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.