad*: consiste en que los sistemas de IA se utilicen de manera tal que sean sólidos en caso de problemas, como alteraciones o el uso ilícito por terceros, y reducir al mínimo los daños no deseados.
3. *Gestión de la privacidad y de los datos*: se entiende que los sistemas de IA deben ser desarrollados y utilizados de conformidad con normas en materia de protección de la intimidad y de los datos, al tiempo que tratan datos que cumplen normas estrictas en términos de calidad e integridad.
4. *Diversidad, no discriminación y equidad*: los sistemas de IA deben incluir a diversos agentes promoviendo la igualdad de acceso, la igualdad de género y la igualdad cultural, evitando los efectos discriminatorios y los sesgos injustos prohibidos por el derecho nacional o el de la Unión Europea.
5. *Bienestar social y ambiental*: los sistemas de IA se deben desarrollar y utilizar

---

caciones y sistemas que supongan un riesgo inaceptable, como los sistemas de puntuación social gestionados por el gobierno, como los que se utilizan en China. En segundo lugar, las aplicaciones de alto riesgo están sujetas a requisitos legales específicos, como una herramienta de escaneo de CV que clasifica a los solicitantes de empleo. Tercero, las aplicaciones que no están explícitamente prohibidas o catalogadas como de alto riesgo quedan en gran medida sin regular.

3 La fiabilidad de la IA se apoya en tres componentes: a) la IA debe ser *lícita*, cumplir todas las leyes y reglamentos aplicables; b) *ética*, de modo que se garantice el respeto de los principios y valores éticos; y c) *robusta*, tanto desde el punto de vista técnico como social, puesto que los sistemas de IA pueden provocar daños accidentales. Cada uno de estos componentes es en sí mismo necesario, pero no suficiente. Lo ideal es que todos ellos actúen en armonía y de manera simultánea.

de manera respetuosa con el medio ambiente, así como en beneficio de todos los seres humanos, al tiempo que supervisan y evalúan los efectos a largo plazo en las personas, la sociedad y la democracia.

6. *Rendición de cuentas* del desarrollo y utilización de los sistemas de IA.
7. *Principio de transparencia*: los sistemas de IA deben ser desarrollados y utilizados de un modo que permita una trazabilidad y aplicabilidad adecuada, que garantice que personas sean conscientes cuando interactúan con un sistema de IA, y que se informe debidamente a los responsables del despliegue acerca de las capacidades y limitaciones de dicho sistema de IA, y a las personas afectadas acerca de sus derechos.

El cumplimiento del principio de transparencia en los sistemas de IA se materializa a través de la provisión de documentación clara, accesible y comprensible, que debe acompañar a cada sistema antes de su despliegue. Esta documentación debe incluir instrucciones de uso detalladas, e información técnica sobre el funcionamiento del sistema, sus algoritmos y los procesos de toma de decisiones automatizadas. Es esencial que los usuarios y responsables tengan acceso a datos sobre los criterios que utiliza la IA para generar resultados, las limitaciones del sistema y cualquier riesgo potencial para la salud, la seguridad o los derechos fundamentales. Esto se refleja en la capacidad de los usuarios de solicitar auditorías o revisiones del sistema para asegurar que su funcionamiento sea conforme a las normativas y estándares aplicables.

Adicionalmente, para que el principio de transparencia se considere plenamente cumplido, la información proporcionada debe estar adaptada al perfil de los usuarios finales. Esto implica que la complejidad técnica del sistema de IA debe ser explicada en un lenguaje que permita su comprensión sin requerir conocimientos avanzados. También deben estar presentes mecanismos de supervisión que permitan a los usuarios monitorear, controlar y corregir el funcionamiento del sistema cuando sea necesario. En términos normativos, la transparencia se concreta mediante la creación de marcos regulatorios que exijan a los desarrolladores y proveedores de IA la entrega de informes periódicos y la realización de evaluaciones de impacto para demostrar que el sistema sigue operando de manera segura y conforme a las leyes vigentes.

Al respecto, el Reglamento establece que, debido a las preocupaciones relacionadas con la opacidad y la complejidad de determinados sistemas de IA, es necesario exigir un alto grado de transparencia en los sistemas clasificados como de alto riesgo, evaluando su impacto antes de ser desplegados. Estos sistemas, cuya operación puede tener un efecto significativo en la seguridad, los derechos fundamentales o la vida de las personas, requieren un diseño que permita a sus implementa-

dores comprender su funcionamiento, evaluar su rendimiento y conocer tanto sus fortalezas como sus limitaciones. La importancia de esta regulación radica en que los sistemas de IA de alto riesgo, debido a su potencial para generar consecuencias graves, deben estar sujetos a medidas estrictas de supervisión humana, auditoría y responsabilidad, garantizando así su seguridad, fiabilidad y cumplimiento con los derechos fundamentales.

En efecto, el principio de transparencia exige que los sistemas de IA proporcionen información clara y accesible para garantizar un uso responsable y seguro. Por ello, la transparencia en la documentación proporcionada es fundamental para que quienes desplieguen estos sistemas tomen decisiones informadas y los utilicen de manera adecuada. Se espera que la información permita a los usuarios seleccionar correctamente el sistema de IA que mejor se ajuste a sus necesidades y que comprendan los usos permitidos y prohibidos. Como resultado se busca que la información que se encuentra plasmada en las instrucciones de uso sea fácil de entender y más accesible, así los proveedores tienen la responsabilidad de asegurar que toda la documentación sea significativa, completa y comprensible, y que esté diseñada considerando los conocimientos y necesidades de los usuarios finales.

Por lo tanto, el cumplimiento de las obligaciones de transparencia aplicables a los sistemas de IA que entran en el ámbito de aplicación del Reglamento no debe interpretarse como un indicador de que la utilización del sistema de IA o de sus resultados de salida es lícito, y por el contrario debe implementarse sin perjuicio de otras obligaciones de transparencia aplicables a los responsables del despliegue de sistemas de IA establecidas en el derecho de la Unión o en la legislación de cada Estado.

III - EL DESARROLLO NORMATIVO DE LA IA EN COLOMBIA

En el caso colombiano, no existe una regulación de la IA. Además, las leyes vigentes en materia de datos personales no contienen disposiciones específicas sobre la IA, por lo que es pertinente plantearse su suficiencia respecto a los riesgos que implica el avance tecnológico de la IA y la materialización de dichos riesgos frente a los derechos fundamentales y la protección de datos personales.

De este modo, la normatividad aplicable respecto al uso de la IA, partiendo del supuesto de que su funcionamiento implica el tratamiento de datos personales, es aquella sobre protección y tratamiento de datos personales, la cual está recogida principalmente en las Leyes 1.266 de 2008 y 1.581 de 2012. De manera conjunta, estas normas han consagrado principios como la transparencia, proporcionalidad, finalidad, responsabilidad proactiva, la implementación de esquemas de cumplimiento normativo y ético, en desarrollo del derecho fundamental del *habeas data*, consagrado en el artículo 15 de la Constitución Política. De este modo, la legislación vi-

gente proporciona un marco robusto que garantiza el control sobre la información personal, en aplicación del principio de transparencia que obliga a las entidades que tratan datos a actuar con apertura y claridad, y permitiendo a los titulares de los datos conocer, en todo momento, cómo y para cuáles fines se utiliza su información personal.

Si bien, como sugerimos, Colombia carece de una regulación integral de la IA, sí se ha dado un desarrollo normativo recogido en directrices de algunas entidades de orden nacional. El CONPES 3975 de 2019 es la principal herramienta de dirección sobre la implementación de la IA en Colombia, con el cual se adoptó una política nacional para la transformación digital e IA, en desarrollo de principios claves con los que se busca balancear la protección de los derechos fundamentales, y el fomento de la innovación y confianza en la IA, para que Colombia pueda aprovechar las oportunidades y enfrentar los retos relacionados con la Cuarta Revolución Industrial.

Recientemente, el Ministerio de Ciencia, Tecnología e Innovación presentó la "Hoja de Ruta de la Inteligencia Artificial para Colombia", un documento con el cual busca guiar el desarrollo de políticas, acciones y decisiones del Gobierno Nacional, y que tiene como puntos esenciales la ética y gobernanza de la IA, haciendo énfasis en la transparencia de los algoritmos, y el manejo seguro de datos para garantizar una adopción ética y sostenible de la IA en el país. Paralelamente, el Ministerio presentó el Proyecto de Ley 447 de 2024 con el objetivo de impulsar el uso responsable de datos para el desarrollo de políticas públicas y la producción de IA en Colombia, en un marco general de aprovechamiento de la infraestructura de datos del Estado, para orientar la toma de decisiones del Gobierno de manera tal que "permitan mejorar la calidad de vida de los ciudadanos y el desarrollo de las actividades sociales y económicas del país" (art. 1). Adicionalmente, en el marco de la Cumbre Nacional de Inteligencia Artificial, el Departamento Nacional de Planeación anunció la publicación de un nuevo CONPES sobre la IA, que busca incentivar su desarrollo, en el marco de un uso ético y sostenible para impulsar la transformación social y económica de Colombia.

A nivel legislativo, en concordancia con lo que sucede a nivel global, en Colombia se ha visto un claro interés por regular la IA, ya que desde el 2023 se han presentado varios proyectos de ley en el Congreso de la República que proponen una regulación integral basada en principios éticos y derechos humanos. Dentro de estos numerosos trámites incluso se llegó a configurar una Comisión Accidental sobre Proyectos de Ley de IA en el Congreso, con el objetivo de unificar criterios y construir consensos, para construir una regulación que respete los principios de transparencia, equidad y justicia, y para que esta tecnología se desarrolle en un entorno ético.

Entre los proyectos de ley presentados están el 59 de 2023, el 91 de 2023, el 130 de 2023, el 156 de 2023, el 200 de 2023 y el 255 de 2024. En términos generales, la mayo-

ría de los proyectos buscan crear un marco general e integral sobre la adopción y uso responsable de la IA. Sin embargo, son proyectos que apenas han avanzado en su trámite legislativo, por lo que ninguno ha llegado a convertirse en ley, y en su mayoría han sido archivados.

Todos los proyectos de ley parten de la incorporación de una definición de la IA, su ámbito de aplicación y los actores obligados al cumplimiento de la regulación. También se ha evidenciado como común denominador la consagración explícita del principio de transparencia. Así, por ejemplo, el PL 59/23C busca que los responsables del uso y desarrollo de IA expliquen las causas que dan lugar a las decisiones o predicciones de los algoritmos (art. 14); el PL 200 de 2023 hace un análisis crítico en relación con el principio de transparencia y los estándares de protección de derechos humanos, por ejemplo, al establecer la información que las empresas tienen que hacer pública acerca de sus productos, los datos que utiliza, el proceso de desarrollo, la finalidad del sistema, así como dónde y quién lo utiliza. Así, se delimitan una serie de responsabilidades en cabeza de las entidades públicas y privadas, y la protección de los usuarios, al plantear que la Superintendencia de Industria y Comercio (SIC) haga procesos de auditoría de IA, sistemas de evaluación de riesgos y de impacto en los derechos fundamentales. De este modo, se obliga a las empresas a registrar sus modelos de IA en una plataforma administrada por la SIC, que certificaría la adecuación de los modelos a los derechos humanos.

De igual forma, la mayoría de los proyectos contienen disposiciones sobre la discriminación, igualdad de trato y oportunidades. Por ejemplo, el PL 200/23 prohíbe la implementación de IA en ciertas actividades como la calificación de perfiles para el otorgamiento de créditos y la predicción de conductas delictivas, o el reconocimiento de emociones y la influencia en votantes (art. 13). En relación con la protección de datos personales se habla del consentimiento informado para el uso de datos personales.

Estos antecedentes demuestran la necesidad de crear un consenso sobre el marco regulatorio adecuado para el desarrollo y uso de IA que vaya de manera acorde con los derechos humanos.

En el ámbito judicial, en la sentencia T-323 de 2024, la Corte Constitucional Colombiana destacó la importancia de la IA como una herramienta para gestionar tareas y asistir en la redacción de decisiones judiciales, pero subrayó que los jueces no deben depender excesivamente de los sistemas de IA, ya que esto podría comprometer el derecho al debido proceso, la independencia e integridad del Poder Judicial. El caso se originó en una tutela en la cual el juez de segunda instancia utilizó ChatGPT para complementar su decisión, lo que generó preocupación sobre la posible vulneración del debido proceso. No obstante, la Corte concluyó que, aunque la herramienta fue utilizada, la decisión final no dependió exclusivamente de ella, y el

juez mantuvo la responsabilidad en la decisión. De este modo, el fallo resaltó la necesidad de regular el uso de IA en el ámbito judicial para asegurar la transparencia, responsabilidad, protección de la privacidad y evitar que la IA reemplace el juicio humano.

Adicionalmente, la Corte instruyó al Consejo Superior de la Judicatura a diseñar una guía para el uso de estas tecnologías en la rama judicial, que contenga pautas integrales que aseguren un uso responsable y ético de la IA, y el respeto por los derechos humanos.

En cuanto a los principios orientados al desarrollo de la IA en Colombia, es necesario analizar aquellos que podrían incidir en la profundización de desigualdades sociales y disparidades. Para abordar estos desafíos, se deben implementar principios que logren equilibrar la protección de los derechos con la promoción de la innovación y la confianza en los sistemas de IA.

En ese sentido, conforme al CONPES 3975 de 2019, es crucial fomentar la creación de un mercado sólido de IA en Colombia, priorizando innovaciones que impulsen el surgimiento de nuevos sectores económicos. Además, resulta indispensable que las políticas regulatorias se basen en evidencia empírica y en métricas de impacto, lo que permitirá una regulación más eficaz y adaptativa. Al mismo tiempo, se debe concebir el mercado de IA como una herramienta para promover la equidad y la inclusión social, asegurando que su desarrollo contribuya al cierre de brechas socioeconómicas.

Es imperativo establecer un marco ético robusto que acompañe la evolución de la IA, dado que su uso plantea retos significativos en torno a principios fundamentales como la justicia, la libertad, la no discriminación, la transparencia, el diseño responsable, la seguridad, la privacidad y la protección de los derechos humanos. La regulación de la IA, por tanto, debe incorporar una dimensión ética transversal que abarque todas las fases de su desarrollo, implementación y monitoreo, garantizando que las tecnologías emergentes operen bajo criterios de responsabilidad social y respeto por los valores democráticos, sin que esto implique de ninguna forma una limitación a su desarrollo.

IV - COMPARACIÓN ENTRE LOS ESTÁNDARES EUROPEOS Y LA PROPUESTA COLOMBIANA

El principio de transparencia es fundamental para garantizar que el desarrollo, despliegue y uso de sistemas de IA sean confiables y éticos. Este principio exige que los procesos, decisiones y operaciones de los sistemas de IA sean comprensibles y accesibles tanto para sus desarrolladores como para los usuarios y las autoridades reguladoras. La transparencia no solo implica la posibilidad de rastrear y explicar

cómo una IA llega a una decisión, sino también de evaluar si estas decisiones son justas y no discriminatorias.

La transparencia también implica la creación de políticas claras y accesibles para los usuarios, educar sobre el funcionamiento y limitaciones de la IA, y garantizar que existan mecanismos de responsabilidad y supervisión. La combinación de estos métodos permite que tanto los expertos en tecnología y la sociedad en general puedan confiar en que los sistemas de IA operan de manera ética, segura y conforme a los estándares legales y de derechos humanos (Comisión Europea, 2018).

Respecto al marco legal vigente relevante para la regulación de IA en el país, la Constitución Política de 1991, en su artículo 15, proporciona una base sólida para la protección de los datos personales, garantizando derechos fundamentales como la privacidad, el buen nombre y el derecho a la rectificación de información. El derecho al *habeas data* está intrínsecamente ligado a la protección de la intimidad personal, y es una herramienta clave para asegurar que los datos personales no sean utilizados de manera indebida. Este derecho se ha convertido en un pilar esencial en el contexto de la IA, debido al creciente uso de tecnologías avanzadas para la recolección y análisis de datos que demanda una protección robusta y efectiva de la información personal.

El desarrollo y despliegue de sistemas de IA deben alinearse con los principios constitucionales, garantizando que el uso de datos respete los derechos fundamentales consagrados en la Constitución, especialmente en lo relacionado con la privacidad y los datos personales.

Sobre esta base constitucional, se erigió la Ley 1712 de 2014 encargada de regular el derecho de acceso a la información pública, promoviendo la transparencia y la rendición de cuentas en el uso de tecnologías de IA en el sector público. Entre los proyectos de ley analizados, cabe destacar el PL 200 de 2023, el cual busca establecer un marco normativo robusto para regular el desarrollo y la implementación de la IA en Colombia. Este proyecto, además, se alinea con los principios y valores propuestos por organismos internacionales como la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), que en su reglamentación sugiere que todo desarrollo tecnológico, especialmente la IA, debe tener un enfoque centrado en los derechos humanos, la seguridad y la protección de las personas y sus datos.

La experiencia internacional ha demostrado que los sistemas de IA pueden llevar a prácticas discriminatorias, injustas y vulneradoras de derechos humanos, por lo cual, los límites éticos son esenciales para permitir un uso responsable de esta tecnología en el país armonizando la innovación y su incentivo. La posibilidad de acceder al código fuente y a la información técnica de estos sistemas permite identificar posibles sesgos, errores o vulnerabilidades, y evitaría decisiones arbitrarias deriva-

das de la "caja negra" que caracteriza a muchos algoritmos actuales (Corvalán, 2017).

Los beneficios de incluir el principio de transparencia en la regulación de IA en Colombia se reflejan principalmente en los sistemas de IA de alto riesgo, debido a que la implementación del principio de transparencia permitirá que los responsables del despliegue interpreten y usen correctamente sus resultados de salida. Con ello se buscaría garantizar que los sistemas de IA estén acompañados de las instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado, las cuales deben incluir información concisa, completa, correcta, pertinente, accesible y comprensible para los responsables del despliegue y, en especial, para los usuarios.

Por lo tanto, incluir el principio de transparencia en la regulación de IA en Colombia es crucial para garantizar la protección de los derechos fundamentales y aumentar la confianza en los sistemas de decisión automatizada. Al establecer la transparencia como un estándar clave, se asegura el acceso a los datos de entrenamiento, validación y pruebas, junto con la documentación técnica que respalda estos sistemas. Esto es esencial para permitir la rendición de cuentas de las entidades responsables reforzando la seguridad y confiabilidad en la IA.

La transparencia facilita un uso ético y equitativo de la IA, al permitir que los expertos independientes y la sociedad evalúen su funcionamiento, lo que es clave para generar la confianza necesaria en su adopción. Además de garantizar el acceso a la información pública, se debe equilibrar la protección de la propiedad intelectual y el secreto industrial, para construir un marco regulatorio que sea ampliamente aceptado por la sociedad y que garantice la justicia y la equidad en la toma de decisiones automatizadas, fomentando tanto la confianza como la innovación.

V - CONCLUSIONES

La Cuarta Revolución Industrial ha transformado de manera significativa diversos sectores económicos a través de la implementación de sistemas de IA. Estos avances han optimizado procesos y mejorado la toma de decisiones, pero al mismo tiempo han generado desafíos importantes, especialmente en la protección de los derechos fundamentales. En este contexto, la regulación de la IA se ha vuelto crucial.

El enfoque regulatorio de la UE se destaca por su base ética y humanista, proponiendo un marco que garantiza un entorno seguro, promueve la innovación y protege los derechos fundamentales. Estos principios buscan equilibrar el avance tecnológico con la rendición de cuentas y la mitigación de riesgos, subrayando la importancia del principio de transparencia como un factor clave en la regulación efectiva de la IA.

En efecto, el principio de transparencia, con sus dimensiones de trazabilidad, explicabilidad y comunicación, es esencial para garantizar la confianza en los sistemas

de IA. La regulación adecuada debe asegurar que los actores involucrados comprendan los beneficios y los riesgos asociados al uso de esta tecnología. En este sentido, la transparencia no solo fortalece la confianza en la IA, sino que también es indispensable para la gestión ética de sus riesgos.

En Colombia, la adopción de un marco regulatorio centrado en la transparencia es crucial para asegurar un uso responsable de la IA. La base constitucional existente, junto con la voluntad política adecuada, puede facilitar la creación de una regulación flexible que proteja los derechos fundamentales. Aunque los proyectos legislativos están en etapas tempranas, la Corte Constitucional ha dado pasos importantes hacia la regulación ética de la IA, marcando un camino prometedor para el futuro del país en este ámbito.

Finalmente, es posible plantear tres recomendaciones para una inclusión efectiva del principio de transparencia en el proyecto de regulación de IA en Colombia. La primera recomendación versa sobre la interdisciplinariedad; la segunda se refiere a la participación efectiva, y, por último, la tercera alude a los espacios de pedagogía y formación.

Una de las estrategias usadas en los procesos normativos de la UE tratados en este texto es la interdisciplinariedad. Varios son los ejemplos donde la reunión de un grupo de expertos desde diferentes áreas amplía la perspectiva sobre la que se parte para iniciar un proyecto regulatorio. Tal como el Grupo de Expertos de Alto Nivel conformado por la Comisión Europea o el Grupo Interdisciplinario que participó en la elaboración de la Carta de Derechos Digitales Española. La interdisciplinariedad en el marco regulatorio colombiano es esencial, la composición plural y equilibrada de un grupo de expertos permite que el trabajo no sea estático, sino que los puntos de vista sustantivos nutran el proceso normativo.

Tanto la perspectiva jurídica como la técnica pueden converger en un trabajo humanista aplicado a un sector netamente tecnológico. Los consensos y disensos que surjan podrían fortalecer la formulación del marco regulatorio y propender a que el abordaje de los beneficios, riesgos y desafíos sea más exhaustivo. Desde el inicio de las discusiones, la información y técnica aplicadas deben ser transparentes, dado el impacto que tendrá una vez sea finalizado el proceso de desarrollo normativo.

Segundo, la interdisciplinariedad debe estar combinada con espacios efectivos de participación. Sobre la participación efectiva, López (2022) expone herramientas para el diseño y análisis de regulaciones. Una estrategia mencionada es el *sandbox* regulatorio, el cual permite una experimentación en ambientes controlados para la prueba de tecnologías que actualmente no se encuentran subsumidas en las reglas. Esto podría resultar insuficiente en el caso colombiano. Sin embargo, elementos de este mecanismo podrían extrapolarse a espacios efectivos de participación más amplios sostenidos por el Estado. Estos elementos son el diálogo continuo y efecti-

vo entre el regulador y los regulados, la amplia información que se obtiene sobre las necesidades de la regulación y el intercambio de conocimientos.

El proceso regulatorio debe cumplir requisitos formales y materiales para tener éxito. El estricto cumplimiento del proceso legislativo contemplado en la Constitución es una responsabilidad que recae en el legislador. Debe ser un proceso justo, accesible y abierto, que se debe combinar con la interdisciplinariedad antes mencionada, asegurando que todas las partes interesadas puedan participar. La participación de expertos en el tema no debe limitarse a aspectos técnicos, científicos y económicos, sino que también se extienda al campo de los derechos humanos. Al final, la evaluación del espacio de participación efectiva versará sobre los costos y beneficios inmersos en el proceso regulatorio, así como la combinación de diferentes estrategias regulatorias basadas en la diversidad de actores que participaron en el espacio (López, 2022).

Por último, la tercera recomendación sobre pedagogía y formación es transversal. La orden de la Corte Constitucional colombiana al Consejo Superior de la Judicatura, en la sentencia T-323 de 2024 sobre la divulgación de una guía, manual o lineamiento sobre el uso de la IA en la toma de decisiones judiciales es un ejemplo de la importancia de la pedagogía y la formación en la implementación de estos sistemas. El uso que se le dé a estas tecnologías determinará en gran medida los beneficios o riesgos que puedan presentarse. Espacios de formación y pedagogía sobre la IA tanto públicos como privados serán provechosos no solo para materializar el principio de transparencia en su arista de comunicabilidad y explicabilidad, sino también para enriquecer y fortalecer la interrelación con esta tecnología que ha llegado para quedarse.

Estas recomendaciones resaltan la necesidad de situar la transparencia como el eje fundamental en la regulación de la IA. La IA, en sí misma, no debe considerarse como inherentemente buena o mala. Su impacto depende del modo en que se gestione y de las decisiones humanas que guíen su funcionamiento. La IA es parte de la vida cotidiana, y se ha vuelto transversal a todos los sectores de la sociedad. Su potencial para generar beneficios es inmenso, siempre que los riesgos asociados y la protección de los derechos fundamentales sean tratados con la seriedad que merecen. El desafío, por tanto, es asegurar un uso responsable, transparente y ético de la IA, que promueva el bienestar común y la confianza en el futuro tecnológico.

REFERENCIAS

Araya Paz, C. (2021). Transparencia algorítmica: ¿un problema normativo o tecnológico?, CUHSO, 31(2), pp. 306-334.

Bermúdez, C. I. M. (2001). Paradigmas de la investigación sobre lo cuantitativo y lo

cualitativo. *Ciencia e Ingeniería Neogranadina*, 10, pp. 79-84.

Carvajal, E. T. (2021). Derechos humanos, ética y transparencia algorítmica. *Ius Et Scientia*, 7(1), pp. 370-386.

Comisión Europea (2018). Directrices éticas para una IA fiable. https://www.algoritmolegal.com/wp-content/uploads/2021/06/Informe-G-Expertos-IA-fiable-junio-2018.pdf (Acceso: 16 de septiembre de 2024).

Comisión Europea (2020). Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52020DC0065 (Acceso: 16 de septiembre de 2024).

Congreso de la República de Colombia. Ley 1712 de 2014 http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html (Acceso: 20 de septiembre de 2024).

Congreso de la República de Colombia. Ley 1266 de 2008. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488

Congreso de la República de Colombia. Ley 1581 de 2012. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Constitución Política de Colombia [C.P.] (1991) Artículos 15 y 71 [Título II].

Corvalán, J. G. (2017). La primera inteligencia artificial predictiva al servicio de la Justicia: Prometea. La Ley.

Courtis, C. (2006). El juego de los juristas. Ensayo de caracterización de la investigación dogmática., En *Observar la ley: ensayos sobre metodología de la investigación jurídica*, pp. 105-156.

Covarrubias, L., Zadamig, J., Mendoza Enríquez, O. A. y Graff Guerrero, M. (2022). Enfoques regulatorios para la Inteligencia Artificial (IA)'. *Revista Chilena de Derecho*, 49(3), pp. 31-62.

Departamento Nacional de Planeación (2019). CONPES 3975 de 2019. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf.

Fanni, S. (2020). La inteligencia artificial y el cuerpo humano digital: a la búsqueda del habeas data'. *Ius Et Scientia*, 6(2), pp. 200-224.

López Murcia, J. D. (2022). *Inteligencia regulatoria: Algunas herramientas para diseñar y analizar regulación*. Editorial Legis & Universidad de la Sabana.

Human Rights Watch (2018). The Toronto Declaration: Protecting the Rights to Equality and Non-discrimination in Machine Learning Systems.

Martínez Espin, P. (2023). La propuesta de marco regulador de los sistemas de Inteligencia Artificial en el mercado de la UE. *Revista CESCO de Derecho de Consumo*, (46), pp. 1–20.

Monasterio Astobiza (2017). Ética algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por algoritmos. *Dilemata*, 9(24).

Morales Oñate, D. A. (2021). Implicaciones jurídicas del algoritmo: derechos intelectuales y privacidad. *Foro: Revista de Derecho*, (36), pp. 111–130.

Parlamento Europeo y Consejo Europeo, Reglamento (UE) 2024/1689, por el que se establecen normas armonizadas en materia de inteligencia artificial.

Parlamento Europeo (2021) Reglamento (UE) 2021/694 por el que se establece el Programa Europa Digital.

Pegoraro, L. y Rinella, A. (2006). *Introducción al derecho público comparado*, pp. 47–146.

Proyecto de Ley Estatutaria 200 de 2023: Por medio de la cual se define y regula la inteligencia artificial, se establecen límites frente a su desarrollo, uso e implementación y se dictan otras disposiciones. Gaceta Nro. 1260/23.

Ruiz, F. J. B. (2022). La paradoja de la transparencia en la IA: Opacidad y explicabilidad. Atribución de responsabilidad. *Revista Internacional de Pensamiento Político*, 17, pp. 261–272.

Schwab, K. (2016). *La cuarta revolución industrial*. Debate.

Tesoro, S. F. y Ruano, P. M. (2021). Derechos digitales: de la Constitución Española a la Carta de Derechos Digitales. *Temas para el debate*, (323), pp. 25–27.

Torres, F. E. R. (2011). La relevancia del paradigma cualitativo en las ciencias sociales: un análisis histórico descriptivo. *Fermentum. Revista Venezolana de Sociología y Antropología*, 21(61), pp.289-319.

Vestri, G. (2021). La inteligencia artificial ante el desafío de la transparencia algorítmica: Una aproximación desde la perspectiva jurídico-administrativa. *Revista aragonesa de Administración pública*, (56), pp. 368-398.

ISSN 3008-9484 **Diálogos y Voces Judiciales** | Vol. 2, Nº 2 (diciembre de 2024): 100-105

EL LADO LUMINOSO DE LA INTELIGENCIA ARTIFICIAL

Entrevista a Mario Adaro[*]

DVJ: Mario, muchísimas gracias por estar con nosotros. Se está hablando mucho de Inteligencia Artificial (IA), sobre todo, este último tiempo. Queríamos saber, en tus palabras, qué se puede considerar IA y cuál considerás que es el impacto que ha tenido en términos históricos y cuál está teniendo.

MA: Inteligencia artificial, así como se conoce técnicamente, es un concepto de los setenta que ha ido teniendo distintos tipos de desarrollo, pero sin duda en los últimos cinco años ha hecho una evolución y una escalabilidad enorme, exponencial. Es una de las tecnologías que, entiendo yo, está modelando la humanidad y la sociedad en miles de instancias. Hace cinco años, quizás tenía que ver más con el consumo, las redes sociales, pero ya hay un nivel de aplicación por el tipo de evolución y de técnica que se usa. Cuando uno habla de IA habla de distintos tipos de tecnología y de prácticas que engloban esta tecnología, pero básicamente es tratar de replicar, con la tecnología, la inteligencia humana en distintas dimensiones. Entonces, en ese sentido, tenés hace cinco años lo que era, por ejemplo, *Machine Learning*. Ahora, el gran boom de la IA generativa, lo que todo el mundo conoce como Chat-GPT (pero hay otras plataformas como Gemini o Copilot que también tienen una buena interfaz de usuario). Es decir, cualquier persona puede hacer uso o iterar con la IA para distintas cuestiones. En mi opinión, esencialmente estamos hablando de lo que es o va a ser considerado como el invento más importante de nuestro tiempo. Va a ir, como te decía, modelando y generando un impacto muy alto en todas las dimensiones, no sólo tecnológica, sino también en salud, en educación, en lo social, en democracia… Hay un gran debate, por ejemplo, sobre el impacto de los *Deepfake* o de la construcción de imágenes o del discurso del odio, de discriminación, en una palabra: toda una dimensión de debate que creo que se tiene que dar, del ser humano, del ser social en el mundo digital, iterando con la IA. Eso en primer lugar, y claramente necesitamos un espacio de reflexión, de debate, de abordaje ético-filosófico, de qué queremos con esto que al principio uno le entendía como herramienta. Pero que es-

* Vicepresidente Primero de la Suprema Corte de Justicia de Mendoza y director de JusLab. Esta entrevista fue grabada el 15 de agosto de 2024, en San Salvador de Jujuy. Disponible en: https://www.youtube.com/watch?v=3C_UWSJJm5A

tá dejando de ser herramienta para ser algo más que una herramienta. Entonces ahí está el debate.

DVJ: Todas estas experiencias, y sobre todo este boom que mencionás de cinco años a esta parte, les están planteando desafíos a los gobiernos. En base a la experiencia de Estados Unidos y Europa fundamentalmente, por cuál postura te inclinás, ¿una más regulatoria o bien una menos regulatoria?

MA: Sí, a ver, Europa siempre fue como el faro regulatorio del derecho. Muchas veces en Latinoamérica hemos seguido ese esquema del derecho continental. En primer lugar, hace cinco años, tuvo que ver más con protección de datos personales. Todavía no estaba la intersección de la IA. Ya hoy, claramente, sí hay un abordaje filosófico, ético, regulatorio de la IA en Europa. En Estados Unidos, si bien en principio utiliza –como siempre ha utilizado– un modelo autorregulatorio del mercado, si se quiere, hoy están estas preocupaciones. No es casual que en los últimos tres años todos los líderes de las grandes compañías tecnológicas hayan pasado por el Senado de los Estados Unidos. Hay una preocupación. Es decir, esto que al principio era la autorregulación del mercado, a la dirigencia política pública de Estados Unidos ahora no le queda tan claro. Y después tenemos la otra dimensión que es, por ejemplo, Asia (fundamentalmente China), que uno no sabe qué está pasando ahí. O sea, si tienen un alto nivel de evolución tecnológica o no. Y cómo lo hacen. Pero, básicamente, las dos grandes instancias a tener en cuenta en la reflexión filosófica y ética es cuánto de regulación es deseable sin que se impida el crecimiento y el desarrollo tecnológico. En otras palabras, que pueda haber un desarrollo tecnológico y que la regulación no llegue al punto de impedirlo. Más allá de la IA, este ha sido el punto de discusión en relación con cualquier tipo de tecnología. La regulación no debe impedir que la humanidad evolucione. De la imprenta en adelante está la discusión si prohibimos o no prohibimos: tipo de herramientas, uso y tecnología. En este caso, la amplificación que esta herramienta da, requiere un nivel de debate de parte de la dirigencia pública, pero no sólo política, sino social, empresarial, académica, en general. Yo me imagino un modelo, más que de regulación, de gobernabilidad cooperativa entre los países. Sobre todo en Sudamérica se tiene que dar un debate propio, porque este impacto genera amplificación de vulnerabilidades propias de la región: brechas digitales, económicas, sociales, pobreza. Hay que ver cómo se abordan estas cuestiones. Me imagino un espacio más de colaboración o cooperación, y después cada país entendiendo su propia regulación. También comprendiendo que esa regulación a veces no tiene un alto impacto. Al ser intangible, el abordaje es complejo. También creo que hay una herramienta muy interesante que se conoce como *sandbox*. Un sandbox, que no está en nuestro modelo cultural jurídico, es experimentar en forma controlada, ética, una herramienta. Por ejemplo, ya en un sector

determinado uno lo experimenta, ve costos-beneficios-riesgo. Y a partir de ahí, de ese pequeño proyecto piloto, controlado, regula en lo general. Esa me parece que podría ser una herramienta interesante para algún tipo de área, por ejemplo, salud o educación, probablemente también justicia. Pero sí, claramente, previo a la regulación se requiere un debate ético, filosófico, para que eso después se plasme en una norma.

DVJ: Hablando ya puntualmente de la Justicia, ¿cómo te parece que la IA podría transformar al sistema judicial en términos de eficiencia, de acceso a la justicia y de equidad?

MA: Es una gran herramienta y una gran oportunidad para organizaciones como la nuestra. Hemos tenido un debate muy interesante en Jujuy desde la innovación. Es decir: desde la posibilidad de empezar a cambiar las cosas para mejorar el servicio de justicia, y una de las grandes exigencias que tiene la ciudadanía con la Justicia, por un lado, es la eficiencia, es decir los tiempos de Justicia, la lentitud de la justicia. Y por otro, aunque no esté en agenda, es la transparencia, la rendición de cuentas que nos debemos los poderes judiciales como servicio de vocación pública. Rendir cuentas de lo que hacemos. En ambos casos, la IA tiene mucho por decir, para mejorar los procesos, sobre todo, para mejorar los tiempos de los procesos, y también para ser más transparentes. Yo creo que tenemos una gran oportunidad, que tenemos un capital humano muy formado en los poderes judiciales de las provincias y que hemos armado una comunidad. Hoy estamos armando un plan de IA, de experimentación o de uso de la IA en actividades jurisdiccionales y procesales. Y creo que eso nos va a ir permitiendo construir equipos para usar esa herramienta, que tiene un alto potencial en aras de la mejora del servicio de justicia.

DVJ: Puntualmente, ¿nos podrías decir qué acciones se están llevando a cabo al respecto a nivel provincial?

MA: En el ámbito de las provincias tenemos experiencias, por ejemplo, en tribunales de ejecución fiscal, que son procesos de alta demanda, de alta carga de trabajo y muy seriados y repetitivos. Por ejemplo, todo lo que es cobro impuestos y tasas en Córdoba. Se está haciendo algo similar en Mendoza y Río Negro también. Después nosotros tenemos el primer antecedente en Justicia, que lo hizo el IALAB de la UBA, que es Prometea. Prometea era un modelo de asistente de automatización documental. Para que se entienda, frente a una posibilidad de un acto procesal, automatizar y dar una opción al operador jurídico de un documento que tuviera que ver con esa decisión. Se están haciendo experiencias así en distintos ámbitos. En Mendoza tenemos Concilia, que es un modo de aplicación de IA para homologar convenios laborales. Dentro del fuero laboral, consiste en automatizar el texto del documento, la

firma ciudadana, y posteriormente se hace un matcheo entre el documento y la homologación jurisdiccional. Creo que hay pequeñas herramientas de uso. Creo que se pueden automatizar también algunas cuestiones procesales, algunas cuestiones también que hoy llevan tiempo y carga de capital humano, que las pueden hacer la herramienta. Siempre, obviamente, con el control humano final.

DVJ: Siguiendo con esa línea, ¿cómo podría la IA mejorar el acceso a la justicia para poblaciones desfavorecidas o con menos recursos?

MA: Bueno, ahí primero hay que tener un debate. Como dijimos inicialmente, Latinoamérica, y Argentina en ese contexto, tiene que darse un debate sobre las brechas: las brechas sociales, las brechas económicas, que tienen un impacto también en la brecha tecnológica (brecha de conectividad y también de alfabetización tecnológica). Todo eso es una dimensión amplísima. De todas maneras, entiendo que todo este desarrollo va a venir de manera cada vez más accesible. Y va a permitir, por lo menos, detectar esas vulnerabilidades. Si hay un Poder Judicial, con equipos que entiendan estas brechas, se debe procurar no amplificar esas vulnerabilidades. Todo lo contrario: utilizaríamos la herramienta, su lado luminoso digamos, en términos de *Star Wars*, para poder atender vulnerabilidades. Por ejemplo, detección automática de dificultades de acceso a la justicia, y así poder hacer conexión directa con la ciudadanía, la que está requiriendo otros caminos, un tipo de servicio de justicia ejemplar. Atender demandas o denuncias que no han sido atendidas. Priorización o detección de emergencias. Porque a veces uno entra en una misma mesa de entrada y no hay distinción, no hay clasificación. Hay que priorizar. Más allá que pueda haber medidas urgentes, cautelares, etcétera. Pero poder detectar en el texto y en el requerimiento ciudadano, detectar esas urgencias, es algo que creo que la IA lo puede hacer muy bien. Que pueda tener una buena performance y darnos la posibilidad de clasificar: qué cosas hay que priorizar sobre otras. Porque, claramente, tenemos un tiempo, un problema de capital humano, de cantidad y cantidad de reclamos. Entonces priorizar podría ayudar mucho para mejorar este aspecto relativo a las vulnerabilidades.

DVJ: ¿Qué lugar te parece que habría que otorgarle a la alfabetización o capacitación de los operadores jurídicos para la adquisición o mejora de habilidades relacionadas con el uso de la IA y las tecnologías emergentes en general?

MA: Esto es central. No solamente con la IA. Vivimos en un contexto, como se dice, de innovación VUCA o BANI, esto es, un contexto volátil, incierto, complejo y ambiguo. Este contexto cambia permanentemente. Los liderazgos cambian permanentemente, y la única posibilidad de reacción al cambio constante es la capacitación permanente. En todo tipo de dimensiones. Claramente, ahora hay una necesidad de

formación que hace cinco años no había, y tiene que ver con otro tipo de habilidades, me refiero a las habilidades blandas (empatía, liderazgo, emociones) y también mucho contenido de comprensión de la herramienta. Si uno no comprende la herramienta que va a usar probablemente el riesgo del uso de esa herramienta sea altísimo. Y no es sólo con la IA. Si yo no sé, para poner un ejemplo clásico, si no sé usar una amoladora, es probable que los riesgos del uso de esa herramienta sean mucho más altos que si me capacito en un curso de, digamos, albañilería o lo que fuera. Creo que cada vez más la capacitación va a ocupar un eje central para un adecuado uso de las nuevas herramientas en nuestras organizaciones, me refiero fundamentalmente a las organizaciones judiciales.

DVJ: En este nuevo contexto, en esta realidad emergente, ¿qué perfil o qué herramientas considerás que debe tener un juez que aspira a concursar un cargo dentro de la Justicia?

MA: Hay muchas dimensiones. Claramente, el conocimiento jurídico. Pero ya no es un conocimiento jurídico como hemos venido evaluando hasta ahora, haciendo esos exámenes de ingreso que son de acumulación de contenido académico, enciclopedista. Va a tener que ver con conocer el contenido jurídico, pero para otro tipo de cuestiones: argumentación, sentido común, empatía, habilidades blandas de liderazgo (porque hay que liderar equipos), con un liderazgo distinto, que ya no es jerárquico. Es un liderazgo que empieza a ser más democrático u horizontal. Comprender que ahora los equipos tienen composición de distintas generaciones (*baby boomers*, *centennials*, *millennials*) con distintos intereses. Entonces la complejidad del mundo actual requiere respuestas de parte de liderazgos complejos con habilidades distintas.

DVJ: Hace un rato mencionaste o aludiste brevemente a la experiencia de Mendoza. ¿Nos podrías comentar un poco cómo se ha incorporado el uso de la IA en la justicia mendocina? También comentar un poco en qué consiste Concilia.

MA: Concilia, básicamente, es una experiencia que hemos hecho dentro del fuero laboral, y dentro del fuero laboral, sólo en la primera circunscripción, que sería el Gran Mendoza. Para arrancar desde el problema, notábamos un gran cuello de botella al momento en que las partes se ponían de acuerdo en cualquier momento (porque los abogados se conocían y podían, a lo mejor, generar acuerdos extrajudicialmente). Para poder homologar ese acuerdo había que hacer concurrencia presencial: pedir turno, redactar el documento, hacer ir a las partes, y eso tenía todo, por decirlo así, un *workflow* procesal de tiempos. Entendíamos que, si podíamos diseñar una herramienta que fuera más ágil, que fuera remota, que generara el documento, y que ese documento pudiera dar la posibilidad de firma digital a las partes

(tanto a los abogados y las abogadas como a los ciudadanos) –y eso, mientras estaba ocurriendo el proceso de firma, nosotros nos quedábamos con el mismo dato e íbamos haciendo el estudio de ese documento. Además, como este dato iba a tener una cuestión, para hacerlo más claro, como encriptada o "hasheada" (cuando digo "hasheada" no se entiende mucho), pero probablemente encriptar un documento, esto es, para que no puede ser modificado. Entonces, como estos procesos ocurren prácticamente de manera simultánea, adelantamos tiempos procesales, y después podíamos llegar a dar la respuesta de la homologación. Básicamente, de eso se trata: una "mini" respuesta a un "mini" problema que, cuando uno lo observa de manera agregada, es un problema grande.

DVJ: ¿Qué otras iniciativas tienen en carpeta para seguir avanzando con el uso de IA? ¿Creés que este modelo, que es incipiente en Mendoza, se puede replicar en otras jurisdicciones que cuenten, tal vez, con menos recursos?

MA: Sí. Nosotros aspiramos, con esto que estamos haciendo a nivel federal, a construir, por un lado, en el instituto de innovación, y por otro lado, la red de innovación JUSLAB, construir una comunidad de experiencia y de intercambio que lo que desarrollemos tenga un nivel, no sé si de *open source*, pero que pueda al menos ser compartido y escalado en la propia provincia para otra instancia o en otras provincias. Eso desde ya: la colaboración de la herramienta. Porque si nosotros no hacemos innovación, nadie va a venir a hacer innovación en los poderes judiciales. Creo que eso es fundamental. Lo que viene es armar equipos a nivel nacional para entrenar redes neuronales de LLM, que sería lo que da la base técnica de las redes neuronales, en español y en texto jurídico, para determinadas actividades: una puede ser anonimización, otra puede ser automatización de documentos, otra puede ser la búsqueda semántica de sentencias, y otra, la búsqueda inteligente de documentos dentro del proceso. Hay un montón de dimensiones. Por ejemplo, otra dimensión es todo el tema de gobernanza de datos. Me parece que esto es esencial. Porque cuando uno hace esto, uno quiere directamente aplicar IA y no tiene gobernados los datos. Nosotros estamos construyendo un *Data Lake*, sobre eso estamos haciendo como un *dashware* o un tablero de control para poder medir el desempeño de la justicia. Lo podemos medir magistrado por magistrado, juez por juez, expediente por expediente; y, sobre eso, podemos correr cuestiones de analítica de datos de IA, o podemos hacer automatización de IA. Creo que por ahí, entiendo yo, es el camino. Después hay otra dimensión que no es de IA, pero está dentro de la agenda, que es este salto de transformación digital, el cual requiere una política de ciberseguridad, una política de protección de datos, etcétera. Digamos para no entrar en otros temas, pero básicamente por ahí me parece que es la agenda de lo que se viene, en los próximos años, en los poderes judiciales.