

**La responsabilidad por daños causados por el uso de IA:****¿responsabilidad objetiva, subjetiva o híbrida?****Liability for damages caused by the use of AI: objective, subjective, or hybrid liability?***Maria Paula Díaz \** y *Cristian Mitrani †***Resumen**

La irrupción de la inteligencia artificial en la vida cotidiana y profesional ha generado desafíos inéditos para el derecho, especialmente en materia de atribución de responsabilidad por daños. La autonomía y capacidad de aprendizaje de los sistemas de IA dificultan la aplicación de los regímenes tradicionales de responsabilidad objetiva y subjetiva, ya que la identificación del sujeto responsable y la reconstrucción de la cadena causal se ven dificultadas por la intervención de múltiples actores y la imprevisibilidad de los resultados. En este contexto, la

---

\* María Paula Díaz es abogada por la Facultad de Derecho de la Universidad de Buenos Aires (2005), con Diploma de Honor. Es actualmente Directora Legal en Tenaris S.A. y hasta noviembre de 2025, se desempeñó como socia del Estudio Mitrani Caballero. Se especializa en asuntos corporativos, cumplimiento normativo y gestión de crisis, protección de datos personales y privacidad, ciberseguridad e innovación.

† Cristian Mitrani es abogado por la Facultad de derecho de la Universidad de Buenos Aires (1978). Es socio fundador del Estudio Mitrani Caballero y responsable de las prácticas de derecho comercial, fusiones y adquisiciones, cumplimiento normativo y gestión de crisis, defensa de la competencia, derecho comercial, derecho público y regulación económica, litigios, arbitraje y resolución de disputas de Mitrani Caballero. Fue socio visitante en Bonelli Erede Pappalardo, Milán (2004-2005) y abogado senior del departamento legal del Grupo Techint (1984-2000). Ejerció como prosecutario letrado y secretario letrado de la Presidencia de la Corte Suprema de Justicia de la Nación (1980-1984) y de la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal (1978-1980). Ha sido condecorado por el Presidente de la República de Italia como Commendatore dell'Ordine della Stella d'Italia (22 de abril de 2008) y como Grande Ufficiale dell'Ordine della Stella d'Italia (14 de julio de 2015). Ha sido recomendado en forma continua como uno de los "Líderes en su Especialidad" (Corporate/M&A-Argentina) para The World's Leading Lawyers for Business publicada por Chambers & Partners anualmente y ha sido seleccionado como Star Individual (Corporate/M&A-Argentina) por Chambers Latin America. Asimismo, ha sido distinguido por Best Lawyers con el premio Lawyer of the Year 2013 (Argentina/Corporate M&A), ha recibido el Client Choice Award 2012 y 2015 por General Corporate Argentina, otorgado por la International Law Office (ILO) y ha sido distinguido individualmente por Latin Lawyer como Law Firm Leader of the Year 2012, por Argentina. Es miembro del Chartered Institute of Arbitrators, del International Centre for Dispute Resolution (AAA), de la International Bar Association (IBA) y de la American Bar Association (ABA). Recientemente, Latin Lawyer le otorgó uno de sus máximos reconocimientos como "Life Achievement Award", en razón de su destacada y amplia trayectoria.

distinción entre sistemas autónomos y supervisados, así como el grado de intervención humana, resultan determinantes para evaluar la imputación de responsabilidad. Un enfoque híbrido y flexible, que permita transitar con inteligencia aspectos del modelo de responsabilidad objetivo y subjetivos, parece propicio frente a los múltiples desafíos y peculiaridades de la IA.

**Palabras clave:** responsabilidad objetiva – responsabilidad subjetiva – Inteligencia Artificial – previsibilidad del daño – factor de atribución – exclusión de responsabilidad

### **Abstract**

The outbreak of artificial intelligence in everyday and professional life has created unprecedented challenges for law, particularly in terms of damage and liability. The autonomy and learning capacity of AI systems make it difficult to apply traditional regimes of strict and fault-based liability since the identification of the responsible subject and the reconstruction of the causal chain are hampered by the intervention of multiple agents and the unpredictability of the outcomes.

In this context, the distinction between autonomous and supervised AI systems, as well as the degree of human intervention, are decisive in assessing the attribution of responsibility. A hybrid and flexible approach, which allows for intelligent transition between aspects of the objective and subjective liability models, seems appropriate in view of the multiple challenges and peculiarities of AI.

**Keywords:** strict liability – fault-based liability – Artificial Intelligence – foreseeability of harm – attribution factor – exclusion of liability

## I. Introducción al régimen de responsabilidad derivado del desarrollo, comercialización y uso de los sistemas de Inteligencia Artificial

La irrupción de la inteligencia artificial generativa (“IA”)<sup>1</sup> afecta de manera singular la esfera profesional y está transformando profundamente los métodos de trabajo y los procesos de producción y comercialización de bienes y servicios. Tal es la magnitud del cambio, que no es posible aún determinar con precisión el alcance último de esta transformación.

A medida que los sistemas de IA adquieren mayor autonomía, resuelven problemas complejos con eficacia y aumentan su capacidad de procesar información y dar respuesta en los más diversos asuntos (intentando incluso imitar o sustituir en su quehacer a profesionales tan trascendentales como médicos, científicos y abogados), surgen interrogantes fundamentales sobre la atribución de responsabilidad legal. Tales interrogantes son especialmente desafiantes en los casos en los que el uso de estos sistemas cause daños a las personas o a los bienes, tras haber fallado la solución ofrecida o la decisión adoptada para alcanzar ciertos resultados.

El debate sobre si la responsabilidad proveniente de los daños derivados del uso de la IA debe regirse por un régimen objetivo, subjetivo o una combinación de ambos (que identificaremos como “híbrido” a lo largo de este trabajo), se ha convertido en un tema relevante para la doctrina jurídica. Existe una abrumadora cantidad de estudios, documentos oficiales de la Organización de Naciones Unidas y la Organización para la Cooperación y el Desarrollo Económicos,<sup>2</sup> antecedentes legislativos y legislación ya

<sup>1</sup> SAP Latinoamérica. ¿Qué es la IA generativa? Sitio Web Oficial <https://www.sap.com/latinamerica/products/artificial-intelligence/what-is-generative-ai.html>. (Vigente al 16/12/2025). “La IA tradicional hace referencia a sistemas de IA que pueden realizar tareas específicas siguiendo reglas o algoritmos predeterminados. Son principalmente sistemas basados en reglas que no pueden aprender de los datos ni mejorar con el tiempo. La IA generativa, por otro lado, puede aprender de los datos y generar nuevas instancias de datos”. En este trabajo referiremos “IA” para referirnos a la inteligencia artificial generativa.

<sup>2</sup> Recomendación del Consejo de la OCDE sobre Inteligencia Artificial (2019; enmendada en 2024): <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (Vigente al 16/12/2025). Observatorio de Políticas de IA de la OCDE (OECD.AI): <https://oecd.ai> (Vigente al 23/10/2025). OPSI – “Hello, World: Artificial Intelligence and its Use in the Public Sector” (2019): <https://www.oecd.org/gov/innovation/hello-world-ai-and-its-use-in-the-public-sector.htm> (Vigente al 16/12/2025). Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial (2021): <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics-of-ai> (Vigente al 23/10/2025).

vigente que tratan, no sin esfuerzo, de delinear un sistema de responsabilidad que resulte eficiente en el marco de un terreno aún poco explorado en los hechos. A esta dificultad, se le agrega la velocidad con la que los sistemas de IA mejoran, expanden sus capacidades y se aplican en las más variadas industrias, servicios, disciplinas y actividades.

La hipótesis que propiciamos señala que la atribución de responsabilidad por daños causados por sistemas de IA exige un modelo híbrido y contextual. En efecto, entendemos preferible un sistema que combine elementos de responsabilidad objetiva y subjetiva, definidos según el grado de autonomía del sistema, la intervención y control humano efectivos, la previsibilidad del daño, la opacidad algorítmica y el marco regulatorio y contractual aplicable.

Este artículo intenta explorar el problema de la responsabilidad derivada del uso de la IA, considerando los lineamientos del sistema tradicional del Código Civil y Comercial de la Nación Argentina (el “Código”). Pero, fundamentalmente, este trabajo formula preguntas que irán encontrando respuesta a medida que la litigiosidad llegue a la Justicia, teniendo empero en cuenta que los jueces suelen preferir soluciones singulares, escapando al *obiter dictum*.

## II. La responsabilidad por daños y los factores de atribución en los sistemas de IA

Antes de iniciar cualquier evaluación sobre los regímenes de responsabilidad, es necesario puntualizar las diferencias entre los sistemas de IA que llamaremos “autónomos” y “supervisados”. Los primeros operan casi en ausencia de intervención humana y los supervisados, por el contrario, demandan algún tipo de asistencia o supervisión del usuario<sup>3</sup>. El ejemplo al que recurriremos para simplificar la distinción es el de los vehículos autónomos frente a sistemas conocidos como LLMs (Large Language Models), de los cuales posiblemente el más conocido sea Chat GPT,<sup>4</sup> que requieren un

---

High-Level Advisory Body on AI (UN) – Governing AI for Humanity (Interim Report, 2023): <https://www.un.org/en/ai-advisory-body/interim-report> (Vigente al 16/12/2025)

<sup>3</sup> Ver las clasificaciones publicadas en Inesdi Business Techschool, Instituto Digital de la Profesiones S.L. de Barcelona <https://www.inesdi.com/blog/tipos-de-inteligencia-artificial/>. (Vigente al 16/12/2025). Si bien las clasificaciones varían según los autores y las “capacidades” o “limitaciones” del sistema que se esté evaluando en cada caso, a efectos de este trabajo, hemos considerado las categorías reflejadas por el citado Instituto.

<sup>4</sup> ChatGPT es una aplicación de chatbot de inteligencia artificial generativa desarrollada en el año 2022 por OpenAI accesible en [www.chatgpt.com](http://www.chatgpt.com).

pedido o solicitud dirigida para brindar respuestas. La integridad y calidad del “prompt” o la forma en la que se interroga la IA, determinará que el sistema sea capaz de satisfacer las expectativas de los usuarios o no. En los sistemas autónomos, por el contrario, el usuario no influye significativamente en la respuesta y reacción de la IA, más que en la elección del destino y, eventualmente, de una ruta u otra para llegar a destino y, a veces, ni siquiera en eso<sup>5</sup>. Si bien, en rigor, ningún sistema es absolutamente autónomo y hay otras categorías que pueden utilizarse en la clasificación, se propone esta simplificación a efectos de segmentar mejor los criterios de análisis y atribución de responsabilidad.

¿Será distinta la solución al momento de atribuir responsabilidad en uno y otro caso? Entendemos que sí.

La distinción entre sistemas autónomos y sistemas supervisados introduce desafíos para la atribución de responsabilidad, ya que la intervención humana puede variar desde una supervisión constante hasta una (casi) completa ausencia de control directo del usuario.

Asimismo, al momento de examinar el problema de la responsabilidad, será relevante la evaluación de las circunstancias del caso, el contexto y la forma en que se produce la interacción entre el usuario y el sistema. Del mismo modo, serán relevantes la finalidad de uso que tiene un sistema de IA determinado e incluso la capacidad y circunstancias personales del usuario. En ese sentido, no será lo mismo evaluar un caso cuando el usuario sea menor de edad, que cuando sea mayor e incluso, desde la perspectiva de la previsibilidad del daño, no será lo mismo atribuir responsabilidad cuando el desarrollador, fabricante o proveedor hayan podido prever daños, comunicando al usuario las advertencias con precisión y en forma eficaz, que cuando esa previsibilidad no haya sido considerada adecuadamente y, mucho menos, advertida al usuario.

Podemos concluir, entonces, que ni para los sistemas autónomos ni para los sistemas supervisados la respuesta puede ser unívoca y, por lo tanto, no podemos inclinarnos de forma excluyente por un régimen objetivo en defecto de uno subjetivo (o viceversa). Habrá una cantidad significativa de factores o variables que deberán considerarse en la búsqueda de la mejor solución del caso.

---

<sup>5</sup> Entendemos que existen grados de autonomía distintos, pero asumiremos en nuestra evaluación una autonomía casi completa, siempre en la intención de simplificar la categorización.

En los sistemas autónomos, la IA opera de manera independiente, tomando decisiones y ejecutando acciones prácticamente sin intervención del usuario que opera el sistema. Este grado de autonomía plantea interrogantes sobre la identificación del sujeto responsable en caso de daño, ya que la cadena de responsabilidad puede diluirse entre el programador, el desarrollador, el fabricante y quién comercializa y dispone el sistema en el mercado. La ausencia de un control humano dificulta la aplicación de los parámetros clásicos de culpa o negligencia, pues resulta complejo determinar si existió una conducta reprochable por parte de algún sujeto al que pueda hacerse responsable económicamente (en algún eslabón de la cadena o en el usuario).

Por otro lado, los sistemas supervisados requieren la intervención, la dirección o la vigilancia de un usuario durante su funcionamiento. En estos casos, el supervisor o usuario mantiene cierto grado de control sobre las acciones del sistema. Sin embargo, la supervisión o interacción puede ser limitada o meramente formal, lo que genera dudas sobre la eficacia real de la intervención humana para prevenir riesgos.

Recientemente, fue noticia la presentación de una demanda en los Estados Unidos que realizó la madre de un joven que había utilizado la IA en un juego de roles y a lo largo del tiempo se había enamorado del personaje que él mismo había creado.<sup>6</sup> El joven (de tan solo 14 años) se suicidó después de una última conversación con el personaje de IA. La tragedia del caso alerta sobre los peligros de la IA, pero en un escenario como este, corresponde preguntarse si verdaderamente un régimen de responsabilidad objetivo es el más apropiado o el que debe aplicarse con prescindencia de cualquier otra consideración.

¿Qué régimen debería aplicarse al caso? ¿Un régimen objetivo que sancione al desarrollador, proveedor, programador o fabricante por la teoría del riesgo creado, por ser responsables de disponer una “cosa riesgosa” en el mercado? ¿O ha de ser preferible un régimen subjetivo capaz de asignar (o no) culpa en función de un acto u omisión negligente? ¿Qué ponderación merecería en un caso así el vínculo inesperado que el usuario generó con el sistema de IA? ¿Pudiéramos verdaderamente afirmar que el programador o desarrollador pudo prever el daño? ¿Será posible afirmar que pudo prevenir la trágica consecuencia para el joven? ¿O el sólo hecho de colocar en el mercado

---

<sup>6</sup> New York Times. Artículo de Kevin Roose. *¿Se puede culpar a la IA del suicidio de un adolescente?* Publicado el 24 de octubre de 2024 <https://www.nytimes.com/es/2024/10/24/espanol/ciencia-y-tecnologia/ai-chatbot-suicidio.html> (Vigente al 16/12/2025).

o ámbito social un producto o tecnología cuyos alcances o consecuencias de la función de aprendizaje no se conocen, genera por sí mismo responsabilidad?

Mientras que en los sistemas supervisados pudiera exigirse al humano mayor de edad una conducta diligente para prevenir resultados lesivos, en los sistemas autónomos la capacidad de anticipar y evitar daños puede estar fuera del alcance del usuario. Esta limitación se presenta, aún, cuando el usuario actúa con prudencia y sigue las recomendaciones previstas por el propio desarrollador o comercializador.

Pudiera postularse que, a mayor intervención del usuario en la gestión, direccionamiento y alimentación del sistema de IA, menor la responsabilidad del fabricante, distribuidor y el desarrollador.

Finalmente, la famosa “opacidad” de los algoritmos a la que muchos autores se refieren y la complejidad técnica de los sistemas de IA hacen difícil establecer y entender la cadena causal determinante del daño<sup>7</sup>. En efecto, durante el entrenamiento, los sistemas de IA “ajustan” internamente sus conexiones de manera compleja y no lineal, lo que hace que, en ciertos casos, el razonamiento detrás de cada decisión o resultado sea prácticamente imposible de rastrear o explicar de forma sencilla.<sup>8</sup> Por ello, establecer y entender exactamente qué elementos ponderó el sistema de IA, cómo los combinó y cómo llega al razonamiento que le permite proponer un resultado, no siempre es posible. Habrá sistemas en los que esa determinación es sencilla y, entonces, es fácil entender dónde se produjo el error, qué está mal programado o qué es lo que sistema no entiende. Por el contrario, cuando los sistemas sean más “opacos”, será más difícil entender por qué se produjo el error y atribuir responsabilidad (al programador, al usuario, al fabricante, al desarrollador o a todos ellos).

Asimismo, y en tanto los sistemas de IA están en condiciones de “aprender” y, por lo tanto, las interacciones modifican y repotencian la información disponible dentro del sistema, tener un completo entendimiento sobre cómo opera, qué información elige y cuál descarta en cada caso o por qué usa una fuente de información y no otra, no siempre será sencillo. Sin ir más lejos, si dos *prompts* se formulan con leves diferencias, pueden arrojar

---

<sup>7</sup> María Celeste Colombo “Justificación del factor de atribución objetivo en la responsabilidad civil por daños causados por la Inteligencia Artificial”, publicado en el Sistema Argentino de Información Jurídico en octubre de 2024 (Id SAIJ: DACF240112).

<sup>8</sup> “El Problema de la Caja Negra en IA”. Publicado en el sitio Big Data. <https://www.bigdata.uma.es/el-problema-de-la-caja-negra-en-la-ia> (Vigente al 16/12/2025).

respuestas diversas e incluso ante un mismo *prompt*, formulado con diferencia de minutos respecto del que lo precedió, la respuesta puede variar. Ante esta situación, algunos autores proponen la implementación de mecanismos de trazabilidad y auditoría algorítmica como herramientas para facilitar la atribución de responsabilidad.<sup>9</sup> No obstante, pareciera que ninguna técnica, hasta el momento, ha eliminado completamente el problema de la opacidad ni asegurado una completa trazabilidad para el entendimiento pleno del razonamiento que realiza el sistema de IA en cada caso. Por lo demás, estamos muy lejos de que exista y se pueda adoptar algún mecanismo de aplicación universal para facilitar la atribución de responsabilidad.

Ante este escenario, podemos anticipar la idea de que cuanto mayor sea la opacidad –es decir, los aspectos del sistema que tengan capacidad de desarrollarse sin control ni conocimiento del proveedor, fabricante, programador, desarrollador o distribuidor– mayor la responsabilidad frente al usuario o a los terceros que sufran un daño. Cuanto más “incierto” o difícil sea prever cómo accionará el sistema, cuánto más “libre” o “ilimitado” sea el sistema a la hora de dar respuestas, mayor la responsabilidad de toda la cadena de valor que lo coloca en el mercado.

En suma, la atribución de responsabilidad en el uso de sistemas de IA, tanto en los sistemas autónomos como supervisados, exige un análisis flexible y contextualizado. Ello demanda considerar la diversidad de roles, los distintos niveles de intervención humana y las circunstancias particulares de cada caso.

Por todo lo dicho, no pareciera posible predeterminar la mayor eficacia de un régimen objetivo por sobre uno subjetivo en forma categórica, ya que la complejidad técnica, la opacidad de los algoritmos y la imprevisibilidad de las interacciones entre usuarios y sistemas de IA plantean desafíos inéditos. No obstante, y aún con esta dificultad, cabe la posibilidad de que la Justicia, en aras de proteger a los usuarios, se incline por formas de responsabilidad objetiva, que en esencia no sea muy distinta de la responsabilidad por riesgo creado.

---

<sup>9</sup>Eva María Mota Sánchez y Esther Herrera Expósito. “Auditoría Algorítmica En La Inteligencia Artificial En El Sector Público”. Universidad Nacional de La Plata, Argentina - ISSN: 1850-6242 - ISSN-e: 2618-5474.

### III. La responsabilidad contractual y extracontractual y la validez de las cláusulas de exclusión de responsabilidad en el marco del uso de sistemas de IA

La responsabilidad contractual y la responsabilidad extracontractual son dos figuras jurídicas que buscan reparar daños, pero se originan en situaciones distintas. En el marco del uso de un sistema de IA, si un vehículo autónomo falla causando un accidente, generará responsabilidad para el desarrollador, el fabricante, quién lo comercializó e incluso quién lo ofreció como responsable del servicio frente al pasajero/usuario que sufre un daño. Frente a este último, la imputación dependerá de las reglas previstas en el contrato y las limitaciones y exclusiones allí contempladas y frente a los terceros afectados por los estragos del accidente,<sup>10</sup> por la vía extracontractual.

En el terreno de la responsabilidad contractual, nos preguntamos acerca de la validez de las cláusulas de exclusión de responsabilidad y, en general, sobre si el conjunto de cláusulas predispuestas que los proveedores imponen a los usuarios al momento de suscribir el uso de sistemas de IA resulta válido, sobre todo en casos en los que, por las particularidades de los sistemas de IA, el usuario puede quedar desprotegido.

Las disposiciones contractuales mediante las cuales una parte busca limitar o eliminar su responsabilidad por ciertos daños que puedan derivarse del uso de un producto o servicio, son frecuentes y válidas en la mayoría de los ordenamientos jurídicos, aunque con fuertes limitaciones (generalmente impuestas por el orden público).

En el contexto de la inteligencia artificial (IA), estas cláusulas quedan potencialmente afectadas en cuanto a su validez debido a la variada capacidad negocial de las partes y dependiendo, además, de la sofisticación del usuario y de su capacidad de asumir y entender el riesgo.

Los regímenes son variados y así, en el derecho civil continental, las cláusulas no pueden excluir la responsabilidad por dolo o culpa grave, ni resultar abusivas para los consumidores.<sup>11</sup> En el ámbito de la IA, esto puede significar que un proveedor no podría

---

<sup>10</sup> “Falló el piloto automático: así fue el accidente por el que Tesla debió pagar US\$240 millones de indemnización”. Publicado en el Diario La Nación 06/08/2025. <https://www.lanacion.com.ar/estados-unidos/florida/fallo-el-piloto-automatico-asi-fue-el-accidente-por-el-que-tesla-debio-pagar-us240-millones-de-nid06082025/> (Vigente al 16/12/2025).

<sup>11</sup> Por ejemplo, no podría privárselos del derecho a ser informados debidamente sobre el servicio o producto que adquieren o negárseles el derecho a reclamar, cuando entiendan que han sido vulnerados sus derechos.

exonerarse de responsabilidad si el daño resulta de un defecto grave en el diseño del sistema o de una omisión intencionada en la información proporcionada al usuario. Misma situación con las reglas de protección al usuario y consumidor que sirven para asegurar cierto piso mínimo protección a los usuarios y consumidores, en un escenario en el que se presupone la mayor preparación, conocimiento y sofisticación del empresario o proveedor de bienes y servicios frente al público que los consume.

En el caso de la IA, la imposibilidad de prever enteramente los potenciales daños puede dificultar que el usuario comprenda plenamente los riesgos asumidos. Todo ellos podría llevar a que los jueces consideren inválidas ciertas exoneraciones por falta de transparencia o por ser contrarias al interés público.

Un aspecto crucial es la asimetría de información y poder entre las partes. Es posible suponer que desarrolladores, fabricantes y proveedores de IA tienen un conocimiento técnico muy superior al de los usuarios, y tal como ocurre con las reglas que aplican en defensa de los consumidores, la ley puede disponer ciertas previsiones para proteger al usuario consumidor en situaciones en las que presume que esa desigualdad en el conocimiento (o en la capacidad de negociar o en las condiciones de necesidad que afectan al usuario) pueden generar situaciones de desequilibrio contractual.

En estos casos, la validez de las cláusulas de exclusión puede ser cuestionada y en los casos de sistemas de IA, objetada si el usuario no estaba en condiciones de comprender el alcance de la exoneración, las advertencias de riesgo o las condiciones de operación y limitaciones del sistema. Los regímenes de protección al usuario y a los consumidores (en Argentina mayormente reflejados en el Título III, “Contratos de Consumo” y en la Ley 24.240 de defensa del consumidor) están justamente encaminados a fijar ciertas reglas en el afán de equilibrar relaciones que, en la mayoría de los casos, están afectadas por la desigualdad de fuerzas entre las partes contratantes. Entendemos que en el marco de la contratación de sistemas de IA estas herramientas son esenciales para entender y, en su caso, moderar el alcance y validez de las cláusulas contractuales predispuestas.

Junto con todas las protecciones ya previstas en los sistemas tradicionales, las reglas de la responsabilidad contractual podrían encontrar un límite adicional en la regulación específica sobre IA. Por ejemplo, el Reglamento de IA de la Unión Europea introduce obligaciones de transparencia, seguridad y responsabilidad para los proveedores de sistemas de alto riesgo, lo que podría limitar la eficacia de las cláusulas de exclusión de

responsabilidad, dada la importancia radical del deber de información (dinamizado, además, por la normativa de privacidad y protección de datos personales).

Si el desarrollador, proveedor o fabricante incumple con las regulaciones aplicables (por ejemplo, en cuestiones tan sensibles como el deber de proveer información adecuada al usuario), tal incumplimiento afecte la validez de las cláusulas del contrato. Si la evaluación previa del sistema de IA falla por no respetar las premisas del diligencia y cuidado de la legislación, como la prevista en el Reglamento de IA de la Unión Europea, es posible que las cláusulas contractuales que pretendan imponerse al usuario arrastren esta misma falta de diligencia, siendo insuficientes desde la perspectiva de transparencia en la provisión de información.

Concluimos, entonces, que las vías de responsabilidad contractual y extracontractual en el marco de los reclamos por resarcimiento de daños aplicarían en el uso de sistema de IA con criterios similares a los que aplican tradicionalmente, pero que, en lo que resulta de interés para la reparación en la vía contractual, la validez de las cláusulas será un asunto de especial trascendencia. En tal sentido, pudiera ser posible que en el marco del uso de los sistemas de IA se requiera ser extremadamente cuidadoso en el diseño del contrato, previendo cláusulas claras, específicas, que no contravengan normas imperativas y, eventualmente, consideren la necesidad de que las cláusulas hayan sido pactadas entre partes similarmente sofisticadas.

Finalmente, el tipo de sistema de IA, sus riesgos, el contexto de uso, la finalidad para la que fue pensado, la condición de mayor o menor preparación del usuario (más arriba referida en la dimensión de la sofisticación) y todas las características que hacen tan particular y novedosos a los sistemas de IA, deben ser tenidos en cuenta al momento de evaluar la validez de las cláusulas dispuestas entre proveedores y usuarios.

#### **IV. Los regímenes de responsabilidad objetivo y subjetivo. ¿Cómo aplicar los criterios tradicionales de culpa, previsibilidad y riesgo cuando el agente responsable no es humano?**

El problema central que trata de desentrañar este trabajo es si existe un único régimen de responsabilidad capaz de resolver mejor que cualquier otro los problemas que plantea la IA, sobre todo considerando que los sistemas de IA presentan un desafío mayúsculo de cara a los criterios tradicionales de culpa e imputabilidad.

Las categorías de voluntad, discernimiento, intención o libertad,<sup>12</sup> necesarias para atribuir responsabilidad a una persona física o jurídica, resultan inaplicables a un ente carente de conciencia y que no es, al menos por el momento, un sujeto de imputación de normas. Sin embargo, los sistemas de IA despliegan conductas que tienen consecuencias en el mundo real, tienen efectos sobre las personas y las cosas, procesan información y dan respuestas, eligen entre alternativas previamente parametrizadas y ejecutan acciones y, en cualquiera de esas instancias, pueden generar daños. Esta situación inexplorada, en la que tenemos que determinar de quién es la responsabilidad, resulta en un área desconocida y seguro requerirá de alguna solución nueva o al menos, flexible, para alcanzar soluciones adecuadas.

Aunque la IA exhiba comportamientos sofisticados, “aprenda” de la experiencia y de toda la información que se le provee en ese aprendizaje (y conforme pasa el tiempo, cada vez esté mejor preparada para resolver los problemas que se le plantean), todos esos procesos están sujetos a ciertas reglas que limitan y van ajustando y modelando ese comportamiento. En efecto, el aprendizaje en los sistemas de IA está sujeto a una serie de criterios o lineamientos (¿algoritmos?) que constriñen su margen de acción y, por lo tanto, las decisiones que finalmente adoptan los sistemas de IA no son enteramente libres, aún con la capacidad ya mencionada de resolver problemas en forma más o menos independiente.

Al no existir una instancia de libre elección, parece muy difícil fundar la culpa o el dolo. Consecuentemente, sólo resta proyectar la responsabilidad sobre quienes integran la cadena de valor (desarrolladores, programadores, fabricantes, proveedores) o sobre quienes detienen el dominio funcional del sistema.

Frente a ese escenario, el régimen de responsabilidad objetiva previsto en los artículos 1722, 1757 y 1758 del Código ofrece una primera vía de solución. Cuando la ley desplaza el análisis de la culpa y vincula la obligación de reparar al mero riesgo o vicio de la cosa, se facilita la posición de la víctima: basta demostrar el daño y la relación causal con la actividad o cosa riesgosa. La carga probatoria se invierte y el demandado sólo puede exonerarse acreditando causa ajena (culpa de la víctima o hecho de un tercero por el que no debe responder). Este esquema pudiera intuitivamente ser muy útil en los supuestos de IA de alto riesgo, en los que rastrear un error humano concreto, puede ser

---

<sup>12</sup> Alterini, Ameal, Lopez Cabana “Derecho de Obligaciones”. ABELEDO PERROT ED. 2000, p. 149.

muy difícil. Si el sistema ocasiona un perjuicio, responderá quien lo introdujo en el tráfico jurídico o quien lo controla, sin necesidad de indagar en su obrar subjetivo.

Es ilustrativo el caso del vehículo autónomo<sup>13</sup> entrenado para detectar peatones pero con menor desempeño frente a la identificación de ciclistas.<sup>14</sup> Aquí el régimen objetivo permite subsumir la cuestión bajo las figuras del “uso de cosas riesgosas”, del “defecto de producto” o de la responsabilidad del guardián, garantizando una tutela eficaz para la víctima sin necesidad de indagar en el algoritmo, en dónde estuvo la falla o en razón de qué se produjo el siniestro.

Por oposición, es interesante también el caso resuelto por la justicia de distrito en Amsterdam,<sup>15</sup> en el que sí se determinó la necesidad de aclarar el algoritmo y arbitrar medidas para evitar soluciones arbitrarias o sesgadas y que resultaran en un perjuicio para los usuarios. En efecto, el tribunal resolvió sobre el reclamo de los conductores de una aplicación de transporte (Ola, similar a Uber), que requerían mayor acceso y transparencia sobre sus datos y el uso de sistemas algorítmicos y de decisiones automatizadas (*automated decision-making*) en la plataforma, a fin de asignar viajes, calificaciones y recompensas. El tribunal sostuvo que varios módulos de la plataforma constituyan elaboración de perfiles (*profiling*) y, por tanto, ordenó proporcionar acceso a esos perfiles. El tribunal concluyó que el módulo de penalizaciones y deducciones del sistema implicaba decisiones basadas exclusivamente en tratamiento automatizado con efectos suficientemente significativos en las condiciones económicas y opciones de los conductores.

El tribunal reafirmó que no basta una intervención humana meramente formal: se requiere intervención humana significativa (*meaningful human intervention*) para que la decisión no sea “exclusivamente automatizada” e impuso a la compañía una serie de acciones concretas para asegurar que los algoritmos de la plataforma llegaran a decisiones arbitrarias o sesgadas. Si bien el caso no se impusieron multas o penalidades específicas,

---

<sup>13</sup> “Inteligencia artificial y responsabilidad civil: un enfoque en materia de vehículos autónomos”. Danesi, Cecilia C. Publicado en: Sup. Esp. LegalTech 2018 (noviembre), 05/11/2018, 39 Cita Online: AR/DOC/2374/2018. Thomas Reuters.

<sup>14</sup> “El gran desafío de los coches autónomos: las bicicletas”. Publicado en “El País” 07/03/2027. [https://elpais.com/tecnologia/2017/02/28/actualidad/1488276689\\_310413.html](https://elpais.com/tecnologia/2017/02/28/actualidad/1488276689_310413.html) (Vigente al 16/12/2025).

<sup>15</sup> Citado y explicado en Guillermo Lazcoz, “Automated Decision-Making Under Amsterdam’s District Court Judgements: Drivers v. Uber and Ola, in Time to Reshape the Digital Society: 40th Anniversary of the CRIDS” 251–266 (Larcier 2021).

si se le requirió a Ola la corrección y ajuste del sistema, en pos de evitar daños a los usuarios conductores de la aplicación.

Con similar criterio, citamos aquí el fallo del tribunal de Bolonia,<sup>16</sup> en el que se resolvió la demanda de un sindicato contra Deliveroo, una plataforma de reparto de comida a domicilio que organizaba el trabajo de sus repartidores mediante un sistema algorítmico que asignaba a cada repartidor un ranking de “fiabilidad” y “participación” para decidir con qué prioridad podían acceder a oportunidades laborales de reparto, en franjas de horario preferidas. El algoritmo penalizaba cancelaciones o ausencias sin distinguir si obedecían a motivos legalmente protegidos (por ejemplo, enfermedad o ejercicio del derecho de huelga), lo que reducía de forma sistemática las oportunidades de trabajo de quienes ejercían actividad sindical. El tribunal reconoció la legitimación del sindicato y entendió que el sistema conducía a situaciones de discriminación en razón de un algoritmo que tenía sesgos y criterios mal definidos al momento de calificar a los usuarios repartidores.

El tribunal entendió que el error en el diseño del sistema era atribuible a la plataforma en tanto explotaba sistemas algorítmicos que afectan al acceso al trabajo y en tal sentido, debió indemnizar al sindicato y publicar la sentencia condenatoria. Junto con estos casos, conviven también otros en los que los criterios de responsabilidad subjetiva parecen resultar en soluciones más ajustadas.

Un ejemplo útil pudiera ser el de los sistemas de IA aplicados para el triaje médico<sup>17</sup> en el que la tasa de acierto en la asignación de prioridades realizado por la IA iguala o supera el de los profesionales humanos.<sup>18</sup> Si tanto el médico como la IA incurren en un error dentro del margen estadístico aceptado, resulta discutible imponer responsabilidad objetiva al desarrollador del algoritmo, su proveedor o fabricante (o a todos ellos), mientras que al profesional se le exige menos, ya que el paciente o sus sucesores deberán demandarlo y probar su culpa o dolo. Esta asimetría normativa podría desincentivar el

---

<sup>16</sup>Fernández Sánchez, Sonia. (2021). Frank, el algoritmo consciente de Deliveroo. Comentario a la Sentencia del Tribunal de Bolonia 2949/2020, de 31 de diciembre. Revista de Trabajo y Seguridad Social. CEF, 457, 179-193.

<sup>17</sup> “AI-driven triage in emergency departments: A review of benefits, challenges, and future directions” Publicado en International Journal of Medical Informatics. <https://www.sciencedirect.com/science/article/pii/S1386505625000553> (Vigente al 16/12/2025).

<sup>18</sup> “La Verdad Sobre el Triaje con IA: ¿Más Rápido que los Médicos Expertos?” Publicado en Shama SGE. <https://www.shaman-sge.com/la-verdad-sobre-el-triage-con-ia-mas-rapido-que-los-medicos-expertos/> (Vigente al 16/12/2025).

desarrollo tecnológico, la inversión y la innovación y en definitiva, dejar de lado el uso de sistemas de IA que demuestran ser eficientes en las tareas que se les proponen.

A su vez, se puede sostener que el régimen de responsabilidad objetiva también ofrece respuestas poco satisfactorias cuando se lo aplica a sistemas de IA supervisados, cuya operación depende significativamente del usuario. Trasladar íntegramente el riesgo a quienes diseñan o comercializan la herramienta, cuando el resultado dañoso puede vincularse con un diseño o empleo inadecuado del sistema, un uso para fines para los que la herramienta no fue diseñada o incluso, por fuera del marco contractual que el proveedor fijó para asegurar un uso “diligente” del sistema de IA, puede resultar en soluciones incorrectas.

Desde la perspectiva del régimen subjetivo, ya anticipamos que el asunto de la imputabilidad y la atribución de la culpa, serán un problema de difícil solución en el marco del funcionamiento de los sistemas de IA. Aunque pudiera determinarse dónde estuvo la actuación “negligente” en las instancias del ciclo de vida del sistema, por ejemplo, en el entrenamiento con datos sesgados o erróneos o en la omisión de pruebas de robustez, la prueba del nexo causal entre esa conducta y el daño concreto puede no ser lineal.

El modelo subjetivo podría resultar adecuado, por ejemplo, cuando un desarrollador omite parametrizaciones de seguridad adecuadas o actualizaciones críticas y por eso el sistema falla, o cuando un proveedor incumple su deber de información, exponiendo al usuario a riesgos que pudieron prevenirse. Allí, cuando sea posible identificar con precisión la falla como causa directa o eficiente del daño y atribuirla a alguien dentro de la cadena de valor, el sistema subjetivo, resulta útil y más eficaz que el objetivo.

De la misma manera, en los sistemas de IA que requieran de un usuario sofisticado para su operación y en los que es el propio usuario el que proporciona las “coordenadas” o “prompts” para obtener una respuesta, pudiera ser totalmente inapropiado atribuir culpa al desarrollador o proveedor. Si efectivamente, el usuario tiene un rol determinante y trazable en la operación del sistema, trasladar la responsabilidad al proveedor o fabricante, pudiera resultar en soluciones sub-óptimas.

En consecuencia, creemos que ningún régimen clásico satisface por sí solo las exigencias de un derecho de daños adaptado a la IA y, por lo tanto, nos inclinaremos por proponer la idea de que la respuesta más razonable descansa en una estructura híbrida. En efecto, el esquema que propiciamos podría combinar elementos objetivos y subjetivos

según el tipo de sistema de IA, su especialización, sus riesgos inherentes, previstos y previsibles, su grado de autonomía, la función específica para la que fue diseñado, las capacidades o habilidades que se exigen en el usuario y un amplio conjunto de variables (algunas más conocidas y otras no tanto) que permitan una mejor evaluación y solución del caso.

Pudiéramos concluir también que, sin que ningún sistema sirva por sí solo para resolver todos los casos, puede atenderse como válida la presunción de riesgo inherente a la IA autónoma y que, por lo tanto, pudiera justificar soluciones objetivas. Por oposición, en los sistemas asistidos, en los que el usuario cumpla un rol central o los que demandan supervisión humana podrían mantener, con matices, el filtro de la culpa, distribuyendo la carga probatoria de manera más proporcionada. Esta aproximación - como ya anticipamos, flexible- preserva la pauta fundamental de protección a la víctima, y, al mismo tiempo, evita sancionar sin más a los proveedores en escenarios en los que, aún con una actuación prudente y razonable, hubiese sido imposible prever o impedir el daño.

## **V. El Reglamento Europeo de Inteligencia Artificial. La ausencia de un régimen autónomo de responsabilidad por daños y la utilidad del régimen de productos defectuosos**

El Reglamento (UE) 2024/1689 sobre Inteligencia Artificial se erige como la norma central para el diseño, la comercialización y el uso de sistemas de IA en la Unión Europea. Su objetivo es armonizar exigencias y evitar la fragmentación normativa, garantizando la libre circulación en el mercado interior bajo estándares uniformes. No crea, sin embargo, un régimen autónomo de responsabilidad por daños, sino que delimita obligaciones preventivas y administrativas a lo largo del ciclo de vida de los sistemas de IA, como por ejemplo, gestión de riesgos, evaluación de conformidad, documentación técnica, supervisión humana, robustez, precisión, ciberseguridad y transparencia. Asimismo, impone deberes de vigilancia post-venta, registro y cooperación con autoridades, reservando la reparación de daños al derecho común de cada Estado miembro.

El sistema descansa en una clasificación por niveles de riesgo: ciertas prácticas se prohíben por incompatibilidad con los valores de la UE; los sistemas de alto riesgo quedan sujetos a requisitos estrictos; y los restantes deben cumplir obligaciones de transparencia. Proveedores y operadores asumen deberes diferenciados: los primeros deben implantar

gestión de riesgos, trazabilidad cuando corresponda, evaluación de conformidad e instrucciones claras; los segundos deben seguir dichas instrucciones, designar responsables de supervisión humana, monitorear, reportar incidentes y, en supuestos previstos, realizar evaluaciones de impacto en derechos fundamentales. El incumplimiento conlleva sanciones administrativas y medidas correctivas.

La reparación de daños, sin embargo, no se articula dentro del Reglamento, sino a través del régimen de responsabilidad por productos defectuosos. La antigua Directiva 85/374/CEE ha sido sustituida por la Directiva (UE) 2024/2853, que actualiza el marco a la luz de las nuevas tecnologías (incluida la IA) y las cadenas de suministro complejas, y busca facilitar el acceso a la indemnización frente a la creciente complejidad técnica y probatoria. La nueva Directiva (UE) 2024/2853 establece normas comunes sobre la responsabilidad de los operadores económicos por daños causados por productos defectuosos y persigue un alto nivel de protección de consumidores y demás personas físicas, reforzando la seguridad jurídica y la competencia en condiciones equitativas.

Entre sus principales novedades, amplía el elenco de operadores potencialmente responsables más allá del fabricante, abarcando al importador, representante autorizado, prestador logístico, distribuidor que no identifique al operador en plazo y a quien modifique sustancialmente el producto. Perfila un sistema de atribución objetivo, con responsabilidad solidaria en supuestos de concurrencia y presunciones sobre defecto y causalidad destinadas a aliviar la carga probatoria de la persona perjudicada. Extiende el ámbito material a cualquier bien mueble, incluso cuando esté incorporado o interconectado con otros bienes, e incluye expresamente la electricidad, los archivos de fabricación digital, las materias primas y los programas informáticos. Define, además, “archivo de fabricación digital”, “servicio conexo” y “componente”, integrando de manera explícita elementos intangibles y servicios digitales en el concepto de producto.

Aunque la Directiva menciona la IA sobre todo en sus considerandos, su alcance funcional permite abarcar los sistemas de IA como productos, con atención a sus particularidades. La noción de defecto (que determina que —el producto no ofrece la seguridad que una persona tiene derecho a esperar, conforme al Derecho de la Unión o nacional) se evalúa considerando la presentación y características, el uso razonablemente previsible, los efectos de capacidades de aprendizaje o actualización tras su puesta en el mercado, la interoperabilidad con otros productos y el momento de introducción. Este

enfoque flexible facilita capturar supuestos en los que una IA, por ejemplo, no logra desempeñarse de modo seguro en atención a su propósito y estado de la técnica.

Aun así, no todo resultado adverso implica un defecto intrínseco. En sistemas de IA, los riesgos pueden derivar de errores de programación, sesgos de datos, dinámicas propias del aprendizaje, integraciones defectuosas o usos maliciosos. Por ello, la referencia a la “seguridad razonable” atendiendo al propósito declarado, a las expectativas legítimas y al control efectivo de cada agente, puede resultar más precisa que una calificación automática de defectuosidad. La pluralidad de intervenientes —desarrolladores de software, proveedores de datos, fabricantes de hardware, integradores y operadores— complejiza la imputación y justifica, en su caso, esquemas de responsabilidad objetiva y solidaria, y soluciones híbridas que reflejen el control real sobre el riesgo y el daño.

En conclusión, el Reglamento de IA y la Directiva (UE) 2024/2853 operan de manera complementaria: el primero previene y disciplina el diseño, comercialización y uso de sistemas de IA; y la segunda proporciona el marco de responsabilidad e indemnización por daños causados por productos, incluidos los de base digital. La correcta interpretación sistemática y pragmática de ambos instrumentos, junto con su transposición y articulación con el derecho interno, será decisiva para ofrecer respuestas coherentes y efectivas ante los desafíos que presentan los sistemas de IA en su despliegue real.

## VI. Conclusiones

La atribución de responsabilidad en el uso de sistemas de inteligencia artificial, sean autónomos o supervisados, parecen requerir un enfoque flexible y contextualizado, atento a la complejidad técnica, la opacidad algorítmica y la diversidad de agentes involucrados.

En esta instancia, no nos parece posible propugnar la adopción preferente de un régimen único –objetivo o subjetivo– de manera categórica, ya que la intervención humana, la previsibilidad del daño y la capacidad de control varían significativamente según el caso. La determinación de la responsabilidad dependerá de la claridad en la asignación de roles, la naturaleza del sistema, el grado de autonomía y las circunstancias particulares, incluyendo la capacidad del usuario y la previsibilidad de los riesgos. En definitiva, la solución jurídica debe ser casuística, ponderando todas las variables relevantes para lograr una respuesta justa y eficaz.

Mientras que el régimen de responsabilidad subjetivo enfrenta obstáculos para probar culpa o nexo causal en el marco del uso de sistemas de IA, el régimen objetivo parece

adaptarse mejor para resolver los casos difíciles, en los que, el riesgo del sistema, las fallas en su diseño o programación o incluso, la sola puesta en funcionamiento de un sistema cuyo desarrollo el fabricante no puede prever, resulten en daños para las personas o las cosas. Y, sin embargo, la responsabilidad inmediata de la cadena de suministro, puede no ser siempre una solución infalible, sobre todo cuando los usuarios aportan supervisión y dirección relevante al funcionamiento de los sistemas de IA.

Por ello, nos parece mejor propiciar una estructura híbrida, que combine elementos objetivos y subjetivos según el tipo de IA, su autonomía, los riesgos involucrados y el rol del usuario. Creemos que esta aproximación flexible permite proteger a las víctimas, incentivar la seguridad y evitar sanciones inadecuadas, adaptando la respuesta jurídica a las peculiaridades de la IA y preservando los principios de reparación, prevención y equidad.

En suma, la evolución constante de la inteligencia artificial y la velocidad creciente que diariamente se le imprime a esa evolución, requerirá, además, de una fenomenal creatividad y precisión en la regulación, que los profesionales del derecho encontremos – con buen criterio– el equilibrio entre la protección de los derechos de las personas y el desarrollo y la promoción de la innovación tecnológica.<sup>19</sup>

---

<sup>19</sup> Diego Monsalves, Pablo Olivares, Fabián Riquelme y Héctor Cornide Reyes. “Inteligencia artificial como servicio: Potenciando la innovación y eficiencia en la industria y las metodologías ágiles”. Revista Chilena de Ingeniería. Noviembre 2024.

## Bibliografía

- Azar, Aldo M. “Responsabilidad por los sistemas de inteligencia artificial en entornos virtuales, aplicaciones, sitios de internet y plataformas digitales.” *RCCyC*, 2024. TR LALEY AR/DOC/1983/2024.
- Banchio, Pablo Rafael. *La ética en la inteligencia artificial y la jurisprudencia en casos emblemáticos*. Universita Virtuale Innovativa, noviembre 2024.
- Barbosa de Godoy Corrêa, Alexandra, y Claudia Ribeiro Pereira Nunes. “Artificial Intelligence in Medical Practice: Ethical and Legal Aspects.” *Doctrina Jurídica. Revista Semestral de Doctrina, Jurisprudencia y Legislación* Año XIII, n.º 29 (febrero 2022): Páginas 1 a 3.
- Bellorini, Gloria P. “La inteligencia artificial y la responsabilidad por daños en la Argentina.” *Errepar*, nota de análisis, 22 de marzo de 2023.
- Carranza Latrubesse, Gustavo. *Sobre la personalidad jurídica de los robots y de otras formas de inteligencia artificial*. Academia Nacional de Derecho y Ciencias Sociales de Córdoba, 2023.
- Erkan, Fikret, y Tirtha Dutta Biswas. “Artificial Intelligence and Liability for Damages.” *International Journal of Social Sciences (Uluslararası Sosyal Bilimler Dergisi)* 9, n.º 41 (2025): pp. 297–343. DOI: 10.52096/usbd.9.41.16.
- Galdós, Jorge M., y Ezequiel Valicenti. “Responsabilidad civil derivada de la inteligencia artificial y los sistemas inteligentes.” *TR La Ley*, 18 febrero 2025. TR LALEY AR/DOC/270/2025.
- Herrán Ortiz, Ana Isabel. *Chatbots en medicina: ética y derecho para la tecnología de los cuidados del siglo XXI*. Universidad de Deusto, 16 abril 2024.
- Hidalgo Cerezo, Alberto. *Inteligencia artificial generativa y propiedad intelectual*. Universidad San Pablo CEU.
- Juárez Ferrer, Martín, y José Fernando Márquez. “Responsabilidad civil por la utilización de inteligencia artificial.” *TR La Ley*, 26 septiembre 2024. TR LALEY AR/DOC/2262/2024.
- Luquin Bergareche, Raquel. *Inteligencia artificial en la prestación de servicios de salud: funcionalidades, riesgos y responsabilidad*. Universidad Pública de Navarra, 2024.

Navarro Mendizábal, Iñigo A. *Ética y Responsabilidad Civil en la Inteligencia Artificial.*

Universidad Pontificia Comillas, 2022.

Negri, Nicolás J., y Pablo N. Guerreiro. “Inteligencia artificial. ¿Colapso del sistema maestro de responsabilidad civil?” *RCCyC*, 2024. TR LALEY AR/DOC/1979/2024.

Ortiz Fernández, Manuel. *Responsabilidad y regulación de sistemas de inteligencia artificial.* Universidad Miguel Hernández de Elche, 2024.

Quiñones, María Constanza. *Daños derivados de la inteligencia artificial.* LA LEY, TR LALEY AR/DOC/2478/2024. (10/10/2024)

Sánchez Díaz, María Fernanda. “El impacto de la inteligencia artificial generativa en los derechos humanos.” *Revista Euro Latin de Derecho Administrativo* 11, n.º 1 (2024): e252.

Tapia Hermida, Alberto J. “*El seguro de responsabilidad civil profesional de los operadores de sistemas de inteligencia artificial*”. Universidad Complutense de Madrid; Estudio Jurídico Sánchez Calero, 13 junio 2024.

Uriol, Livia Mercedes. “*Análisis de las recomendaciones de ONU y OCDE sobre la regulación de la Inteligencia Artificial. El estado de situación en Argentina*”. Universidad de Salamanca.