

[Buenos Aires, lunes 8 de septiembre de 2025 - N° 16.042]

EL DERECHO

Edición especial

REVISTA DE DOCTRINA Y JURISPRUDENCIA

**FACULTAD DE DERECHO Y CIENCIAS SOCIALES
Y POLÍTICAS, UNIVERSIDAD NACIONAL DEL NORDESTE**

**En homenaje a los profesores Edgardo I. Saux,
Carlos Clerc y Juan Carlos Palmero.**

**"In memoriam" de los profesores César A. Abelenda,
Antonio J. Rinesi, Lisandro Segovia**

DIRECTOR DE EL DERECHO: ALEJANDRO BORDA

COORDINADOR DE REDACCIÓN: MARCO RUFINO

*Comisión 3. DAÑOS DERIVADOS DE PRODUCTOS,
SERVICIOS Y BIENES DIGITALES*

Director: Maximiliano Cossari

Autores:

EMILIANO CARLOS LAMANNA GUIÑAZU

CARLOS ALBERTO FOSSACECA

JOSÉ MARÍA SABAT MARTÍNEZ

DIEGO ALEJANDRO LO GIUDICE

VERÓNICA ELVIA MELO

MATILDE PÉREZ

FERNANDO ALFREDO UBIRÍA

CONSEJO DE REDACCIÓN:

Gabriel Fernando Limodio, Luis María Caterina, Martín J.
Acevedo Miño, Daniel Alejandro Herrera, Nelson G. A. Cossari

XXX JORNADAS NACIONALES DE DERECHO CIVIL, CORRIENTES 25, 26 Y 27 DE SEPTIEMBRE DE 2025
10 AÑOS DE VIGENCIA DEL CÓDIGO CIVIL Y COMERCIAL DE LA NACIÓN



EL DERECHO

© (5411) 3988 3256 | info@elderechodigital.com.ar

Contenido

PRESENTACIÓN

Daños derivados de productos, servicios y bienes digitales.
Nota de presentación, por Maximiliano Cossari
Cita Digital: ED-VI-CCXL-163

ARTÍCULOS

Demasiado humanos: chatbots, antroporfismos y responsabilidad civil, por Emiliano Carlos Lamanna Guiñazu, Carlos Alberto Fossaceca y José María Sabat Martínez
Cita Digital: ED-VI-CCXL-164

La prevención de daños en las plataformas digitales, por Diego Alejandro Lo Giudice
Cita Digital: ED-VI-CCXL-165

La responsabilidad derivada de daños causados por productos digitales: una necesaria revisión de conceptos, por Verónica Elvia Melo
Cita Digital: ED-VI-CCXL-166

Inteligencia artificial explicable (AIX) y prevención de daños, por Matilde Pérez
Cita Digital: ED-VI-CCXL-167

Arquitecturas que manipulan: culpa estructural y tutela reforzada de los vulnerables en el ecosistema digital. A propósito de TikTok y Robinhood, por Fernando Alfredo Ubiría
Cita Digital: ED-VI-CCXL-168

Artículos

Daños derivados de productos, servicios y bienes digitales

Nota de presentación

por MAXIMILIANO COSSARI

La editorial EL DERECHO ha tenido la gentileza de invitarnos a dirigir este Número Especial sobre Derecho de Daños con el título “Daños derivados de productos, servicios y bienes digitales”, tema que será abordado en el marco de las XXX Jornadas Nacionales de Derecho Civil.

Se trata de un tópico de indudable relevancia en la actualidad. No cabe duda de que el avance de la tecnología y la creciente digitalización de la vida cotidiana han transformado profundamente las relaciones jurídicas, generando a su vez nuevos escenarios para la circulación de bienes, la prestación de servicios y el consumo de productos. Surgen así nuevas formas de daños que desafían las categorías tradicionales del régimen de responsabilidad civil, planteando la necesidad de una reflexión jurídica profunda y renovada.

Explica Ubiría que “Los principios de ‘no dañar a otro’ y de ‘buena fe’, aplicados en materia de responsabilidad por productos, servicios y bienes digitales, imponen proteger especialmente a los sujetos vulnerables como por ejemplo niños y adultos mayores, potenciales víctimas de graves daños”, tutela que alcanza tanto a intereses individuales, como colectivos o difusos⁽¹⁾.

En esta línea, resulta indispensable revisar conceptos clave como la noción de bienes digitales, que abarca tanto bienes inmateriales como el patrimonio digital, adaptar la noción de producto, repensar el concepto de proveedor y definir cuál será, en definitiva, el régimen normativo adecuado para atender al resarcimiento de daños causados por productos o servicios digitales⁽²⁾.

NOTA DE REDACCIÓN: Sobre el tema ver, además, los siguientes trabajos publicados en EL DERECHO: *Las “tecnologías reproductivas” y la ética médica*, por ELISABET AGUSTINA VIDAL, ED, 259-913; *Responsabilidad civil en internet: avance de las nuevas tecnologías de la información y asignaturas pendientes del sistema jurídico*, por MARCELO OSCAR VUOTTO, ED, 261-860; *El nuevo Código Civil y Comercial y el rol de nuestra formación jurídica*, por MARIO A. ZINNY, ED, 263-870; *El Código Civil y Comercial en clave de derechos humanos. El impacto del derecho internacional de los derechos humanos en la aplicación e interpretación del nuevo derecho privado argentino*, por MARCELO TRUCCO, ED, 264-810; *El uso de la tecnología y la gestión de la comunicación en la mediación actual*, por JUAN FERNANDO GOUVERT, ED, 275-771; *El derecho ante la inteligencia artificial y la robótica*, por VERÓNICA ELVIA MELO, ED, 276-493; *La protección de los datos personales en internet (una tarea ineludible)*, por ESTEBAN RUIZ MARTÍNEZ, ED, 284-726; *La comunidad humana en la era tecnológica*, por LEONARDO PUCHETA, ED, 282-1044; *Robótica e inteligencia artificial: nuevos horizontes de reflexión*, por LEONARDO PUCHETA, ED, 283-925; *Los paradigmas del derecho privado codificado. El caso argentino: de persona a individuo*, por GABRIEL F. LIMODIO, ED, 286-461; *El concepto de persona frente a las tecnologías disruptivas: persona humana, persona jurídica, ¿persona electrónica?*, por VERÓNICA ELVIA MELO, ED, 289-1386; *Derecho de los robots*, por PILAR MOREYRA, ED, 291-708; *Alcances del deber de seguridad y la conducta procesal como fundamento para la imposición de una sanción punitiva*, por WALTER F. KRIEGER, ED, 291-293; *La figura del daño punitivo en la Ley de Defensa del Consumidor. Un aporte para la inagotable polémica sobre los requisitos de procedencia y su valoración judicial*, por BELÉN JAPAZE, ED, 292-462. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(1) Ubiría, Fernando A., “Arquitecturas que manipulan: culpa estructural y tutela reforzada de los vulnerables en el ecosistema digital. A propósito de TikTok y Robinhood”.

(2) Melo, Verónica, “La responsabilidad derivada de daños causados por productos digitales: una necesaria revisión de conceptos”.

Es imprescindible indagar también acerca de los deberes concretos de prevención de daños que recaen sobre las plataformas que brindan servicios digitales, especialmente en lo que respecta a la necesidad de brindar información suficiente, en particular cuando se está frente a una relación de consumo⁽³⁾.

A su vez, la presencia de la inteligencia artificial (IA) plantea nuevos interrogantes en lo que respecta a productos, servicios y bienes digitales. Se requiere de un análisis pormenorizado de las funciones de la responsabilidad civil aplicada a la IA, sus alcances y la atribución de responsabilidad en supuestos de daños⁽⁴⁾.

La problemática se acentúa al considerar aquellos supuestos en los que la IA interviene en la causación de los daños pero resulta difícil reconocer con certeza los mecanismos mediante los cuales ha llegado a ciertos resultados o decisiones. La opacidad existente requiere poner en discusión nuevos principios vinculados con la transparencia de los procesos internos y de las lógicas de decisión de los algoritmos para la gestión de riesgos y evitación de daños⁽⁵⁾.

Mucho más grave es el caso cuando se utilizan los algoritmos como estrategia empresarial deliberada de captación, que transforma al usuario en objeto de diseño comercial y se causan daños que derivan del diseño de arquitecturas digitales que inducen comportamientos previsiblemente nocivos⁽⁶⁾.

En definitiva, hemos convocado a destacados autores para reflexionar sobre estas y otras problemáticas con rigurosidad conceptual y compromiso práctico. Confiamos en que este aporte será útil para nutrir el debate doctrinario, enriquecer la labor de los operadores jurídicos y, sobre todo, contribuir a una respuesta jurídica más eficaz y actualizada frente a los nuevos riesgos que plantea la era digital.

VOCES: CÓDIGO CIVIL Y COMERCIAL - INTELIGENCIA ARTIFICIAL - RESPONSABILIDAD CIVIL - RESPONSABILIDAD CONTRACTUAL - PERSONAS JURÍDICAS - INTERNET - PODER JUDICIAL - DERECHOS Y GARANTÍAS CONSTITUCIONALES - RESPONSABILIDAD OBJETIVA - TECNOLOGÍA - INFORMÁTICA - DAÑOS Y PERJUICIOS - DEFENSA DEL CONSUMIDOR - DERECHOS HUMANOS - DERECHO COMERCIAL - ACTOS DE COMERCIO - CONTRATOS COMERCIALES - DAÑO PATRIMONIAL - OBLIGACIÓN DE SEGURIDAD - DERECHOS DEL CONSUMIDOR - OBLIGACIONES - COMUNICACIONES ELECTRÓNICAS - COMERCIO ELECTRÓNICO - DAÑO PUNITIVO - E-COMMERCE - RESPONSABILIDAD OBJETIVA

(3) Lo Giudice, Diego, “La prevención de daños en las plataformas digitales”.

(4) Lamanna Guiñazu, Emiliano C.; Fossaceca, Carlos A.; Sabat Martínez, José M., “Demasiado humanos: chatbots, antroporfismos y responsabilidad civil”.

(5) Pérez, Matilde, “Inteligencia artificial explicable (AIX) y prevención de daños”.

(6) Ubiría, Fernando A., “Arquitecturas que manipulan: culpa estructural y tutela reforzada de los vulnerables en el ecosistema digital. A propósito de TikTok y Robinhood”.

Demasiado humanos: chatbots, antroporfismos y responsabilidad civil

por EMILIANO CARLOS LAMANNA GUIÑAZÚ^(*), CARLOS ALBERTO FOSSACECA^(**) y JOSÉ MARÍA SABAT MARTÍNEZ^(***)

Sumario: I. INTRODUCCIÓN. — II. LA INTELIGENCIA ARTIFICIAL Y LOS MODELOS DE LENGUAJE. — III. APLICACIÓN DEL DERECHO CONSUMERIL. — IV. LA ANTJURIDICIDAD. — V. LA RELACIÓN DE CAUSALIDAD. — VI. FACTOR DE ATRIBUCIÓN. — VII. PERSPECTIVA DE LAS JORNADAS NACIONALES DE DERECHO: UNA VIEJA PREOCUPACIÓN IUSPRIVATISTA. — VIII. FUNCIÓN PREVENTIVA. — IX. LEGITIMACIÓN PASIVA. — X. CONCLUSIONES.

I. Introducción

El presente trabajo versa sobre temas controvertidos, opinables, analizados en una materia cuyos márgenes no están plenamente definidos, pero que resulta ser siempre novedosa, y que su *ratio* particular es la de encontrarse en constante evolución. De tal manera, no puede esperarse que existan opiniones definitivas, ni una doctrina estable en el punto basadas en tecnologías algorítmicas. Empero, se tratará el tema con las herramientas de nuestro tiempo, de lo que se entiende vigente en la actualidad. En suma, de lo que ofrece la actualidad jurídica. Ahora, parece claro que se trata de uno de los desafíos más salientes que ofrece al Derecho de esta época.

La materia en cuestión no solo involucra tecnologías innovadoras, sino también, cuestiones de indudable raíz ética, como ser la ponderación acerca de si es o no deseable que se restrinjan ciertos aspectos del diseño de la IA, en orden a proteger a los ciudadanos.

En cuanto al análisis jurídico, será necesario intentar conjugar los nuevos problemas que conlleva la IA con las normas existentes. También se deberá tener en cuenta los conflictos que la IA plantea en otros sistemas jurídicos y ver su posible correlato en el nuestro.

A eso apuntamos en estas líneas.

NOTA DE REDACCIÓN: Sobre el tema ver, además, los siguientes trabajos publicados en *EL DERECHO*: *Las “tecnologías reproductivas” y la ética médica*, por ELISABET AGUSTINA VIDAL, ED, 259-913; *Responsabilidad civil en internet: avance de las nuevas tecnologías de la información y asignaturas pendientes del sistema jurídico*, por MARCELO OSCAR VUOTTO, ED, 261-860; *El nuevo Código Civil y Comercial y el rol de nuestra formación jurídica*, por MARIO A. ZINNY, ED, 263-870; *El Código Civil y Comercial en clave de derechos humanos. El impacto del derecho internacional de los derechos humanos en la aplicación e interpretación del nuevo derecho privado argentino*, por MARCELO TRUCCO, ED, 264-810; *El uso de la tecnología y la gestión de la comunicación en la mediación actual*, por JUAN FERNANDO GOUVERT, ED, 275-771; *El derecho ante la inteligencia artificial y la robótica*, por VERÓNICA ELVIA MELO, ED, 276-493; *La protección de los datos personales en internet (una tarea ineludible)*, por ESTEBAN RUIZ MARTÍNEZ, ED, 284-726; *La comunidad humana en la era tecnológica*, por LEONARDO PUCHETA, ED, 282-1044; *Robótica e inteligencia artificial: nuevos horizontes de reflexión*, por LEONARDO PUCHETA, ED, 283-925; *Los paradigmas del derecho privado codificado. El caso argentino: de persona a individuo*, por GABRIEL F. LIMODIO, ED, 286-461; *El concepto de persona frente a las tecnologías disruptivas: persona humana, persona jurídica, ¿persona electrónica?*, por VERÓNICA ELVIA MELO, ED, 289-1386; *Derecho de los robots*, por PILAR MOREYRA, ED, 291-708; *Alcances del deber de seguridad y la conducta procesal como fundamento para la imposición de una sanción punitiva*, por WALTER F. KRIEGER, ED, 291-293; *La figura del daño punitivo en la Ley de Defensa del Consumidor. Un aporte para la inagotable polémica sobre los requisitos de procedencia y su valoración judicial*, por BELÉN JAPAZE, ED, 292-462. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) Abogado (UBA). Doctor en Ciencias Jurídicas (UCA). Especialista en Derecho de la Alta Tecnología (UCA). Profesor Titular de la Pontificia Universidad Católica Argentina (UCA) en “Derecho de las Obligaciones” y “Derecho de Daños”. Por las mismas asignaturas es Profesor Titular en la Universidad del Museo Social Argentino (UMSA), y webmaster en la Facultad de Derecho de la Universidad de Buenos Aires (UBA). Coordinador académico del Doctorado en Ciencias Jurídicas de la Facultad de Derecho (UCA). Coordinador del Centro de Innovación Jurídica de la Facultad de Derecho (UCA). Director del suplemento “Derecho, Innovación & Desarrollo Sustentable” de la editorial *El Derecho*. Su dirección de correo electrónico: emilianolamanna@uca.edu.ar

(**) Abogado (UCA). Doctor en Ciencias Jurídicas (UCA). Especialista en Derecho de Daños (UCA). Profesor Adjunto en las asignaturas “Derecho de las Obligaciones” y “Derecho de Daños” de la Facultad de Derecho de la Pontificia Universidad Católica Argentina (UCA). Autor de numerosos artículos de doctrina, ponente en Jornadas Nacionales y conferencista en temas de su especialidad. Su dirección de correo electrónico: fossaceca@uca.edu.ar

(***) Abogado (UCA). Especialista en Asesoramiento Jurídico de Empresas (UCA). Profesor Titular de “Obligaciones” y de “Derecho de Daños” (USAL). E-mail: jose.sabat@usal.edu.ar

II. La Inteligencia Artificial y los modelos de lenguaje

El derecho requiere de la existencia de un objeto, entendida esta como una realidad. Determinar la norma aplicable y distribuir facultades y deberes importa definir primero a aquella realidad a ser ordenada.

En el caso de la IA, la necesidad de contar con una definición se da de bruce con la realidad pretendida. De momento, no se ha logrado una definición distintiva y, sobre todo, uniforme en el tiempo. Las que nos importan, al menos, han sido modificadas por fuerza de las nuevas potencias que la propia tecnología ha producido, y que se nos dificulta describir. La reacción que esto produce es que no hay una *agenda de seguimiento* que pueda elaborar una definición clara, distintiva y abarcativa de la Inteligencia Artificial. Sus finalidades infinitas van marcando la época, y las definiciones también.

Veamos ...

Allá por el mes de mayo de 2019, la Organización para la Cooperación y Desarrollo Económico (OCDE) emitió un documento donde definió a la IA como “un sistema basado en una máquina que puede, para un objetivo definido por el ser humano, hacer predicciones, recomendaciones o decisiones que influyen en entornos reales o virtuales. Los sistemas de IA están diseñados para funcionar con distintos niveles de autonomía”.

Posteriormente, y merced al impacto causado por el lanzamiento de ChatGpt el 30 de noviembre de 2022, y con el texto normativo propuesto por la Unión Europea aún en fase de aprobación (Propuesta de Reglamento de Inteligencia Artificial), corriendo el año 2023, la OCDE actualizó la definición, pasando a entender a la IA como “un sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere, a partir de la información que recibe (input), cómo generar resultados como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los distintos sistemas de IA varían en sus niveles de autonomía y adaptabilidad tras su despliegue”⁽¹⁾.

Más allá de lo mencionado con anterioridad, ambas definiciones son reveladoras de una misma idea descrita transversalmente por ambas definiciones: es una tecnología multipropósito, cuyos *propósitos* aún no los conocemos en su totalidad. Lo que apareja incertidumbre, pero también, ausencia de sorpresa frente a sus potenciales resultados. La cuestión, al menos en torno a su definición, se encuentra lejos de estar cerrada. La definición de IA sigue abierta.

Por su parte, los grandes modelos de lenguaje –conocidos bajo sus siglas de uso como LLM– permiten a la IA *entrenarse* para *comprender*, en base al lenguaje natural, los objetivos que se le proponen o los servicios que se le requieren. En este caso, para el humano obraría como una potencial compañía técnica que mejoraría sus limitadas capacidades.

Junto con estas ventajas, que se celebran –por ejemplo– en función de la optimización laboral, se ha reportado, también, su potencial dañoso. Así, por ejemplo, se informó del suicidio de un adolescente de catorce años, presuntamente relacionado con la interacción con un chatbot, y cuyas ulterioridades produjeron escalofríos en desarrolladores y consumidores de este tipo de tecnologías. Los hechos parecen explicarse del siguiente modo: todo parece indicar que la víctima comenzó a interactuar con una app denominada “Character AI”, que le permitía tener conversaciones que buscaban asemejarse a las que se producen en la interacción humana, llegando a insistir y replicar, todo lo posible, su carácter real. El joven manifestó sentirse enamorado del programa (al que no veía como tal, claramente), desarrollando una obsesión al respecto. Su salud mental fue declinando, hasta llegar al desenlace

(1) Reglamento de Inteligencia Artificial, P9_TA(2024)0138, Artículo 3, 1), y en el sitio web https://www.lksnext.com/es/noticias_boletin/la-ocde-actualiza-la-definicion-del-concepto-inteligencia-artificial/

luctuoso. Su madre, Megan García, inició un litigio⁽²⁾, que se pasará a comentar.

En este trabajo buscaremos tomar los conflictos y planteos esgrimidos en aquel proceso, y darle una lectura a la luz del derecho argentino.

III. Aplicación del derecho consumeril

La complejidad propia de los sistemas de IA convierte a su titular en un *proveedor*. La asimetría de información entre quienes son responsables de estos sistemas, por un lado, y los usuarios, por el otro, denotan la profesionalidad a que refieren tanto el art. 2 de la ley 24.240 como el art. 1093 del CCCN.

El usuario, en tanto, debería ser considerado consumidor (excepto el caso en que incorpore la IA a un proceso productivo, comercial o profesional).

En el caso “Megan García” se discute si la IA constituye un producto o un servicio. Ello se debe a que, según el derecho aplicable en Florida, la responsabilidad objetiva (*strict liability*) rige respecto de los productos. Allí se decidió que se podría estar ante un producto, toda vez que los daños se derivarían de un defecto de diseño del programa, y no de ideas o expresiones allí obrantes.

En la ley 24.240, por su parte, la responsabilidad por daños está referida al “vicio o riesgo de la cosa o de la prestación del servicio” (art. 40).

En nuestro derecho, la ausencia de materialidad impide considerar a los chatbots como una cosa. De todos modos, entendemos que el art. 40 es aplicable a los productos inmateriales. A todo evento, los chatbots también podrían ser tenidos como servicio. Su naturaleza coincide con las nociones de “*encargo, actuación, prestación, trabajo, favor, misión, asistencia, función, oficio, ocupación, ayuda, auxilio*”⁽³⁾.

IV. La antijuridicidad

Más allá de las dificultades y perplejidades que este presupuesto representa a nivel del derecho local, debemos situarnos en el caso sometido a estudio, y a los distintos pormenores que ha sabido generar. Por lo pronto, Megan García, madre del adolescente fallecido, centró su acusación en torno a cuatro ejes. Veamos:

- a) de violar la legislación antipornográfica, siendo que alguna de las interacciones podría configurar una simulación de actividad sexual;
- b) en una omisión del deber de informar acerca de los riesgos propios de la tecnología empleada;
- c) de incurrir en prácticas engañosas, mediante la cual los bots insistían en ser personas reales, incluso aquellos que personificaban a especialistas en salud mental;
- d) de enriquecimiento injusto, toda vez que los demandantes podrían haber utilizado la información personal del actor sin una contraprestación suficiente.

Por su parte, los demandados invocan como defensa la garantía constitucional a la libertad de discurso (*speech*) contenida en la Primera Enmienda. Sostienen para ello que la app “Character AI” configura un discurso que los usuarios tienen derecho a recibir.

Las infracciones invocadas por la demandante tienen un correlato en la legislación argentina. Más allá de ello, en nuestro país la antijuridicidad estructurada por la responsabilidad civil es de carácter material, en el sentido de que basta con acreditar que se ha sufrido un daño no justificado (daño injusto, como cláusula general del sistema). Lo que nos lleva a tener que considerar si la libertad de expresión constituye o no una causa de justificación.

En torno a esto último, el derecho a expresarse libremente surge del art. 14 de nuestra Carta Magna. Asimismo, el art. 1 de la ley 26.032 dispone que “La búsqueda, recepción y difusión de información e ideas de toda índole, a través del servicio de Internet, se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión”⁽⁴⁾.

Empero, no caigamos en el error de confundir la prohibición de la censura previa con las responsabilidades que puedan corresponder por los abusos producidos mediante

su ejercicio⁽⁵⁾. Son dos situaciones diversas, y con soluciones diversas.

De tal manera que los daños causados mediante chatbots no son justificados por la mera invocación del ejercicio de los derechos enumerados en la ley 26.032.

V. La relación de causalidad

Aquí resultan aplicables tres (3) criterios, con la solidez que significa el haber sido reconocidos en las XXIX Jornadas Nacionales de Derecho Civil de 2024, realizadas en la Universidad Austral en torno a la IA en general:

- Las reglas de la causalidad adecuada son aplicables a los daños de la IA;
- El hecho del damnificado debe ser apreciado en forma prudente cuando los daños son causados por la IA;
- La doctrina de las cargas dinámicas puede ser útil para la prueba de la causalidad.

La peculiaridad, en el caso de los chatbots, consiste en que será necesario demostrar cuatro (4) verticales posibles:

- a) La interacción entre el chatbot y la víctima;
- b) Que el chatbot expuso al damnificado a contenidos nocivos, susceptibles de causarle un daño;
- c) La ocurrencia del daño, que puede presumirse en el supuesto del perjuicio extrapatrimonial;
- d) Que exista una relación de previsibilidad entre el perjuicio sufrido y el material suministrado por el chatbot.

Cabe completar el análisis con una consideración acerca de la responsabilidad generada por los llamados *riesgos del desarrollo*. Si se sostuviera que los daños causados por la IA son imprevisibles debido al estado actual de la ciencia, ello no exoneraría la responsabilidad ni configuraría un caso fortuito. Esto se debe a que tales daños constituyen una contingencia propia de la actividad (art. 1773, inc. e) del CCCN).

VI. Factor de atribución

La actividad desarrollada por los chatbots es especialmente propensa a causar daños. Al respecto, se ha señalado que el *antropomorfismo* de los modelos LLM supera las capacidades humanas para persuadir, inferir sentimientos, cambiar el tono de las conversaciones, generar desinformación, engaños y la consecuente manipulación, añadiéndose que el común de la población no está preparado para los desafíos que importa la proliferación de esta tecnología⁽⁶⁾.

Siendo así, la responsabilidad concomitante será *objetiva*, al tratarse de una actividad peligrosa, conforme lo previsto por el art. 1757 del CCCN.

En el ámbito consumeril, la responsabilidad también será objetiva, a tenor del art. 40 de la LDC.

VII. Perspectiva de las Jornadas Nacionales de Derecho: una vieja preocupación iusprivatista

La problematización en la interacción entre la tecnología y el derecho es una tarea que ocupa un lugar central en la doctrina civilista de las últimas cuatro décadas. Por encima de cualquier otra área o rama jurídica, es el derecho civil el que ha tomado el liderazgo en su discusión científica.

En efecto, las XI Jornadas Nacionales de Derecho Civil de 1987 celebradas en la Universidad de Belgrano, en la Comisión 2 (en esos tiempos destinada a Derecho de las Obligaciones y, dentro de estas a la responsabilidad), debatieron la “Responsabilidad civil emergente de la Informática”. En ella se señaló *–de lege ferenda*, claro– que podía haber responsabilidad civil contractual por *errores* y *disfuncionalidad* en los programas de computación (software), y en similar sintonía se propuso una muy interesante categoría de soluciones⁽⁷⁾. Lo que impone

(5) Hacemos aplicación aquí de la doctrina de la CSJN *in re* “Ponzetti de Balbin” (Fallos 306:1892).

(6) Peter, Sandra – Riemer, Kai – West, Javin D. “The benefits and dangers of anthropomorphic conversational agents” PNAS, 16/05/2025, rec. el 19/06/2025 en <https://www.pnas.org/doi/10.1073/pnas.2415898122>

(7) V) Responsabilidad extracontractual: Cuando la actividad informática causa daños a terceros la responsabilidad se sitúa en el ámbito extracontractual debiendo distinguirse: a) Cuando se trata de perjuicios causados por la cosa interviniendo activamente rige el sistema de responsabilidad objetiva del artículo 1113 2° párrafo del Código Civil. En tal supuesto, además, el proveedor vendedor responde en su calidad de fabricante o transmitente de un producto elaborado (Hardware y software); b) Cuando la cosa no interviene autónomamente en la producción del daño, sino respondiendo al actuar del operador, su regulación se efectuará por aplicación del artículo 1109 del Código

(2) United States District Court, Middle District of Florida, Orlando Division “Megan García v. Character Technologies, Noam Shazeer, Daniel de Fietas, Google LLC and Alphabet Inc”, Case Nro 6: 24-cv-1903-ACC-UAM

(3) Diccionario de la Real Academia Española, vocablo “servicio”. Rec. el 03/06/2025 en <https://dle.rae.es/servicio>

(4) B.O. 17/06/2005.

señalar que casi cuarenta años antes ya existía una preocupación sobre el tema, con el condimento extra de una fusión codificada como era el Proyecto Camisar de 1987 de unificación civil y comercial⁽⁸⁾.

Más acá en el tiempo, septiembre de 2019, asoman las XXVII Jornadas Nacionales de Derecho Civil realizadas en la Facultad de Ciencias Jurídicas y Sociales de la UNL donde la Comisión 3 (Derecho de Daños) lanzó el tema inherente a la “Responsabilidad por actividades riesgosas o peligrosas” y en sus conclusiones tuvieron especial atención e incidencia las actividades producidas en el ámbito cibernético. Por ejemplo, dentro de lo que podemos denominar enumeración ejemplificativa de actividades riesgosas, puede mencionarse el siguiente despacho: *la utilización de algoritmos, las actividades cibernéticas, las plataformas digitales y sistemas operados por Inteligencia Artificial* (unanimidad)⁽⁹⁾.

Cerrando este camino, aparecen las recientes, y también mencionadas, XXIX Jornadas Nacionales de Derecho Civil –septiembre de 2024–, celebradas en la Universidad Austral, donde en el seno de la comisión Nro. 3 se debatió sobre “Daños derivados de la inteligencia artificial” con importantes definiciones sobre los distintos temas, como ser, un despacho unánime que refiere: “En el Código Civil y Comercial Argentino, los sistemas de I.A., robots y algoritmos, están comprendidos en el concepto normativo de cosa y actividad, es decir como objeto de derechos, descartando su calificación jurídica como sujetos o centro de imputación de derechos y obligaciones”.

En lo tocante a la relación de causalidad en dichas jornadas se dijo: “Las reglas de la causalidad adecuada son aplicables a los daños de la IA”.

En lo referente al hecho del damnificado, sostuvo: “El hecho del damnificado debe ser apreciado en forma prudente cuando los daños son causados por la IA”.

Lo que proyectan estos despachos plasmados en distintas Jornadas Nacionales de Derecho Civil es que vemos una línea directriz que pone al Derecho Civil argentino en un espacio de estelaridad para seguir gestionando el debate continuo de esta problemática, que, como vimos, lleva casi cuatro décadas de observación, análisis y propuesta de soluciones.

VIII. Función preventiva

Los *legitimados pasivos* –frente a la demanda de Megan García– sostuvieron que no tenían ninguna relación especial con el menor fallecido que amerite, de parte de ellos, un deber de cuidado.

El decisorio, en tanto, sostuvo que ese deber puede existir si los demandados eran conscientes de los riesgos concernientes a la app que habían creado; o si produjeron un riesgo que les era posible controlar. En tal caso, debían disminuir el riesgo o tomar precauciones suficientes.

En nuestro derecho, el *deber de prevención* no constituye una obligación, en cuanto no hay un deudor o un acreedor en concreto. Por el contrario, es un deber a cargo de “toda persona... en cuanto de ella dependa” (art. 1710, CCCN), vaguedad que se celebra si vemos el asunto “García” con ojos y derecho argentino.

Civil o en su caso, por aplicación del artículo 1113 2° párrafo, 1ra. parte. VI) En aquellas hipótesis en que el damnificado no pudiera identificar al autor del daño, resultará aplicable la responsabilidad grupal o colectiva y siempre que se verifiquen en el caso los requisitos generales imprescindibles para su operatividad; VII) El tratamiento automático de datos debe efectuarse sin menoscabo para las personas y el avance sobre los derechos personalísimos origina responsabilidad (C.C. art. 107 bis); VIII) El derecho de hacer cesar tales actividades debe contemplarse como función preventiva de la responsabilidad civil. En el sitio web DC de la Facultad de Ciencias Jurídicas y Sociales UNLP <https://www.derechocivil.jursoc.unlp.edu.ar/index.php/17-jornadas-nacionales-de-derecho-civil/83-1987-xi-jornadas-nacionales-de-derecho-civil-universidad-de-belgrano-buenos-aires>

(8) “En 1986 la Cámara de Diputados impulsó dos proyectos de unificación de la legislación civil y comercial en materia de obligaciones y contratos, creándose a tal efecto una comisión especial –integrada por los doctores Héctor Alegría, Atilio Alterini, Jorge Alterini, Miguel Araya, Francisco de la Vega, Horacio Fargosi, Sergio Le Pera y Ana Isabel Piaggi– que elaboró un dictamen que se aprobó por la Cámara de Diputados en 1987 y luego por la Cámara de Senadores en 1991, dando lugar a la Ley 24.032, vetada en su totalidad por el P.E.N. en dicho año”. Merlo, Leandro Martín, “El Derecho alimentario en el proyecto”, en DFyP 2012, 1/7/2012, 189 en el sitio web Pensamiento Civil: https://www.pensamientocivil.com.ar/system/files/el_derecho_alimentario_en_el_proyecto_rdfyp.pdf

(9) En el sitio web de la Facultad de Ciencias Jurídicas y Sociales (FCJS) en <https://www.fcjs.unl.edu.ar/jndc2019/> y en el sitio web derivado en la misma página: <https://drive.google.com/drive/folders/1IdO5Q7vVKJPTBYIsPR0kA5iX5JoU4ybY>

En el marco consumeril, en tanto, el principio se acenúa con el llamado *deber de seguridad* (art. 5, ley 24.240). Tal deber se extiende a los entornos digitales, en donde opera con mayor intensidad el principio protectorio⁽¹⁰⁾. La diferencia de tono es la incertidumbre que dicho entorno ofrece.

Dentro de esta *prevención del daño*, corresponde analizar la posibilidad de aplicar filtros, restricciones o configuraciones que impidan la producción del daño. Es decir, medidas consistentes en evitar causar un daño que no tiene justificación posible.

En “R., M.B.”⁽¹¹⁾ la CSJN determinó, para el caso de los buscadores de Internet, que la existencia de filtros podría implicar censura previa; y que tal principio solo cedía en casos especialísimos, como, por ejemplo, cuando está en juego el interés de un menor de edad. Esta consideración ha resultado palmaria y un sistema de pensamiento aplicado por el máximo tribunal argentino.

Entendemos que tal criterio no es aplicable al supuesto en estudio. En el caso de los buscadores, se analiza la responsabilidad del buscador por facilitar, de alguna manera, el acceso a contenido creado por terceros. En el caso de los proveedores de IA, se trata de una responsabilidad por el producto o servicio propio, independientemente de las fuentes que hayan empleado para entrenar a su sistema.

Siendo así, entendemos que debe exigirse que los sistemas de IA cumplan con determinados requisitos; y que ello incluya deberes *ex ante* y controles *ex post*. Es decir, recaudos que los desarrolladores deben observar antes de lanzar el producto al consumo masivo e indeterminado, y la posibilidad de que los organismos públicos establezcan medidas eficaces en caso de que se observe un accionar contrario a derecho.

En ese sentido cabe aplaudir el criterio del Reglamento Europeo sobre IA⁽¹²⁾, que en su art. 5 prohíbe técnicas tales como:

- las que fueren subliminales, deliberadamente manipuladoras o engañosas;
- las que exploten las vulnerabilidad o discapacidades de las personas;
- las que tiendan a clasificar o evaluar personas en pos de su comportamiento social, o que inferan las emociones de una persona humana en el ámbito laboral o educativo.

Asimismo, el Reglamento incluye el deber de los proveedores de IA de retirar del mercado, desactivar o recuperar el programa que no cumpla con los estándares que la norma prevé (art. 20).

En nuestro derecho, la CSJN ha admitido la existencia de contenidos manifiestamente ilícitos, tales como “pornografía infantil, datos que faciliten la comisión de delitos, que instruyan acerca de éstos, que pongan en peligro la vida o la integridad física de alguna o muchas personas, que hagan apología del genocidio, del racismo o de otra discriminación con manifiesta perversidad o incitación a la violencia, que desbaraten o adviertan acerca de investigaciones judiciales en curso y que deban quedar secretas, como también los que importen lesiones contumeliosas al honor, montajes de imágenes notoriamente falsos o que, en forma clara e indiscutible, importen violaciones graves a la privacidad exhibiendo imágenes de actos que por su naturaleza deben ser incuestionablemente privados, aunque no sean necesariamente de contenido sexual”⁽¹³⁾.

Es evidente, entonces, que el diseño de los programas de IA no puede promover la difusión de contenidos semejantes, y que, ante su presencia, es lícito que se dispongan medidas judiciales que resulten eficaces para evitar que la situación continúe.

Lo dicho es sin perjuicio de lo que se prevea en la normativa particular. Así, por ejemplo, quien realiza actos discriminatorios puede ser obligado a cesar en su realización (art. 1, ley 23.592⁽¹⁴⁾).

IX. Legitimación pasiva

En “Megan García” se demandó a Character Technologies, en su carácter de titular de los derechos de la app Character AI.

(10) XXVIII Jornadas Nacionales de Derecho Civil, Comisión 5 (Derecho de los Consumidores), conclusión 2.1.

(11) CSJN, 28/10/2014, “R., M.B. c/ Google Inc. y otros s/ Daños y perjuicios”, Fallos 337:1174.

(12) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024.

(13) *In re* “R., M. B.”, cit.

(14) B.O. 05/09/1988.

También se demandó a dos ingenieros, quienes, trabajando para Google, habrían desarrollado un modelo denominado LaMDA, que permite que el chatbot intervenga en conversaciones en las cuales se invita y propone al interlocutor el poder compartir informaciones y pensamientos. En Google hubo objeciones, debido al riesgo de que los humanos les asignen un significado real a las expresiones del chatbot. Más adelante, los ingenieros se alejaron de Google y fundaron Character Technologies. Sin perjuicio de ello, Google celebró acuerdos con Character para brindarle asistencia tecnológica.

El reclamo también se hizo extensivo a Google. Ello, debido a que se alegó que el modelo utilizado por la app fue inventado y desarrollado inicialmente por Google, quien habría aportado propiedad intelectual y tecnología para su desarrollo y manutención.

Se señaló también que Google habría actuado con complicidad, ya que contaba con un conocimiento actual de la dañosidad de la tecnología empleada, proveniente de su antropomorfismo.

En nuestro derecho, la ocurrencia de un daño en el marco de una *relación de consumo* conlleva una responsabilidad de tipo solidario para todos los que integren la cadena de producción, distribución y comercialización del producto (art. 40, LDC).

En lo que hace al derecho civil, si más de un sujeto hubiera tenido incidencia causal en la producción del daño, existirá una responsabilidad civil desdoblada: en efecto, será *solidaria* en caso de complicidad o dolo, o se verificará una responsabilidad *concurrente* si los daños procedieran de causas distintas, pero cuya interacción resulta ser previsible.

X. Conclusiones

La IA es una tecnología *multipropósito*, cuya definición —en la etapa actual— solo puede ser discutible y provisoria.

La *complejidad* propia de los sistemas de IA convierte a su titular en un profesional y, por lo tanto, en un proveedor.

En nuestro país no existe una regulación específica concerniente a la IA ni a los chatbots. Sin perjuicio de ello, la antijuridicidad estructurada por la responsabilidad civil es de carácter material, basta con acreditar que se ha sufrido un daño no justificado. La *libertad de expresión* no justifica los daños que un chatbot pueda causar.

El *antropomorfismo* de los chatbots los hace especialmente propensos a la causación de daños. Siendo así, la responsabilidad concomitante será la propia de las actividades peligrosas, prevista en el art. 1757 del CCyCN.

La *relación de causalidad* debe ser probada. Rige el principio de la causalidad adecuada. Los riesgos del desarrollo no pueden ser invocados como eximente.

El titular del chatbot debe observar el deber de prevención, aun cuando no tenga una relación particular o especial con la víctima. En los entornos digitales se acentúa el principio protectorio.

Los criterios de responsabilidad que la CSJN señala para los *buscadores de Internet* no son aplicables a los chatbots. Una cosa es la facilitación del acceso a contenidos de terceros y otra, muy diferente, la responsabilidad derivada por el producto o servicio propio.

Existen contenidos manifiestamente ilícitos que no deben ser difundidos por los chatbots. Esto implica a sus titulares el *deber de evitarlos* y activa la potestad de las autoridades públicas para tomar las medidas adecuadas en caso de que se infrinja al derecho.

En caso de *multiplicidad* de responsables, rigen los principios tanto sea del derecho consumeril como del derecho común: *solidaridad* en el ámbito consumeril; en tanto, en el derecho común habrá *solidaridad* en caso de complicidad o dolo, o bien responsabilidad *concurrente* si los daños procedieran de causas distintas, pero cuya interacción resulta ser previsible.

A los chatbots les es aplicable el art. 40 de la LDC, toda vez que no cabe distinguir entre vicio o riesgo de la cosa o del producto. Sin perjuicio de ello, un chatbot también podría ser tenido como servicio.

VOCES: PERSONA - TECNOLOGÍA - INFORMÁTICA - DAÑOS Y PERJUICIOS - DEFENSA DEL CONSUMIDOR - DERECHOS HUMANOS - CÓDIGO CIVIL Y COMERCIAL - DERECHO CIVIL - RESPONSABILIDAD CIVIL - RESPONSABILIDAD CONTRACTUAL - INTELIGENCIA ARTIFICIAL - ORDEN PÚBLICO - PERSONAS JURÍDICAS - PRINCIPIOS GENERALES DEL DERECHO - INTERNET - PODER JUDICIAL - DERECHOS Y GARANTÍAS CONSTITUCIONALES - RESPONSABILIDAD DEL GUARDIÁN - RESPONSABILIDAD OBJETIVA

La prevención de daños en las plataformas digitales

por DIEGO ALEJANDRO LO GIUDICE^(*)

Sumario: I. LAS PLATAFORMAS DIGITALES. – II. LA FUNCIÓN PREVENTIVA. 1. ASPECTOS GENERALES. 2. LA PREVENCIÓN EN MATERIA DE CONSUMO. – III. PREVENCIÓN Y OBLIGACIÓN DE SEGURIDAD. 1. ASPECTOS GENERALES. 2. LA PREVENCIÓN DEL DAÑO EN LA LEY DE DEFENSA DEL CONSUMIDOR. – IV. LA NECESIDAD DE BRINDAR INFORMACIÓN. – V. LA PUBLICIDAD ILÍCITA. – VI. VÍAS PARA PREVENIR. 1. EN GENERAL. 2. EN MATERIA DE CONSUMO. – VII. CONCLUSIONES.

I. Las plataformas digitales

La cuestión debe asimilarse a los supuestos en los cuales se realiza la actuación entre presentes⁽¹⁾. Es necesario tener en cuenta todas las posibles variables en cada acto a realizar y, además, las particularidades propias del sistema (la utilización de apps o sitios web, las medidas de seguridad que ellos implican, etc.).

Las plataformas pueden ser brindadas por el vendedor de productos (como sucede con las casas de electrodomésticos, supermercados con envíos, entre otros) o dedicarse a la intermediación. Cada caso tiene notas propias.

Puede tratarse de una relación basada en el derecho del consumidor o no. Ello trae distintas consecuencias, aunque no son tantas como puede parecer (en ambos supuestos debe informarse adecuadamente, pueden existir distintos plazos de prescripción según la acción a promover⁽²⁾, la responsabilidad tiene consecuencias similares, etc.).

II. La función preventiva

1. Aspectos generales

La prevención del daño es un principio general del derecho y se extiende a todos los ámbitos.

El art. 1710 del CCCN marca un estándar de actuación, al establecer que toda persona debe procurar evitar (inc. a), disminuir (inc. b) o no agravar el daño (inc. c), en cuanto de ella dependa.

Para cumplir con esta directiva, no basta con una actitud pasiva. Corresponde adoptar las medidas para lograrlo (art. 1710, inc. b del CCCN). En estos casos –y teniendo en cuenta la modalidad de las actividades desarrolladas–, debe brindarse información adecuada, advertir cuando sea necesario, garantizar la seguridad, etc.

A continuación, trataremos algunos de estos supuestos.

2. La prevención en materia de consumo

En esta rama del derecho es indispensable la actuación preventiva por los intereses que se encuentran en juego y la necesidad de contar con una respuesta rápida.

Son exigibles gestiones positivas que permitan evitar víctimas. Cobran importancia aspectos tales como la información, cooperación y advertencia de los proveedores hacia los consumidores⁽³⁾.

En nuestro país se fue gestando la prevención en el ámbito del consumo de forma gradual, hasta llegar a la reforma constitucional en 1994. Allí se contempló la protección al consumidor en el art. 42 de la Carta Magna.

La Ley de Defensa del Consumidor contemplaba a la prevención del daño incluso antes de su regulación en el Código Civil y Comercial. En su art. 52 le otorga al consumidor la posibilidad de ejercer acciones judiciales no solo cuando sus intereses resulten afectados, sino también cuando se encuentren *amenazados*.

A la vez, en la normativa específica también se advierte esta finalidad preventiva.

Los arts. 4, 5 y 6 de la Ley 24.240 contemplan pautas relativas a la información y la seguridad de los consumidores, que ayudan a prevenir daños.

También es importante la inclusión del deber de otorgar un trato digno y equitativo a los consumidores (previsto en el art. 8 bis de la Ley de Defensa del Consumidor y en los arts. 1097 y 1098 del CCCN), con el fin de evitar conductas vergonzantes, vejatorias o intimidatorias.

En materia de cláusulas abusivas, la Ley de Defensa del Consumidor le impone a la autoridad de aplicación el deber de controlar los contratos de adhesión o similares para verificar que no se encuentren incluidas (art. 38) y le otorgan la posibilidad de modificarlos (art. 39).

Debe tenerse en cuenta, además, que el Anteproyecto de Código de Defensa del Consumidor⁽⁴⁾ se encargó de tratar con mayor detenimiento esta cuestión (arts. 5, 20, 21 y 22). Se consignaron soluciones similares en la restante normativa proyectada (Proyectos 5156-D-2020 y 1898-D-2021).

III. Prevención y obligación de seguridad⁽⁵⁾

1. Aspectos generales

Se trata de dos caras de la misma moneda: primero debe mantenerse la seguridad del otro contratante y, si no se lo hace, puede surgir la responsabilidad. Hoy en día, cabe destacar que también puede promoverse una acción preventiva para lograr que se adopten las medidas necesarias si se genera una amenaza.

La predominancia de los factores objetivos de responsabilidad tiene eficacia para evitar daños, ya que el sujeto no podría especular en qué casos dejar adoptar las medidas necesarias, para no indemnizar.

El límite se advierte cuando no “depende” del sujeto evitar el daño, en los términos del art. 1710 del Código Civil y Comercial. Aquí sería inevitable y, salvo que se configure algún supuesto excepcional (art. 1733 del Código Civil y Comercial), se configuraría la eximente del caso fortuito.

2. La prevención del daño en la Ley de Defensa del Consumidor

El art. 5 de la Ley 24.240 se refiere a que los productos o servicios no deben generar peligros para los consumidores. Se trata de una norma que impone un deber de seguridad al proveedor y, a la vez, podría dar lugar a una acción preventiva o la indemnización de daños y perjuicios para el caso de incumplimiento.

Esta solución se complementa con el art. 6, que hace alusión a la protección del consumidor frente a cosas o servicios que puedan generar peligro para su salud o inte-

NOTA DE REDACCIÓN: Sobre el tema ver, además, los siguientes trabajos publicados en EL DERECHO: *Comercio electrónico y relaciones de consumo*, por EMILIANO CARLOS LAMANNA GUINAZÚ, ED, 225-989; *Estafa por medios electrónicos. Análisis del art. 173, inc. 16 (ley 26.388). Crítica. Manipulación informática. Estafas cometidas vía Internet*, por GUSTAVO JUAN VANINETTI y HUGO ALFREDO VANINETTI, ED, 223-776; *La protección de los datos personales en Internet: lineamientos que caben deducirse del fallo de la Corte Suprema*, por ESTEBAN RUIZ MARTÍNEZ, ED, 260-861; *Responsabilidad civil en internet: avance de las nuevas tecnologías de la información y asignaturas pendientes del sistema jurídico*, por MARCELO OSCAR VUOTTO, ED, 261-860; *Los contratos electrónicos de consumo en el derecho argentino*, por JOHN GROVER DORADO (h.), ED, 270-641; *Régimen jurídico de un sitio web. Identificación. Contenidos. Responsabilidades civiles derivadas de internet*, por HORACIO FERNÁNDEZ DELPECH, ED, 273-799; *Luces y sombras en un nuevo pronunciamiento de la Corte Suprema de Justicia de la Nación respecto de la responsabilidad civil de los buscadores de internet*, por GUSTAVO ARIEL ATTA, ED, 275-521; *El carácter de la responsabilidad del operador de sitio de e-commerce*, por RITA CASTIGLIONI y NICOLÁS MOFFAT, ED, 278-25; *El actuar de los “cazadores de ofertas” en la compraventa electrónica y la figura del abuso del derecho*, por JUAN IGNACIO CRUZ MATTERI, ED, 304; *Responsabilidad de las plataformas de comercio electrónico frente al consumidor*, por MARÍA EUGENIA D’ARCHIVIO, ED, 305; *Matices de la responsabilidad civil de las plataformas en línea ante la diversidad de modelos de negocios*, por SANDRA A. FRUSTAGLI, ED, 310. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) E-mail: diego.alg03@gmail.com.

(1) Conclusión nro. 1 de las XXIX Jornadas Nacionales de Derecho Civil, Comisión N° 4, Derecho de Consumo – por unanimidad.

(2) Al respecto puede verse: Dauverné, Julián S. – Testoni, Gianfranco I., “El plazo de prescripción en el contrato de seguro: un fallo esclarecedor. Comentario a fallo C - 125525 – ‘Toscano Jorge Luis c/ Caja de Seguros S.A. s/ daños y perj. incump. contractual [exc. Estado]’- SCBA”, *elDial* DC355A); Raschetti, Franco; “Tensiones entre el derecho de seguros y el régimen de defensa del consumidor. La problemática del plazo de prescripción liberatoria”, *RCCyC* 2024 (abril), TR LALEY AR/DOC/298/2024.

(3) Zavala de González, Matilde, *Resarcimiento de daños*, Buenos Aires, Hammurabi, 1999, t. 4, pág. 423.

(4) Nro. 3143-D-2020.

(5) Hemos analizado el tema en Lo Giudice, Diego – Mangialardi, Florencia, “La obligación de seguridad de las concesionarias viales. La necesidad de analizar los alcances de su responsabilidad con las nuevas tecnologías disponibles”, *ED, Diario del 11/11/2024*, nro. 15.866.

gridad física. A estos fines, el proveedor debe adoptar los mecanismos, instrucciones y normas establecidas o razonables para garantizar la seguridad del consumidor.

La Corte ha sostenido en el fallo “Ledesma” que “un contratante racional y razonable juzgaría adecuado invertir dinero, prestar un servicio, obtener ganancias, así como adoptar los cuidados para que los usuarios puedan gozar del mismo en paz y seguridad. La persecución racional de la utilidad no es incompatible con la protección de la persona, sino por el contrario, es lo que permite calificar a un comportamiento como lo suficientemente razonable para integrar una sociedad basada en el respeto a sus integrantes”⁽⁶⁾.

A la vez, quien tiene a cargo una obligación de seguridad puede ser sujeto pasivo de una acción preventiva, sea por haber generado la amenaza o por encontrarse en mejores condiciones para evitarla.

IV. La necesidad de brindar información

Las plataformas pueden vincularse con quienes las utilizan en relaciones que puedan ser calificadas como de consumo o no.

i. En el primer supuesto, el art. 4 impone que la información sea otorgada en forma cierta, clara y detallada respecto de los bienes y servicios comercializados y las condiciones en las que se lo hace. Es una herramienta importante para equilibrar la situación de debilidad en la que se encuentra el consumidor, quien contará con elementos suficientes para tomar una decisión razonada⁽⁷⁾. Les impone una carga a los proveedores que, en caso de ser incumplida, podría generarles consecuencias desfavorables. Los requisitos que impone para su cumplimiento protegen al consumidor de gran cantidad de abusos. Se ha entendido que también deben *advertirles* sobre los riesgos de los productos o servicios⁽⁸⁾, lo que implica una medida de prevención de daños.

Cuando el contrato de consumo sea celebrado a distancia y las partes utilicen técnicas de comunicación electrónica o similares, el art. 1107 del Código Civil y Comercial establece que el proveedor tiene el deber de brindar información extensa y detallada al consumidor.

A su vez, el art. 1102 del Código Civil y Comercial contempla la cesación de la publicidad ilícita.

Por otra parte, el art. 17 del Anteproyecto de Defensa del Consumidor refiere a los deberes de protección y seguridad hacia la persona y los bienes de los consumidores.

ii. En el supuesto en el que no sea aplicable la Ley de Defensa del Consumidor, el deber de información igualmente deriva de la buena fe. Pueden darse distintas situaciones: a) que se contrate con el titular de la plataforma; b) que se contrate con otro sujeto a través de ella.

En el primer caso, se trata de una relación en la cual uno de los contratantes no solo comercializa el producto o servicio, sino que también se encarga de manejar la publicidad, oferta, medios de pago, etc.

Cuando se contrata con otros sujetos, la plataforma cumple un rol de intermediación. Ante ello, las características de su actividad tienen otras particularidades y se encaminan a permitir que el negocio entre quienes utilizan la plataforma se desarrolle sin inconvenientes.

No vemos motivo para que en estos supuestos la información a brindar sea menor a la prevista en el art. 4 de la Ley 24.240. En este mundo digital, la vulnerabilidad se extiende. Se trata de una situación en la que quien organiza la actividad tiene un mayor conocimiento del estado de cosas, tecnología y características del negocio (incluso quien es avezado con el manejo de internet desconoce muchos aspectos que sólo maneja el titular). Ello impone actuar con mayor diligencia que la habitual (art. 1725 del CCCN) y lo asimilan en este aspecto a las relaciones de consumo.

iii. En cualquiera de los supuestos anteriormente mencionados, podría iniciarse una acción preventiva solicitando el cumplimiento de este deber.

iv. Las plataformas pueden tener deberes preventivos por las amenazas que generan (por ejemplo, si cuentan con

información deficiente) o para evitar daños que puedan provocar sus usuarios (sería el caso en el cual exista una alerta de que alguno de ellos pueda realizar una estafa).

v. Se les han impuesto medidas preventivas de este tipo en algunas ocasiones.

En el fallo “Mussi” se realizó una contratación entre dos sujetos, con la intermediación de MercadoLibre. El consumidor demandó tanto a quien le vendió el producto como a la plataforma. Si bien se eximió a esta última de responsabilidad, el tribunal le impuso “... implementar las medidas necesarias a fin de muñirse de todos los datos que identifiquen debidamente a los oferentes de productos y servicios”⁽⁹⁾.

Se advierte allí un mandato exhortativo, a pesar de haberla considerado irresponsable. Ello evidencia la importancia de la seguridad en este ámbito.

También se le impuso un mandato preventivo a Booking.com, en virtud de las deficiencias en la información, que podían llevar a confusión a los usuarios. En virtud de ello, se le ordenó a la empresa nacional que ajuste su conducta y, además, que ponga en conocimiento a su principal que reside fuera del país⁽¹⁰⁾.

vi. Otro aspecto muy importante es la identificación de los sujetos que se encuentran a cargo de estas plataformas. Es lo mínimo que se debe resguardar frente a la complejidad que implica la navegación en internet. Ello es una misión del Estado, pero podrían los particulares accionar en ese sentido.

Por este motivo, frente a una empresa que no podría identificarse (y que en su página ofrecía tasas de interés exorbitantes) se dispuso el bloqueo del acceso al sitio hasta tanto cumpla con la comunicación del nombre, domicilio y CUIT (art. 8, 2do. párrafo de la Ley de Defensa del Consumidor). También se ordenó que el ENACOM comunique a las prestatarias del servicio de internet y que se publique la resolución en su página digital⁽¹¹⁾.

vii. La información debe ser adecuada. Es necesario que esté a la vista, que tenga un tamaño adecuado, que no induzca a error y que cumpla con los parámetros antes mencionados.

Sin embargo, no puede exigirse en términos que excedan lo razonable⁽¹²⁾.

viii. Es indispensable el deber de advertencia. No solo respecto de los productos y servicios en general, sino también de la posibilidad de que la conducta de otros usuarios pueda perjudicar al comprador. A modo de ejemplo, la calificación que hace MercadoLibre de los vendedores (si ha tenido inconvenientes, si despacha sus pedidos a tiempo, etc.).

El art. 1107 del Código Civil y Comercial establece que, en los supuestos de contratación electrónica, el proveedor debe informar “... además del contenido mínimo del contrato y la facultad de revocar, todos los datos necesarios para utilizar correctamente el medio elegido, para comprender los riesgos derivados de su empleo, y para tener absolutamente claro quién asume esos riesgos”.

ix. Debe procurarse la prevención de conflictos y facilitar al individuo la posibilidad de reclamar, sea por aspectos de la propia plataforma o de la conducta de quienes publican en ella.

Ante ello, se puede generar una responsabilidad posterior por su omisión e incluso, si se trata de una relación de consumo, generar la aplicación de daños punitivos⁽¹³⁾.

(9) CCC Azul, Sala I, “Mussi, Julio César c. Mercado Libre S.R.L. y otro”.

(10) JCC 10 de Córdoba, “Berrondo Lion, Valeria Elisa c/ Booking. Com Argentina S.R.L. - Abreviado - Cumplimiento/Resolución de contrato - Trám. oral”, Expte. 11667667.

(11) CFed. Rosario, sala B, 8/8/2022, “Usuarios y Consumidores Unidos c. Ente Nacional de Comunicaciones (ENACOM) s/ Daños y Perjuicios”, La Ley 14/09/2022, 3, La Ley Online AR/JUR/103267/2022.

(12) De tal modo, se rechazó la medida preventiva contra una empresa proveedora del servicio de cable, telefonía e internet tendiente a la entrega en soporte físico de los productos a sus clientes. El juez entendió que no existió una acción u omisión antijurídica (CN-Com., sala F, 5/11/2019, “Asociación por la Defensa de Usuarios y Consumidores c. Telecentro SA s/ ordinario”, La Ley Online AR/JUR/37438/2019).

(13) Hemos tratado la cuestión de los daños punitivos frente a los medios electrónicos en Lo Giudice, Diego A., *Daños punitivos. Análisis doctrinario y jurisprudencial. Aspectos sustanciales y procesales*, El Derecho, 2024, pág. 290. Ello puede darse por sus incumplimientos en materia de seguridad (pág. 293) y por su reincidencia (págs. 281 y ss.).

(6) CSJN, 22/4/2008, “Ledesma, María Leonor c/ Metrovías S.A. s/ Recurso de hecho deducido por la actora”, Fallos: 331:819.

(7) Cossari, Maximiliano, “Prevención y precaución de daños en las relaciones de consumo”, La Ley 08/04/2022, 1, La Ley Online AR/DOC/1196/2022.

(8) Frustagli, Sandra A. – Hernández, Carlos A., “Las exigencias de seguridad en la relación de consumo”, Suplemento Especial Obligación de Seguridad, septiembre 2005, 2.

V. La publicidad ilícita

Los responsables de las plataformas no deben realizar publicidad que induzca a error, engaño o confusión. Sin embargo, no se agota allí: también tienen el deber de actuar para evitar que otros publiciten en forma indebida dentro de ellas.

Ello tiene su regulación en:

a) La Ley de Lealtad Comercial (art. 9), que la define en los siguientes términos: “Queda prohibida la realización de cualquier clase de presentación, de publicidad o propaganda que mediante inexactitudes u ocultamientos pueda inducir a error, engaño o confusión respecto de las características o propiedades, naturaleza, origen, calidad, pureza, mezcla, cantidad, uso, precio, condiciones de comercialización o técnicas de producción de bienes muebles, inmuebles o servicios”.

b) La Ley de Defensa del Consumidor (art. 8), que aclara que obliga al proveedor y se tiene por incluida en el contrato.

c) En el CCCN (art. 1101) se mencionan distintos supuestos de publicidad prohibida. Allí menciona los supuestos en los que “a. contenga indicaciones falsas o de tal naturaleza que induzcan o puedan inducir a error al consumidor, cuando recaigan sobre elementos esenciales del producto o servicio;

b. efectúe comparaciones de bienes o servicios cuando sean de naturaleza tal que conduzcan a error al consumidor;

c. sea abusiva, discriminatoria o induzca al consumidor a comportarse de forma perjudicial o peligrosa para su salud o seguridad”.

A su vez, el art. 1102 del Código Civil y Comercial les otorga a los consumidores la posibilidad de solicitar “la cesación de la publicidad ilícita, la publicación, a cargo del demandado, de anuncios rectificatorios y, en su caso, de la sentencia condenatoria”. Se ha sostenido que la información en este ámbito también previene, en cuanto colabora a evitar que se cometan fraudes publicitarios⁽¹⁴⁾.

Lo importante no es la intención, sino la posibilidad de que lleve a error, engaño o confusión⁽¹⁵⁾.

En las Jornadas Nacionales de Derecho Civil celebradas en 2024 se concluyó por unanimidad: “El deber de brindar trato digno y no discriminatorio obliga a las plataformas a adoptar mecanismos que habiliten al consumidor a conocer los parámetros utilizados para el direccionamiento publicitario a fin de que puedan modificarlos; a conocer los sistemas de recomendación de información, y a poner a su disposición mecanismos que le permitan oponerse a recibir publicidad directa. Este deber se intensifica frente a niños, niñas y adolescentes y otras situaciones de hipervulnerabilidad” (apartado II.7.iii).

Se ha sostenido que la publicidad, en estos casos, no puede valorarse con los estándares habituales, sino que corresponde adoptar una menor rigidez, analizando las circunstancias en concreto y teniendo en cuenta que la mayoría de la gente no es minuciosa ni analítica frente a los anuncios publicitarios⁽¹⁶⁾.

Es posible la prevención en estos supuestos.

Se ha ordenado cesar la publicidad ilícita: a) frente al anuncio de una bebida (agua saborizada H2O) que puede llevar a error y no cumple con el Código Alimentario⁽¹⁷⁾; b) a una empresa que comercializa cervezas y realizó una publicidad de su producto junto al de otra marca, aumentando con “efecto lupa” las etiquetas, lo que puede inducir al consumidor a una equivocación sobre sus características y composición⁽¹⁸⁾; y c) a un medio televisivo que publicó un aviso con personas en posturas obscenas, que ofrecían servicios sexuales, teniendo en cuenta que

pueden acceder a ella niños y adolescentes en etapa de formación⁽¹⁹⁾.

Ello es extensible a las plataformas.

VI. Vías para prevenir

1. En general

Si bien el art. 1711 del CCCN contempla a la “acción preventiva”, no se hace referencia al tipo de proceso aplicable. Esta tarea queda a criterio de las provincias, aunque la mayoría todavía no han adecuado sus normativas⁽²⁰⁾.

Ello conlleva discusiones respecto a la vía que corresponde utilizar. Muchos códigos procesales contemplan el juicio ordinario para los supuestos en que no exista otro aplicable. Aquí entendemos que es indispensable la utilización de un proceso acotado (ya que la prevención no siempre es apremiante, pero tampoco amerita tanta demora) y pueden ser útiles herramientas para los procesos urgentes como la medida autosatisfactiva o la tutela anticipada⁽²¹⁾.

Debe recordarse, además, que la Corte Nacional ha sostenido que los jueces deben tener en cuenta la urgencia en este tipo de pretensiones y que para ello “deben encauzar los trámites por las vías expeditivas y evitar que el rigor de las formas pueda conducir a la frustración de derechos que hoy cuentan con particular tutela constitucional, lo cual se produciría en el caso si el reclamo efectuado por la actora tuviese que aguardar a la resolución del referido juicio ordinario y en ese lapso quedarán sin protección alguna los intereses cuya satisfacción se requiere en estos autos”⁽²²⁾.

Ello sin perjuicio de la posibilidad de dictar mandatos preventivos, que pueden ser indispensables en algunos supuestos.

2. En materia de consumo

Tradicionalmente los autores propusieron distintas vías para hacer efectiva la prevención en este ámbito: algunos pensaban que era necesario recurrir al amparo, debido a la carencia de precisiones puntuales del texto normativo⁽²³⁾, mientras que otros se fundaban en el daño temido⁽²⁴⁾.

Hoy en día, esta función se encuentra regulada de modo general en el Código Civil y Comercial y sus previsiones son plenamente aplicables a los casos fundados en la Ley de Defensa del Consumidor.

En la normativa de consumo se prevé la aplicación del proceso más abreviado para los consumidores, salvo que el juez, por la complejidad de la cuestión, considere necesario tramitar un procedimiento de conocimiento más adecuado (art. 53). Aquí se evitan las discusiones sobre el proceso a utilizar en estos casos.

Sin embargo, en algunos supuestos puede suceder que las circunstancias aconsejen adoptar otra modalidad (por ejemplo, medidas autosatisfactivas o tutela anticipada).

El mandato preventivo cobra especial importancia en el ámbito de consumo, debido a que se extiende a otros posibles afectados en un futuro⁽²⁵⁾.

(19) CNCiv., Sala I, 4/11/2003, “R.R., A. c. Diario Clarín S.A. y otros”, La Ley Online 2004-E, 278.

(20) Se ha regulado en el art. 3, ap. II, inc. 5 del Código Procesal Civil, Comercial y Tributario de Mendoza y el art. 299 del Código Procesal Civil y Comercial de Santa Cruz.

(21) Nos remitimos al tratamiento del tema en Lo Giudice, Diego A., “Análisis de las conclusiones de las XXVI Jornadas Nacionales de Derecho Civil sobre prevención del daño”, El Derecho, diarios de los días 16, 17 y 18 de mayo de 2018, ISSN 1666-8987, Nros. 14.407, 14.408 y 14.409, Año LVI, ED 277.

(22) CSJN, 6/2/2001, “Guckenheimer, Carolina Inés y otros c/ Kleiman, Enrique y otro”, Fallos: 324:122, considerando 8. En el mismo sentido: CSJN, 9/6/2009, “Rivero, Gladys Elizabeth s/ amparo/apelación”, Fallos: 332:1394; CSJN, 8/6/2004, “Martín Sergio Gustavo y otros c/ Fuerza Aérea Argentina Dirección General Bienestar Pers. Fuerza Aérea s/Amparo”, Fallos: 327:2127.

(23) Echevesti, Carlos, “El servicio público. Los derechos del usuario. La motorización por la vía del amparo y la reciente ley de protección al consumidor”, Jurisprudencia Argentina 1994:885.

(24) Mosset Iturraspe, Jorge – Lorenzetti, Ricardo, *Defensa del consumidor*, ed. Rubinzal-Culzoni, Santa Fe, 1994, pág. 385.

(25) Entre otros: CCC Azul, sala II, 11/11/2015, “Biordo Miguel Ángel c/ Rutas al Sur Concesionario Vial s/ daños y perjuicios”, Microjuris MJJU-M-95745-AR, MJ95745; CCC 4° de Córdoba, 28/4/2016, “M., M. M. E. c. Empresa Provincial de Energía de Córdoba (EPEC) - Ordinario - Daños y perj. - Otras formas de respons. extracontractual - Recurso de apelación”, Expte. N° 1279260/36, La Ley Online, AR/JUR/19592/2016. Se le ha impuesto a una plataforma en JCC 10 de Córdoba, “Berrondo Lion, Valeria Elisa c/ Booking.Com Argentina S.R.L. - Abreviado - Cumplimiento/Resolución de contrato - Trám. oral”, Expte. 11667667.

(14) Ondarcu, José I., “La prevención del daño en el derecho del consumidor. Análisis, en particular, de la acción de cesación de la publicidad ilícita como mecanismo preventivo”, La Ley 22/04/2022, I, Responsabilidad Civil y Seguros 2022-IV, 24, La Ley Online AR/DOC/1302/2022.

(15) Chamatropulos, Demetrio A., *Estatuto del derecho del consumidor comentado*, Buenos Aires, La Ley, 2016, e-book, Biblioteca Proview, comentario al art. 8, ap. III.1.

(16) Quaglia, Marcelo C., “Realidades de la industria 4.0: vulnerabilidad y publicidad”, La Ley 22/10/2021, I, RCCyC 2021 (diciembre), 21, TR LALEY AR/DOC/2961/2021.

(17) CNPenal Económico, Sala B, 19/8/2005, “Redonhelo S.A.”, Jurisprudencia Argentina 2005-IV-349, La Ley Online AR/JUR/5726/2005.

(18) CFed. Civ. y Com., Sala I, 19/5/2005, “Cervecería y Maltería Quilmes c. Casa Isenbek”, Responsabilidad Civil y Seguros 2005-489.

Son frecuentes las medidas cautelares en distintos supuestos: a) en casos de *phishing*, desconocimiento de consumos de tarjetas o cobros indebidos se suele pedir que no se informe como deudor al consumidor, que no se le realicen débitos o se reintegren, según el caso, etc.⁽²⁶⁾; b) para que se reajusten o no se incrementen cuotas de planes de autoahorro o créditos; c) a veces –de modo excepcional– mediante medidas innovativas para que se devuelva el monto descontado; entre otros.

(26) Hemos tratado el tema en Dauverné, Julián S. – Lo Giudice, Diego A., “La problemática del phishing en contratos de consumo de servicios financieros por plataformas electrónicas”, La Ley 12/2/2025, 6. En la jurisprudencia, puede verse: CNCom., sala F, 18/10/2024, “Schwarzkopf, Caterina c. HSBC Bank Argentina S.A. y otro s/ Medida precautoria”, La Ley 19/11/2024, 8, La Ley 18/12/2024, 6, La Ley Online AR/JUR/155183/2024.

VII. Conclusiones

La prevención del daño ha tenido una notable importancia en el derecho del consumidor. El comercio actual por medio de plataformas aumenta la vulnerabilidad y, por lo tanto, es indispensable una mayor protección.

VOCES: DERECHO COMERCIAL - COMERCIANTE - ACTOS DE COMERCIO - CONTRATOS COMERCIALES - TECNOLOGÍA - INFORMÁTICA - INTERNET - CÓDIGO CIVIL Y COMERCIAL - RESPONSABILIDAD CIVIL - RESPONSABILIDAD SUBJETIVA - DAÑOS Y PERJUICIOS - OBLIGACIÓN DE SEGURIDAD - JURISPRUDENCIA - DERECHOS DEL CONSUMIDOR - OBLIGACIONES - COMUNICACIONES ELECTRÓNICAS - ABUSO DEL DERECHO - COMERCIO ELECTRÓNICO - MULTA - DAÑO PUNITIVO - E-COMMERCE

La responsabilidad derivada de daños causados por productos digitales: una necesaria revisión de conceptos

por VERÓNICA ELVIA MELO^(*)

Sumario: 1. INTRODUCCIÓN. — 2. MARCO CONCEPTUAL. 2.1. ¿QUÉ SON LOS BIENES DIGITALES? 2.2. NATURALEZA JURÍDICA. — 3. RÉGIMEN DE RESPONSABILIDAD EN EL DERECHO ARGENTINO. — 4. PRODUCTOS Y SERVICIOS DIGITALES: ¿LAGUNA LEGAL? 4.1. ADAPTAR LA NOCIÓN DE PRODUCTO. 4.2. REVISAR EL CONCEPTO DE PROVEEDOR. 4.3. REVISAR LA NOCIÓN DE DEFECTO. — 5. CONCLUSIONES.

1. Introducción

El impacto de la tecnología en la dogmática jurídica es innegable, a la vez que atraviesa un enorme espectro de temas, como, por ejemplo, la protección de datos personales, los delitos informáticos, la incidencia de la tecnología en el ofrecimiento y producción de las pruebas en juicio, contratos informáticos, responsabilidades derivadas de la inteligencia artificial, entre tantos más. Como sostiene Hernández, coexisten problemas clásicos que requieren de una necesaria relectura, junto a nuevas realidades que obligan a pensar el derecho en términos de innovación⁽¹⁾.

En consecuencia, el traslado de las relaciones jurídicas al entorno digital interpela al derecho a repensar ciertos conceptos. Concretamente, las relaciones de consumo han cambiado notablemente, y aparecen bienes y servicios de naturaleza muy diferente de la tradicional, como, por ejemplo, una app para el teléfono celular, el servicio de streaming para acceder a contenido audiovisual, entre otros. En este sentido, la responsabilidad por bienes y servicios digitales merece una reflexión sistemática.

En este trabajo, procuraremos abordar las nociones de producto, servicio, proveedor, defectos, desde la perspectiva de la digitalización de las relaciones jurídicas.

2. Marco conceptual

2.1. ¿Qué son los bienes digitales?

El concepto de patrimonio ha experimentado una transformación sustancial, que involucra los bienes materiales y que en la actualidad abarca también el patrimonio digital.

Esta nueva noción de patrimonio digital refleja una realidad dinámica que está en constante evolución y comprende un acendrado conjunto de activos intangibles que exhiben la presencia de cada persona en el ciberespacio. De esta manera, el patrimonio digital engloba los archivos multimedia, documentos electrónicos, perfiles en redes sociales, activos financieros digitales, fotografías, vídeos, correos electrónicos, blogs, así como muchos otros elementos que representan nuestra existencia en el mundo online. Este nuevo contexto es más que una simple acu-

mulación de datos, se trata de la materialización de nuestra actividad en un formato digital⁽²⁾.

Constituido este patrimonio digital, su abordaje jurídico presenta desafíos que van desde la protección de datos hasta la necesidad de diseñar instrumentos jurídicos adecuados que permitan regular las problemáticas que, cada vez con más frecuencia, se producen en este tipo de bienes.

En breve, el patrimonio digital se compone del conjunto de activos y elementos que una persona va acumulando a lo largo de su vida en el contexto digital y que tienen un valor. Así, a diferencia del patrimonio tradicional, que está compuesto de una diversa gama de bienes materiales, el patrimonio digital lo conforman archivos y datos que, al estar en un formato digital, ostentan una naturaleza intangible. En este sentido, la Carta de la UNESCO sobre la preservación del patrimonio digital establece que el patrimonio digital “consiste en recursos únicos que son fruto del saber o la expresión de los seres humanos. Comprende recursos de carácter cultural, educativo, científico o administrativo e información técnica, jurídica, médica y de otras clases, que se generan directamente en formato digital o se convierten a éste a partir de material analógico ya existente. Los productos de ‘origen digital’ no existen en otro formato que el electrónico”⁽³⁾.

Y una vez definidos los bienes digitales, corresponde clasificarlos en dos categorías: por un lado, los bienes digitales puros (por ejemplo, software descargable, servicios en la nube) y, por otro, los bienes digitales incorporados (el software incorporado a un robot aspiradora)⁽⁴⁾.

2.2. Naturaleza jurídica

La naturaleza jurídica de estos activos intangibles está sujeta a debate, y no contamos con doctrina o jurisprudencia nacional que pueda zanjar la cuestión. El interrogante sería si se trata de bienes o de servicios.

El reciente fallo norteamericano “García v. Character Technologies”⁽⁵⁾ genera un precedente relevante en esta materia. Los hechos relevantes pueden sintetizarse como sigue: la actora, Megan García, era la madre del adolescente Sewell Setzer, quien se suicidó luego de interactuar con el chatbot de Character Technologies Inc. empresa demandada (juntamente con sus fundadores, Google LLC y Alphabet Inc.). La pretensión de la actora consistió en un reclamo de indemnización por productos defectuosos, negligencia, daño emocional intencional, homicidio culposo y violaciones a la ley de prácticas comerciales desleales de Florida. La demandada argumentó que no se trata de un producto, sino de un servicio de expresión amparado por la garantía constitucional de la libertad de expresión. El tribunal resolvió que el chatbot desarrollado por la demandada puede ser considerado un producto a los fines de la aplicación de la normativa que regula la responsabilidad por productos defectuosos. Si bien se trata de una resolución preliminar, se abre la puerta para la aplicación del régimen de responsabilidad objetiva que impera en materia de responsabilidad por productos defectuosos.

Este asunto refleja la complejidad de la calificación jurídica de estas tecnologías, especialmente cuando interactúan activamente con los usuarios.

3. Régimen de responsabilidad en el derecho argentino

En el derecho argentino, el marco normativo para la responsabilidad por productos lo encontramos en los ar-

NOTA DE REDACCIÓN: Sobre el tema ver, además, los siguientes trabajos publicados en *EL DERECHO: Comercio electrónico y relaciones de consumo*, por EMILIANO CARLOS LAMANNA GUINAZÚ, ED, 225-989; *Estafa por medios electrónicos. Análisis del art. 173, inc. 16 (ley 26.388). Crítica. Manipulación informática. Estafas cometidas vía Internet*, por GUSTAVO JUAN VANINETTI y HUGO ALFREDO VANINETTI, ED, 223-776; *La protección de los datos personales en Internet: lineamientos que caben deducirse del fallo de la Corte Suprema*, por ESTEBAN RUIZ MARTÍNEZ, ED, 260-861; *Responsabilidad civil en internet: avance de las nuevas tecnologías de la información y asignaturas pendientes del sistema jurídico*, por MARCELO OSCAR VUOTTO, ED, 261-860; *Los contratos electrónicos de consumo en el derecho argentino*, por JOHN GROVER DORADO (h.), ED, 270-641; *Régimen jurídico de un sitio web. Identificación. Contenidos. Responsabilidades civiles derivadas de internet*, por HORACIO FERNÁNDEZ DELPECH, ED, 273-799; *Luces y sombras en un nuevo pronunciamiento de la Corte Suprema de Justicia de la Nación respecto de la responsabilidad civil de los buscadores de internet*, por GUSTAVO ARIEL ATTA, ED, 275-521; *El carácter de la responsabilidad del operador de sitio de e-commerce*, por RITA CASTIGLIONI y NICOLÁS MOFFAT, ED, 278-25; *El actuar de los “cazadores de ofertas” en la compraventa electrónica y la figura del abuso del derecho*, por JUAN IGNACIO CRUZ MATTERI, ED, 304; *Responsabilidad de las plataformas de comercio electrónico frente al consumidor*, por MARÍA EUGENIA D’ARCHIVO, ED, 305. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) Abogada (UCA). Magíster en asesoramiento jurídico de empresas (Universidad Austral). Especialista en derecho de la alta tecnología (UCA). Doctora en Derecho (Universidad Nacional de Rosario). Docente de grado y de posgrado. Directora de la carrera de especialización en derecho de daños (UCA Rosario).

(1) Hernández, Carlos, “El derecho del consumidor en los entornos digitales”, TR LALEY AR/DOC/1656/2021.

(2) Cucurull Poblet, Tatiana, “Más allá de lo tangible: la herencia de los activos digitales”, *Revista Claves Jurídicas* N° 13, enero-junio 2024, pp. 49-67, ISSN 3020-1608.

(3) Artículo 1 de la Carta de la UNESCO sobre la preservación del patrimonio digital, https://unesdoc.unesco.org/ark:/48223/pf0000229034_spa (consultado el 2/6/2025).

(4) Arnau Raventos, Lidia, “Bienes y elementos digitales: ¿dos mundos aparte?”, Universidad de Barcelona, 2021. Recuperado de <https://dialnet.unirioja.es/descarga/articulo/8103851.pdf>

(5) García v. Character Technologies, Inc., No. 6:24-cv-01903, (M.D. Fla. 2024), <https://www.courtlistener.com/docket/69300919/garcia-v-character-technologies-inc/> (consultado el 20/5/2025).

títulos 1092 a 1122 del Código Civil y Comercial, que abordan los contratos de consumo, y en la ley 24.240 que establece un régimen de responsabilidad objetiva para el supuesto en análisis. Asimismo, el artículo 1757 del CCyC establece la responsabilidad objetiva por el daño causado por el riesgo o vicio de las cosas y actividades riesgosas o peligrosas, dentro de las que encontramos los daños causados por productos elaborados.

Análogamente a lo que sucedía en el Código Civil, el actual Código Civil y Comercial no regula expresamente los daños causados por productos defectuosos. Se mantiene, con algunas modificaciones, el régimen de vicios redhibitorios⁽⁶⁾ y el sistema de responsabilidad objetiva por la intervención de cosas, derivadas de su riesgo y vicio⁽⁷⁾.

Por otro lado, el régimen previsto en la Ley de Defensa del Consumidor no se ha visto alterado por la normativa del CCyC.

En el marco del estatuto consumeril, se considera producto a toda cosa que resulta de un proceso de industrialización, que implica introducir en la materia prima transformaciones de alguna índole⁽⁸⁾.

La doctrina y jurisprudencia nacional ha tratado al vicio o defecto del producto como sinónimos. “Vicio es un defecto de la cosa, de fabricación (u originario) o sobreviniente (desgaste, cansancio de materiales, mal o excesivo almacenamiento, rotura, etc.), que la hace impropia para su destino normal o funcionamiento regular”⁽⁹⁾. Es decir, una cosa es viciosa cuando presenta un defecto de fabricación, de funcionamiento, de conservación o de información, que la tornan inepta para la función a que está destinada de acuerdo con su naturaleza.

Siguiendo la taxonomía de defectos que desarrolla Jalil⁽¹⁰⁾, el producto elaborado resulta vicioso o defectuoso cuando presenta:

a) un defecto de diseño, que puede ocurrir en la fase inicial, en la de elaboración del prototipo o en la de revisión del diseño;

b) un defecto de fabricación, esto es, cuando deviene de una falla humana o mecánica generada durante el proceso de fabricación en sentido estricto o en la fase de controles intermedios o final;

c) un defecto de conservación, que sobreviene por incumplimiento de las normas y pautas que atienden al mantenimiento del producto en estado apto durante la etapa que transcurre entre su fabricación y su consumo;

d) un defecto de información, que, si bien es extrínseco al producto elaborado, tiene esencial incidencia en la generación o potenciación de riesgo.

e) un defecto por publicidad engañosa, que se configura cuando se afirma alguna cualidad impropia del producto que puede derivar en daño para el potencial consumidor.

El rasgo común es que estas anomalías importan la introducción de un riesgo en el medio social, sea por tornar riesgoso a un producto que no lo es ni por naturaleza ni por modo de empleo, sea por potenciar su peligrosidad intrínseca⁽¹¹⁾.

Así, los legitimados pasivos en una acción de responsabilidad por daños causados por productos elaborados serán el productor, el fabricante, el importador, el distribuidor, el proveedor, el vendedor y quien haya puesto su marca en la cosa o servicio⁽¹²⁾. Por su lado, el actor deberá demostrar los cuatro presupuestos de la responsabilidad civil. Merece especial atención la relación de causalidad, pues la doctrina es unánime al sostener que solo ha de resultar inexcusable cuando se muestre el nexo causal suficiente entre el daño y la ausencia o deficiencia del control

debido⁽¹³⁾. El nexo causal que habrá de acreditarse es el que surge entre el producto defectuoso y el daño, aunque en el proceso de daños bastará con la de presunciones para establecer ese vínculo causal, toda vez que juega la teoría de la carga probatoria dinámica⁽¹⁴⁾.

Con relación a los servicios —que en el ecosistema digital se aplicaría a streaming, almacenamiento en la nube, etc.—, la ley 24.240 ordena en su artículo quinto que “Las cosas y servicios deben ser suministrados o prestados en forma tal que, utilizados en condiciones previsibles o normales de uso, no presenten peligro alguno para la salud o integridad física de los consumidores o usuarios”⁽¹⁵⁾.

4. Productos y servicios digitales: ¿laguna legal?

Ya es un lugar común sostener que la actual normativa del CCyC y de defensa del consumidor puede presentar dificultades a la hora de su aplicación para obtener el resarcimiento de daños causados por productos o servicios en el marco de la economía circular y digital. En particular, algunas características de la IA dificultan identificar las personas potencialmente responsables, probar el defecto del producto y la relación de causalidad que vincula la actuación del posible responsable con el daño producido⁽¹⁶⁾. Estas dificultades, unidas a otras características de la IA, dan lugar a que determinados aspectos de la actual regulación de la responsabilidad por productos defectuosos sean insuficientes o inapropiados⁽¹⁷⁾.

En tal sentido, postularemos en esta parte de este trabajo la necesidad de ampliar la noción de producto, fabricante y defecto, a los fines de facilitar la tutela del damnificado en el ámbito de los productos digitales defectuosos.

4.1. Adaptar la noción de producto

Hemos ya enunciado que, en el ámbito de tutela al consumidor, se considera producto a toda cosa que resulta de un proceso de industrialización, que implica introducir en la materia prima transformaciones de alguna índole. Así, este concepto de producto se ciñe a los bienes muebles, incluidos los que se han incorporado a un mueble o inmueble, y a la electricidad. En este sentido, podría sostenerse que el software instalado en una cosa mueble (por ejemplo, en una máquina), que permanece inalterable y que no se actualiza, puede ser considerado como parte integrante de la máquina y, por lo tanto, como producto. No obstante, resulta vidrioso si el damnificado puede reclamar contra el desarrollador de dicho software como fabricante de un componente y cuál es el régimen jurídico del software que se instaló o actualizó después de la puesta en circulación del producto⁽¹⁸⁾. El Tribunal de Justicia de la Unión Europea se ha pronunciado en el sentido de que los datos como tales no son productos⁽¹⁹⁾.

A los fines de adecuar la normativa a las necesidades que plantea el auge de los bienes y servicios digitales, es menester ampliar la noción de producto para que queden comprendidos los productos con elementos digitales, tanto si incluyen contenidos como si incluyen servicios digitales, siempre que sean imprescindibles para que los elementos en los que se incorporen o con los que estén interconectados puedan desempeñar sus funciones⁽²⁰⁾. Sin embargo, se discute en la doctrina europea si la definición del nuevo producto debe incluir los datos o no⁽²¹⁾.

(13) Galdós, Jorge M., “Responsabilidad extracontractual del Estado en la Corte Suprema de la Nación. Principales pautas directrices”, *Revista Derecho de Daños*, Rubinzal-Culzoni, Santa Fe, 2000, t. 9, p. 63.

(14) Sagarna, Fernando, “Responsabilidad civil. Doctrinas esenciales VI”, *La Ley*, Buenos Aires, 2007, p. 455.

(15) Ver <https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/638/textact.htm> (consultado el 1/6/2025).

(16) Martín Casals, Miquel, “Desarrollo tecnológico y responsabilidad extracontractual. A propósito de los sistemas de inteligencia artificial (IA)”, en José María Pérez Collados (Coord.), “La cultura jurídica en la era digital”. Cuadernos digitales Derecho y Nuevas Tecnologías, Aranzadi, 2022, pp. 101-138.

(17) “Liability rules for artificial intelligence”, https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en (consultado el 23/5/2025).

(18) Fairgrieve, D.; Howells, G.; Mogelvang Hansen, P.; Straetmans, G. y otros, “Product Liability Directive”, en P. Machnikowski (Editor), *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*, Intersentia, 2016, pp. 17-108.

(19) Martín Casals, M., cit., p. 126.

(20) Ídem.

(21) La European Law Institute Response, p. 12, se manifiesta en contra de la extensión de la noción de producto a los Datos, “Commission Guidelines on the Application of the Definition of an AI System and the Prohibited AI Practices Established in the AI Act”, <https://www.>

(6) Arts. 1051 y subsiguientes del Código Civil y Comercial de la Nación.

(7) Arts. 1757 y 1758 del Código Civil y Comercial de la Nación.

(8) Jalil, Julián, “Los productos elaborados y la responsabilidad por daños en el estatuto del consumo. Incidencias del nuevo Código Civil y Comercial en el campo resarcitorio”, Cita: TR LALEY AR/DOC/5081/2015.

(9) “Calvo de Cuttini, Carmen v. Pepsi-Cola de Argentina S.A.”, RCyS 2000-381, con nota de Fernando Alfredo Sagarna.

(10) Jalil, J., cit.

(11) Ídem.

(12) Conforme lo ordena la Ley de Defensa del Consumidor: Artículo 40. – Si el daño al consumidor resulta del vicio o riesgo de la cosa o de la prestación del servicio, responderán el productor, el fabricante, el importador, el distribuidor, el proveedor, el vendedor y quien haya puesto su marca en la cosa o servicio. El transportista responderá por los daños ocasionados a la cosa con motivo o en ocasión del servicio, <https://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/638/textact.htm> (consultado el 1/6/2025).

La Directiva (UE) 2024/2853 del Parlamento Europeo y del Consejo contempla en su considerando número trece: “Los productos en la era digital pueden ser tangibles o intangibles. Los programas informáticos, como los sistemas operativos, los microprogramas, los programas de ordenador, las aplicaciones o los sistemas de IA, son cada vez más comunes en el mercado y desempeñan un papel cada vez más importante para la seguridad de los productos. Los programas informáticos pueden introducirse en el mercado como productos autónomos o, posteriormente, pueden integrarse en otros productos como componentes, y pueden causar daños al ejecutarse. En aras de la seguridad jurídica, debe aclararse en esta Directiva que los programas informáticos son un producto a efectos de la aplicación de la responsabilidad objetiva, independientemente de su modo de suministro o uso, y, por tanto, con independencia de si el programa informático está almacenado en un dispositivo, se accede a él a través de una red de comunicaciones o tecnologías en la nube o se suministra a través de un modelo de programa informático como servicio. Sin embargo, la información no debe considerarse un producto, por lo que las normas sobre responsabilidad por productos defectuosos no deben aplicarse al contenido de los archivos digitales, como los archivos multimedia o los libros electrónicos o el mero código fuente de los programas informáticos. Un desarrollador o productor de programas informáticos, incluidos los proveedores de sistemas de IA en el sentido del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, debe ser tratado como un fabricante⁽²²⁾. Y el mismo documento, en el artículo cuarto establece: “A los efectos de la presente Directiva, se entenderá por: 1) «producto»: cualquier bien mueble, aun cuando esté incorporado a otro bien mueble o a un bien inmueble o interconectado con estos; incluye la electricidad, los archivos de fabricación digital, las materias primas y los programas informáticos⁽²³⁾”.

Con relación a la responsabilidad del fabricante del bien, debería ser irrelevante si el contenido digital se instaló antes o después de la puesta en circulación del bien tangible, siempre que su funcionalidad dependa de este contenido digital⁽²⁴⁾. El fabricante de bienes con elementos digitales también debería estar alcanzado por la responsabilidad objetiva cuando el daño causado por el contenido digital proporcionado por un tercero si dicho contenido digital es esencial para el correcto funcionamiento de tales bienes.

Por lo demás, considerando que cada vez es más frecuente que los servicios digitales estén interconectados con un producto de tal forma que la ausencia del servicio impediría que el producto realizara alguna de sus funciones (por ejemplo, el suministro continuo de datos de tráfico en un sistema de navegación) es necesario extender la responsabilidad objetiva a dichos servicios digitales, ya que determinan la seguridad del producto tanto como los componentes físicos o digitales. Dichos servicios conexos deben considerarse componentes del producto al que están interconectados cuando están bajo el control del fabricante de ese producto, en el sentido de que son suministrados por el propio fabricante o que el fabricante los recomienda o influya de otro modo en su suministro por parte de un tercero⁽²⁵⁾.

La creciente e irreversible digitalización de las relaciones jurídicas torna inadecuado el concepto de producto para la aplicación del régimen de la responsabilidad objetiva. La evolución normativa que representa la redefinición de producto en el marco de la directiva aludida parece necesaria para garantizar una tutela jurídica efectiva de los derechos de los consumidores frente a los riesgos derivados de la interacción entre elementos físicos y digitales, y constituye un paso necesario hacia la adecuación del régimen de responsabilidad civil a las exigencias del entorno digital contemporáneo.

4.2. Revisar el concepto de proveedor

El artículo 2 de la ley 24.240 define al proveedor como “la persona física o jurídica de naturaleza pública o

privada, que desarrolla de manera profesional, aun ocasionalmente, actividades de producción, montaje, creación, construcción, transformación, importación, concesión de marca, distribución y comercialización de bienes y servicios, destinados a consumidores o usuarios”.

Sin embargo, en el caso de los bienes digitales, la cadena de producción y distribución no finaliza en un momento determinado y puede involucrar sujetos responsables que no se mencionan en la letra de la ley. Así, en el régimen de la responsabilidad por productos actual hay materias primas que se utilizan para fabricar componentes que, a su vez, se utilizan para fabricar productos terminados que se colocan en el mercado en un momento determinado en el que el productor pierde el control del producto⁽²⁶⁾.

A diferencia de esto, los bienes digitales suelen interactuar con otros productos y servicios, y los datos circulan de un producto a otro del producto o hacia los consumidores, en ambas direcciones. Estos otros productos y servicios pueden ser operados por otros productores o proveedores de servicios, y la interconexión no se detiene cuando el producto se comercializa porque su funcionamiento requiere actualizaciones periódicas y un flujo continuo de datos⁽²⁷⁾.

En este sentido, parecería más adecuada la noción de “operador económico” que contempla la directiva mencionada en su artículo cuarto, inciso quince: “15) «operador económico»: todo fabricante de un producto o componente, prestador de un servicio conexo, representante autorizado, importador, prestador de servicios logísticos o distribuidor⁽²⁸⁾”.

4.3. Revisar la noción de defecto

Hemos dicho que la doctrina y la jurisprudencia nacional asimilan las nociones de vicio y defecto, entendiendo que una cosa es viciosa cuando presenta un defecto de fabricación, de funcionamiento, de conservación o de información, que la tornan inepta para la función a que está destinada de acuerdo con su naturaleza.

Sin embargo, muchos bienes digitales están sujetos a actualizaciones periódicas no solo para mejorar su utilidad, sino también para mejorar su seguridad. Esta particularidad parece indicar que la responsabilidad del proveedor debería extenderse más allá del momento de la puesta en circulación del bien digital. En esta línea, el artículo siete de la directiva (UE) 2024/2853 ya aludida establece: “Carácter defectuoso 1. Un producto se considerará defectuoso cuando no ofrezca la seguridad que una persona tiene derecho a esperar y que se exige asimismo en virtud del Derecho de la Unión o nacional. 2. Al valorar el carácter defectuoso de un producto, se tendrán en cuenta todas las circunstancias, incluso: a) la presentación y las características del producto, incluidos su etiquetado, diseño, características técnicas, composición y envase, y las instrucciones de montaje, instalación, uso y mantenimiento; b) el uso razonablemente previsible del producto; c) el efecto en el producto de toda capacidad de seguir aprendiendo o adquirir nuevas características después de su introducción en el mercado o puesta en servicio; d) el efecto razonablemente previsible en el producto de otros productos de los que se pueda esperar que se utilicen junto con el producto, también mediante interconexión; e) el momento en que el producto fue introducido en el mercado o puesto en servicio o, si el fabricante conserva el control sobre el producto después de ese momento, el momento en que el producto dejó de estar bajo el control del fabricante; f) los requisitos de seguridad del producto pertinentes, incluidos los requisitos de ciberseguridad pertinentes para la seguridad; g) cualquier retirada del producto o cualquier intervención pertinente relacionada con la seguridad de los productos por parte de una autoridad competente o de un operador económico contemplado en el artículo 8; h) las necesidades específicas del grupo de usuarios finales a los que se destina el producto; i) en el caso de un producto cuya finalidad sea precisamente evitar daños, el eventual incumplimiento de dicha finalidad por parte del producto. 3. Un producto no se considerará defectuoso por la única razón de que un producto mejor, incluidas las actualizaciones o mejoras para un producto, ya se haya introducido

europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Response_on_the_definition_of_an_AI_System.pdf (consultado el 1/6/2025).

(22) Ver <https://www.boe.es/doue/2024/2853/L00001-00022.pdf> (consultado el 30/5/2025).

(23) Ídem.

(24) Martín Casals, M., cit., p. 127.

(25) Ídem.

(26) Twigg Flesner, Christian, “Guiding Principles for Updating the Product Liability Directive for the Digital Age”, ELI Innovation Paper Series, 2021, p. 6.

(27) Twigg Flesner, C., cit., p. 5.

(28) Ver <https://www.boe.es/doue/2024/2853/L00001-00022.pdf> (consultado el 30/5/2025).

en el mercado o puesto en servicio, o se introduzca en el mercado o se ponga en servicio posteriormente”⁽²⁹⁾.

En definitiva, la calificación de un producto como vicioso, tradicionalmente vinculada a los defectos enumerados *supra*, debería reformularse desde la perspectiva de las características de los bienes digitales. La directiva europea mencionada podría ser una fuente de consulta para el legislador nacional por cuanto incorpora elementos como la capacidad del producto para actualizarse, requisitos de ciberseguridad y control posterior a su ingreso en el mercado, en consonancia con las razonables expectativas de seguridad del consumidor digital.

5. Conclusiones

La sociedad contemporánea se rehúsa a aceptar los daños que se derivan de las nuevas tecnologías digitales como si fueran un designio inevitable. En orden a no interferir en el desarrollo de los sistemas de inteligencia artificial, parece necesario elevar los estándares de seguridad aplicables a ellos, a fin de preservar la confianza de los usuarios y prevenir, en la medida de lo posible, los eventuales daños que pudieran derivarse de su funcionamiento.

(29) Ver <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022PC0496> (consultado el 30/5/2025).

En el orden jurídico vigente, la responsabilidad por productos elaborados nos desafía a revisar sus fundamentos clásicos, para hacer lugar al principio de precaución, que se torna especialmente relevante ante la incertidumbre y los riesgos que entrañan estas nuevas tecnologías.

A lo largo de este trabajo, nos hemos referido a la novel normativa europea, que amplía el concepto de “producto” para incluir software y archivos digitales, y flexibiliza la carga probatoria en favor del consumidor, admitiendo la notoria dificultad de demostrar el nexo causal en entornos tecnológicos complejos. Así, el principio precautorio se convierte en una pieza clave para anticipar y mitigar los riesgos asociados a la innovación digital, reforzando la función preventiva y reparadora del derecho de daños.

VOCES: DERECHO COMERCIAL - COMERCIANTE - ACTOS DE COMERCIO - CONTRATOS COMERCIALES - TECNOLOGÍA - INFORMÁTICA - INTERNET - CÓDIGO CIVIL Y COMERCIAL - RESPONSABILIDAD CIVIL - RESPONSABILIDAD SUBJETIVA - DAÑOS Y PERJUICIOS - OBLIGACIÓN DE SEGURIDAD - JURISPRUDENCIA - DERECHOS DEL CONSUMIDOR - OBLIGACIONES - COMUNICACIONES ELECTRÓNICAS - ABUSO DEL DERECHO - COMERCIO ELECTRÓNICO - MULTA - DAÑO PUNITIVO - E-COMMERCE

Inteligencia artificial explicable (AIX) y prevención de daños

por MATILDE PÉREZ^(*)

Sumario: I. INTRODUCCIÓN. – II. LAS CAJAS NEGRAS O BLACK BOX. – III. SALIR DE LA OPACIDAD. LA BÚSQUEDA DE UNA IA EXPLICABLE. – IV. ¿QUÉ ES LA INTELIGENCIA ARTIFICIAL EXPLICABLE (XAI)? – V. PRINCIPIOS APLICABLES A LA IAE. – VI. LA IAE COMO INSTRUMENTO DE GESTIÓN DE RIESGOS ANTE LA INCERTIDUMBRE. – VII. HERRAMIENTAS Y MÉTRICAS PARA UNA INTELIGENCIA ARTIFICIAL MÁS CONFIABLE. – VIII. CONCLUSIÓN.

I. Introducción

En ocasión de celebrar el 10º aniversario de la entrada en vigor del Código Civil y Comercial, la organización de las XXX Jornadas Nacionales de Derecho Civil continúa la línea de las cuatro últimas jornadas respecto del derecho de daños y las tecnologías.

Es en este sentido que la vorágine de las innovaciones tecnológicas requiere de los operadores jurídicos especial atención en lo que hace a áreas tan sensibles como la libertad, la autonomía de la voluntad o la centralidad de la dignidad humana.

En esta Era 4.0 la colaboración y transversalidad entre el Derecho y otras ciencias es una realidad que trasunta todas las áreas del conocimiento y hace que las tecnologías basadas en sistemas de IA deban ser analizadas desde el desarrollo de su diseño hasta su posterior utilización.

En esta oportunidad, el abordaje propuesto por las XXX Jornadas de Derecho Civil en la Comisión 3 es el de “Daños derivados de productos, servicios y bienes digitales” afirmación que coloca a estas nuevas realidades en la órbita jurídica de la responsabilidad civil.

En la vida cotidiana, los productos digitales son bienes intangibles que se producen, almacenan y distribuyen en formato digital. El software, los libros electrónicos, música, videos, cursos, plantillas, entre muchos otros, se caracterizan por su inmediatez, su fácil uso y formatos accesibles.

Los servicios digitales son actividades o funcionalidades ofrecidas a través de plataformas o redes digitales. Almacenamiento en la nube, redes sociales, software como servicios (SaaS) o programas de streaming requieren de una conexión de acceso a internet, pueden ser personalizadas de acuerdo con las necesidades del usuario y, por lo general, se obtienen por suscripciones sean pagas o gratuitas.

El concepto de bienes digitales comprende aquellos objetos virtuales que se pueden comprar, vender o coleccionar en línea. Se representan, por lo general, en tokens

no fungibles (NFT) y en criptoactivos. Entre los más conocidos, las criptomonedas, activos digitales, arte digital o el mundo del metaverso.

Se percibe de manera más o menos consciente la existencia de estas realidades, así como la presencia de la inteligencia artificial en los distintos sistemas que se valen de ella o servicios y productos que se desarrollan o utilizan la IA, que transforman la sociedad, las formas de pensar, de relacionarse o cómo realizar las tareas más simples o complejas.

Si esa percepción se transforma en pregunta acerca de cómo la IA funciona, cómo se crea, cómo se aplica, quiénes están detrás o qué pasa si la IA se equivoca o no sabe, la mayoría ignora o tiene un conocimiento somero o superficial al respecto.

Quizás, en muchos casos, la persona se queda con la cara amable en el ahorro de tiempo, la disponibilidad de información o el acceso a bienes y servicios. Sin embargo, hay situaciones en áreas como la sanidad o el uso de datos en que parecen mostrar lo contrario, pues se presentan situaciones como discriminación, sesgos negativos o tomas de decisiones por estos sistemas difíciles de explicar o comprender.

Y es que estos modelos de IA impactan en un amplio abanico de cuestiones tan dispares como la solicitud de un préstamo, el dictado de un acto administrativo, una praxis médica o el ingreso universitario.

La propuesta de este trabajo es analizar posibles soluciones a los problemas conocidos como de *cajas negras* o *black box* en los que hay una dificultad de interpretar y comprender cómo un modelo de IA llega a una determinada conclusión que se verá reflejada en el espectro de los productos, servicios o bienes digitales, con la posibilidad de generar daños de entidad y extensión diversas.

Esa búsqueda se enmarca en la función preventiva del daño a través de sus principios integradores, a los que se agrega la posibilidad de pensar en una IA explicable (IAE o AIX) o cómo desde el diseño del producto se puede anticipar la existencia de dañadores tecnológicos y así contribuir a la seguridad jurídica, la protección de los usuarios, los consumidores y los proveedores, así como ser parte de la gobernanza de los Estados.

II. Las cajas negras o *black box*

Existen sistemas algorítmicos basados en lenguajes de aprendizaje automático o *machine learning* en los que no se sabe con certeza cuáles son los mecanismos que realizan para llegar a un resultado, esto es, las llamadas cajas negras o *black box*.

Estos fenómenos se engloban dentro de los defectos de diseño y, por tanto, con potencialidad nociva desde su desarrollo inicial.

En estas situaciones, el sistema actúa como una red neuronal en la que es muy difícil poder determinar cómo se llega a determinados resultados.

Este aprendizaje automático presenta varios modelos: a) *Supervised learning* o aprendizaje supervisado en el que el sistema está entrenado con conjuntos de datos estructurados para predecir resultados de manera precisa. b) *Reinforcement learning* o aprendizaje de refuerzo que es un sistema entrenado a base de prueba de error sin contar con un conjunto de datos. c) *Deep learning* o aprendizaje profundo. El sistema debe ser entrenado en un conjunto masivo de datos, millones de datos; este entrenamiento puede ser estructurado o no estructurado, sin necesidad de intervención humana para el procesamiento de tales datos. d) Redes neuronales profundas. El diseño de diagramas neuronales cada vez más extensos requiere de un sistema que permita garantizar la transparencia de tales procesos.

En el *machine learning* se da la posibilidad de “aprender” sin haber programado de una manera explícita. Se basa en la identificación de patrones sobre los *inputs* y la aplicación subsiguiente del “conocimiento”.

A mayor autonomía del sistema se advierte una mayor falta de transparencia y accesibilidad con relación a las predicciones y soluciones a las que llegan estos sistemas.

El estado de los conocimientos científicos se topa con nuevos contextos de incertidumbre que nacen de cómo se autoprocesan los algoritmos y se abocan a sus soluciones;

NOTA DE REDACCIÓN: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: *Las “tecnologías reproductivas” y la ética médica*, por ELISABET AGUSTINA VIDAL, ED, 259-913; *Responsabilidad civil en internet: avance de las nuevas tecnologías de la información y asignaturas pendientes del sistema jurídico*, por MARCELO OSCAR VUOTO, ED, 261-860; *El nuevo Código Civil y Comercial y el rol de nuestra formación jurídica*, por MARIO A. ZINNY, ED, 263-870; *El Código Civil y Comercial en clave de derechos humanos. El impacto del derecho internacional de los derechos humanos en la aplicación e interpretación del nuevo derecho privado argentino*, por MARCELO TRUCCO, ED, 264-810; *El uso de la tecnología y la gestión de la comunicación en la mediación actual*, por JUAN FERNANDO GOUVERT, ED, 275-771; *El derecho ante la inteligencia artificial y la robótica*, por VERÓNICA ELVIA MELO, ED, 276-493; *La protección de los datos personales en internet (una tarea ineludible)*, por ESTEBAN RUIZ MARTÍNEZ, ED, 284-726; *La comunidad humana en la era tecnológica*, por LEONARDO PUCHETA, ED, 282-1044; *Robótica e inteligencia artificial: nuevos horizontes de reflexión*, por LEONARDO PUCHETA, ED, 283-925; *Los paradigmas del derecho privado codificado. El caso argentino: de persona a individuo*, por GABRIEL F. LIMODIO, ED, 286-461; *El concepto de persona frente a las tecnologías disruptivas: persona humana, persona jurídica, ¿persona electrónica?*, por VERÓNICA ELVIA MELO, ED, 289-1386; *Derecho de los robots*, por PILAR MOREYRA, ED, 291-708. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(*) Doctora en Ciencias Jurídicas. Especialista en Derecho Administrativo. Directora del Centro de Innovación Jurídica UCA. Profesora titular de las asignaturas Obligaciones Civiles y Comerciales, Derecho de Daños y Derechos Reales en la Facultad de Derecho de la Universidad Católica Argentina. Profesora en el Doctorado en Ciencias Jurídicas y en la Maestría de Derecho Civil Patrimonial, miembro del Comité Asesor del Doctorado en Ciencias Jurídicas y miembro de la Comisión de Abogacía Digital (UCA). Profesora invitada en Universidades nacionales y extranjeras. Subdirectora del Suplemento “Derecho, Innovación y Desarrollo Sustentable” en Editorial El Derecho. Autora de libros, capítulos de libros y ponencias. Correo electrónico matildeperez@uca.edu.ar. Código ORCID 009-0008-2189-701X.

sin embargo, la probabilidad dañosa existe, está presente el “humor de peligro” que debe mover a todos los operadores a canalizar alternativas para lograr que esos efectos nocivos derivados de las decisiones adoptadas en estos contextos impacten lo menos posible.

En idéntico sentido, al determinarse la responsabilidad por los daños causados por el uso de estas tecnologías, no puede argumentarse como eximente de la responsabilidad la existencia de un caso fortuito interno o la falta de conocimiento científico.

III. Salir de la opacidad. La búsqueda de una IA explicable

Esas mejoras reconocen en la trazabilidad y la transparencia dos mecanismos esenciales tanto desde la perspectiva del estudio de la relación costo-beneficio como desde la función preventiva de daños, los servicios de atención al cliente y la disminución de efectos negativos de carácter masivo como aquellos que provienen de los casos fortuitos internos, respecto a la transparencia, seguridad y confiabilidad de las decisiones automatizadas.

Ante este panorama, la *inteligencia artificial explicable* adquiere una relevancia primordial, puesto que permite acercarse al procesamiento de datos interno de los algoritmos para tornarlos comprensibles y evitar decisiones discriminatorias o perjudiciales, por lo que es una herramienta que encuadra en las disposiciones de los arts. 1710, 1711 y 1712 del CCC.

Los algoritmos basados en IA, en especial, las redes neuronales profundas tienen una mayor presencia en cada tarea cotidiana debido al incremento del uso del aprendizaje profundo o *deep learning*.

En sectores como la salud, finanzas y justicia, la IA explicable garantiza que las decisiones automatizadas sean comprensibles y justificadas, evitando daños derivados de interpretaciones erróneas o falta de transparencia⁽¹⁾.

IV. ¿Qué es la Inteligencia Artificial Explicable (XAI)?

La inteligencia artificial explicable (IAE o XAI por su sigla en inglés) se orienta a transparentar los procesos internos y las lógicas de decisión de los algoritmos. Esto implica que, en lugar de operar como *cajas negras*, los sistemas de IA deben ofrecer mecanismos de interpretación que posibiliten a desarrolladores, usuarios y autoridades comprender, auditar y supervisar sus decisiones.

La explicabilidad se torna en un principio que busca entender y comprender cómo los sistemas llegan a esas decisiones.

El término IAE fue acuñado por el Proyecto DARPA⁽²⁾ en 2016 destinado a solucionar la falta de transparencia y el entendimiento de los sistemas de IA, en especial, en aplicaciones militares.

Promueve un conjunto de herramientas tecnológicas y algorítmicas que puedan brindar explicaciones de alta calidad, interpretables e intuitivas para los seres humanos.

Esa explicabilidad debe estar dirigida a asegurar que la decisión adoptada por estos sistemas no es sesgada, es antidiscriminatoria y los procesos de carga de datos están atravesados por la buena fe.

Se pretende evitar la existencia de una relación de causalidad entre la *caja negra* y el daño, dado que al ser explicable las personas pueden evaluar cómo sus datos son utilizados y tomar decisiones acerca de ellos o de su privacidad.

Aun así, pueden existir brechas o grietas acerca de la manera en que la transparencia y la explicabilidad afectarán la confianza pública o si tales sistemas pueden ser dirigidos de manera dolosa como una mera formalidad.

Es por ello que la IAE debe partir de la detección de sesgos algorítmicos que son considerados como errores sistemáticos y estructurados en un sistema de IA que generan desigualdades y resultados injustos. La existencia de *cajas negras* es, como se dijo, un defecto de diseño que ni los desarrolladores pueden explicar con fiabilidad porque se desconoce cómo se llega a ese sesgo.

La IAE tiene que abrir un camino para facilitar el reconocimiento y la concientización precisa de posibles sesgos entre las diversas partes interesadas en ese ecosistema de IA para lograr la anticipación o mitigación de estos agentes con potencialidad dañosa.

Ir hacia *cajas blancas* o *cajas de cristal* es parte del derecho a la explicación por el que la persona titular de datos tiene el derecho a la explicación de la decisión tomada después de la evaluación algorítmica, esto es, la información significativa sobre la lógica involucrada en las decisiones automatizadas⁽³⁾.

En el caso de las empresas ubicadas en la jurisdicción de la Unión Europea, solo pueden tomar determinadas decisiones siempre que puedan brindar explicaciones de cómo se llega a esa decisión para que sean más visibles y fáciles de detectar al revelar qué está haciendo el sistema y cómo llega a sus decisiones⁽⁴⁾.

En esta búsqueda de *cajas blancas*, la explicabilidad es una necesidad inherente a los seres humanos que se vincula con la percepción y la cognición, esto es, una expresión de que todos los seres humanos por naturaleza tienden al saber.

Y es allí donde acude la puesta en marcha de estudios de espectro de usuarios donde la experiencia personal sustituya o complementa a las técnicas de computación o evaluaciones basadas en la funcionalidad, en especial, en materia de sesgos y discriminación. Las investigaciones sin referencias en lo humano no logran contextualizar la IAE como mecanismos para eliminar la opacidad de los modelos.

Esa incorporación de la perspectiva humana se centra, primero, en la incorporación de expertos como desarrolladores de IA o usuarios profesionales como en el caso de los profesionales de la salud con relación a las herramientas de IA para el diagnóstico, en áreas de cibercrimen o en el desarrollo de sistemas para la toma de decisiones judiciales, a modo de ejemplo⁽⁵⁾.

No obstante, pareciera que los usuarios que no son expertos son los que se pueden ver más afectados por las decisiones de la IA y con preocupaciones legítimas sobre trato injusto por parte del sistema.

Este es un punto clave para que la transparencia, la responsabilidad y la explicabilidad de la IA se centre en el ser humano como viene propugnándose en los diversos textos internacionales.

Los estudios de usuarios en materia de IAE deben partir de la *interpretabilidad*, esto es, la capacidad del sistema para explicar o presentar predicciones del modelo en términos que puedan ser entendidos por las personas.

Las explicaciones comprensibles, las interfaces accesibles y las interacciones centradas en el usuario permiten convertir a la IAE en una herramienta de ayuda a los usuarios para comprender por qué se deriva –o no– un resultado de un sistema, cuándo puede tener éxito o fallar o cuándo confiar en el sistema o saber que cometió un error⁽⁶⁾.

V. Principios aplicables a la IAE

El Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos establece cuatro principios claves de la IAE como método para garantizar que los sistemas de IA sean transparentes, comprensibles y confiables para los usuarios⁽⁷⁾.

[3] Selbst, A.; Powles, J., “Meaningful information and the right to explanation”, *Proceedings of 1st. Conference on Fairness, Accountability and Transparency*, PMLR, 81, p. 48, 2018. Disponible en selbst18a.pdf, consultado el 05/06/2025.

[4] Y. Rong et al., “Towards Human-Centered Explainable AI: A Survey of User Studies for Model Explanations”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 46, no. 4, pp. 2104-2122, abril 2024. Disponible en <https://ieeexplore.ieee.org/abstract/document/10316181>, consultado el 05/06/2025.

[5] Ching-Hua, Ch., Ruoyu, S.; Shiyun, T.; Wan-Hsiu, S., “Explainable Artificial Intelligence (XAI) for facilitating recognition of algorithmic bias: An experiment from imposed users’ perspectives”, *Telematics and Informatics, Revue*, Volume 91, 2024, 102135. Disponible en <https://www.sciencedirect.com/science/article/pii/S073658532400039X>, consultado el 05/06/2025.

[6] Gunning, D.; Aha, D., “DARPA’s Explainable Artificial Intelligence (XAI) Program”, *AI Magazine*, 40(2), 2019, pp. 44-46. Disponible en <https://doi.org/10.1609/aimag.v40i2.2850>, consultado el 05/06/2025.

[7] Phillips, J.; Hahn, C. et al., *NISTIR 8312 Four Principles of Explainable Artificial Intelligence*. National Institute of Standards and Technology, septiembre 2021. Disponible en <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8312.pdf>, consultado el 05/06/2025.

[1] González-Arencibia, M.; Ordoñez-Erazo, H.; González-Sanabria, J., “Explainable Artificial Intelligence as an Ethical Principle”, *Rev. Ingeniería*, N° 29, vol. 2, dic. 2024. Disponible en <https://doi.org/10.14483/23448393.21583>, consultado el 05/06/2025.

[2] DARPA. Defense Advance Research Project Agency. Información adicional disponible en <https://onlinelibrary.wiley.com/doi/epdf/10.1609/aimag.v40i2.2850>, consultado 04/06/2025.

1. Transparencia y comprensibilidad: A través de ellos se puede ir hasta el diseño del sistema con el objeto de poder detectar errores, sesgos o comportamientos no previstos.

2. Detección anticipada de riesgos: En los procesos de toma de decisiones automatizadas la gestión de los riesgos permite abaratar costos directos, pero también evitar daños presentes como la detección de sesgos y daños futuros generados por el uso indebido de datos personales por estos sistemas, riesgos de desarrollo de producto detectado como daño tardío o, a través de la información y el lenguaje claro, contribuir a que los ciudadanos conozcan cómo operar determinados sistemas.

3. Responsabilidad y consentimiento informado: Con la transparencia proporcionada por la XAI, tanto reguladores como responsables internos pueden evaluar críticamente los procesos automatizados, lo que favorece la rendición de cuentas y la adaptación de medidas correctivas en tiempo real.

4. Fortalecimiento de la confianza: Al hacer comprensible el algoritmo, se fomenta la confianza de todos los actores involucrados –desde clientes hasta organismos reguladores– en que los sistemas se gestionan de manera ética y segura.

VI. La IAE como instrumento de gestión de riesgos ante la incertidumbre

En el derecho de daños, el análisis de los riesgos y su gestión en contextos de incertidumbre permite acceder al control de la causalidad y, así, controlar la posibilidad de producción de daños masivos.

El despliegue de sistemas de IAE contribuye a identificar anomalías o sesgos discriminatorios en fases tempranas de los ciclos de IA, lo que permite la puesta en marcha de estrategias que tiendan a evitar la opacidad de los modelos.

Posibilita la evaluación continua y la adaptación a las nuevas normativas por cuanto la transparencia que hace a la esencia de la IAE facilita una revisión constante automatizada y humana de los algoritmos, lo que permite actualizar protocolos de actuación, marcos de autorregulación y adaptaciones legislativas.

El hacer públicos los mecanismos de decisión es un aliciente para los desarrolladores y operadores para procurar una mejora en los estándares de integridad y seguridad acudiendo a medidas de prevención y técnicas de *compliance*, lo que también puede contribuir a resultados más satisfactorios en auditorías y evaluaciones externas.

En paralelo, se presentan varias dificultades.

La complejidad técnica en el desarrollo de algoritmos potentes y transparentes requiere de mayores inversiones en investigación, desarrollo y capacitación que no siempre están en condiciones de ser soportadas o sus costos se trasladan a los productos y servicios.

La vertiginosidad de los sistemas de IA débil y fuerte, la competencia del mercado, la falta de estándares universales y marcos normativos tan dispares como el Reglamento General de Protección de Datos o el Reglamento de IA de la Unión Europea o la aplicación de normativas generales atentan contra una IAE segura y responsable.

Desde los aspectos computacionales pueden presentarse situaciones en las que la explicabilidad puede comprometer la eficiencia o la precisión del sistema, por lo cual debe establecerse el balance entre un diseño explicable de la IA y la puesta en marcha del sistema en forma autónoma o como soporte.

Es entonces que la colaboración entre los organismos públicos, el sector privado y los expertos se erige como uno de los baluartes en la búsqueda de mecanismos sin opacidades en sistemas complejos.

VII. Herramientas y métricas para una inteligencia artificial más confiable

Desde hace más de cien años es una constante el recurrir a diversos mecanismos de *soft law* y, dentro de ellos, la autorregulación que desarrolla y armoniza un sistema de referencias propias y vinculantes para quienes las suscriben frente a la burocracia o la inoperancia estatal⁽⁸⁾.

Bajo este paraguas de la autorregulación, el Observatorio de Políticas de Inteligencia Artificial de la OCDE recopila y comparte diversas herramientas y métricas diseñadas para ayudar a los diversos actores de la IA a desarrollar sistemas confiables que respeten los derechos humanos, que sean transparentes, explicables y seguros⁽⁹⁾.

Se destacan dos metodologías:

1. Local Interpretable Model-agnostic Explanations (LIME) permite aproximar modelos complejos con versiones más simples y que se puedan interpretar para explicar predicciones de tipo individual de una manera rápida.

2. SHapley Additive exPlanations (SHAP) que cuantifica la contribución exacta de cada variable de entrada a una predicción para lo que utiliza principios de la gamificación o teoría de los juegos. Es mucho más precisa que la anterior, pero tiene un costo mayor.

Uno de los ámbitos en los que se procura la implementación de estos modelos para la IAE es el de diagnóstico médico que puede contribuir, por ejemplo, a interpretar que la edad y la presión arterial de un paciente pueden ser los principales factores que concluyen en un diagnóstico de algo riesgo de infarto, aunque SHAP explicaría de manera exacta cómo contribuye cada variable.

En el caso de una entidad bancaria, se puede implementar un sistema de aprendizaje profundo para la detección de fraude, y usar valores SHAP para auditar sus decisiones y garantizar que no se toman decisiones discriminatorias.

Existen otras propuestas que combinan el uso de datos abiertos con sistemas de IAE debido a su interconectividad, lo que permite entonces potenciar la transparencia, la confianza y la responsabilidad en la toma de decisiones basadas en IA.

VIII. Conclusión

La *inteligencia artificial explicable* representa una herramienta poderosa para la gestión de riesgos, en tanto que su capacidad para clarificar y verificar el proceso de toma de decisiones se alinea estrechamente con el *principio de precaución*. Este enfoque permite anticipar vulnerabilidades y prevenir daños en entornos donde la incertidumbre y la complejidad tecnológica pueden desembocar en consecuencias indeseadas.

De cara al futuro, es crucial fomentar la colaboración interdisciplinaria y el desarrollo normativo que encauce la innovación hacia prácticas seguras, éticas y transparentes. La sinergia entre XAI y el principio de precaución no solo fortalece la confianza del usuario, sino que también contribuye a construir sistemas de IA que, lejos de ser cajas negras, sean mecanismos abiertos al escrutinio y la mejora continua.

VOCES: PERSONA - TECNOLOGÍA - INFORMÁTICA - TRATADOS INTERNACIONALES - DERECHOS HUMANOS - CÓDIGO CIVIL Y COMERCIAL - DERECHO CIVIL - RESPONSABILIDAD CIVIL - DAÑOS Y PERJUICIOS - INTELIGENCIA ARTIFICIAL - ORDEN PÚBLICO - PERSONAS JURÍDICAS - PRINCIPIOS GENERALES DEL DERECHO - INTERNET - PODER JUDICIAL - DERECHOS Y GARANTÍAS CONSTITUCIONALES - RESPONSABILIDAD DEL GUARDIÁN - RESPONSABILIDAD OBJETIVA

(8) Pérez Álvarez, M., *El principio de precaución y los riesgos de desarrollo*, Buenos Aires, El Derecho, 2024, pp. 143-155.

(9) OECD.AI. *Policies, data and analysis for trustworthy artificial intelligence*, julio 2024. Disponible en <https://oecd.ai/en/>, consultado 05/06/2025.

Arquitecturas que manipulan: culpa estructural y tutela reforzada de los vulnerables en el ecosistema digital.

A propósito de TikTok y Robinhood

por FERNANDO ALFREDO UBIRÍA

Sumario: 1. LA LÓGICA ECONÓMICA DE LA MANIPULACIÓN ALGORÍTMICA. – 2. LA “DECISIÓN” SOBRE EL MODELO DE NEGOCIO COMO FUNDAMENTO DE IMPUTACIÓN JURÍDICA. – 3. EL APOORTE DE LA “CULPA ESTRUCTURAL” COMO SUSTENTO AXIOLÓGICO Y PRESUPUESTO DE ATRIBUCIÓN DE RESPONSABILIDAD. – 4. QUID SOBRE LA VIRTUALIDAD DEL CUMPLIMIENTO DE “PROTOCOLOS”. – 5. LA DIFICULTAD PROBATORIA DEL NEXO CAUSAL. – 6. LIBERTAD DE EMPRESA VS. SALUD PÚBLICA. – 7. CONCLUSIONES.

1. La lógica económica de la manipulación algorítmica

Los principios de “no dañar a otro” y de “buena fe”, aplicados en materia de responsabilidad por productos, servicios y bienes digitales, imponen proteger especialmente a los sujetos vulnerables como, por ejemplo, niños y adultos mayores, potenciales víctimas de graves daños, tutela que alcanza tanto intereses individuales (plano de lesiones psicofísicas, pérdida de autonomía, perjuicios económicos, etc.) como colectivos o difusos (distorsión de hábitos sociales, impacto en la salud pública, manipulación de datos masivos, etc.).

Sin mengua del aliento de innovaciones tecnológicas, el sistema legal dista de ser riguroso en materia de exigibilidad de adopción de medidas preventivas y cumplimiento de estándares de seguridad, como por ejemplo sucede con: 1) la red social “TikTok” (y otras), cuyos mecanismos de scroll infinito y retroalimentación emocional generan un proceso de absorción progresiva de la atención que puede derivar en trastornos de ansiedad, alteraciones del ritmo circadiano, disminución de la capacidad de concentración y afectación de la autonomía decisional, especialmente los jóvenes; 2) la fintech “Robinhood” (y otras) que al gamificar las inversiones financieras trivializa riesgos sustanciales, con consecuencias como la pérdida de ahorros, el sobreendeudamiento, e incluso –en casos extremos– impactos negativos en la salud mental y social.

Se trata de supuestos que tienen un patrón común: la manipulación algorítmica como estrategia empresarial deliberada de captación y ganancia, arquitectura tecnológica que actúa de forma subrepticia, acumulativa y personalizada que transforma al usuario en objeto de diseño comercial⁽¹⁾.

Nos interpela la tensión existente entre las leyes del mercado y las leyes de la Constitución, la convergencia entre economía y derecho: mientras en las primeras sobresale el afanoso propósito de lucro que actúa como motor

del crecimiento, las segundas imponen el debido resguardo de los derechos fundamentales⁽²⁾.

En el presente trabajo enfocaremos un problema importante del derecho de daños escasamente abordado: los fundamentos axiológicos en que se apoya la disciplina cuando los daños derivan del diseño de arquitecturas digitales que inducen comportamientos previsiblemente nocivos.

2. La “decisión” sobre el modelo de negocio como fundamento de imputación jurídica

El derecho no debe obstaculizar el desarrollo económico, pero sí orientarlo hacia la consecución de fines que respeten los derechos fundamentales y el bien común. Cuando la técnica es opaca cabe visibilizar y transparentar, no hay desarrollo legítimo sin la consecuente responsabilidad.

Las empresas tecnológicas como proveedoras de servicios, al incorporar continuas mejoras en sus plataformas, además de asegurarse el más elevado control o dominio de la causalidad operativa en su praxis (mejora de *know how* como valioso activo intangible), robustecen la previsibilidad de causación de daños injustos. Al practicar el “mapeo de riesgos” de sus actividades, emergen las probables implicancias dañosas que están obligadas a gestionar de manera profesional y eficaz, tanto por imposición legal como por sus propias políticas de *compliance*⁽³⁾.

Se trata de actividades riesgosas cuya prestación responde a determinado “plan de negocio” que define el “apetito de riesgo” empresarial, y –por tanto– fundamenta la imputación de las contingencias dimanantes: como reza la máxima jurídica “donde está el beneficio está la carga” (*ubi emolumentum, ibi onus*)⁽⁴⁾. Se tensa el diálogo economía-derecho, y sin perjuicio de que dominen las reglas del mercado, las leyes brindan protección a los usuarios y consumidores en tanto sujetos vulnerables (art. 42, CN y diversos tratados internacionales).

El sistema jurídico no debe ser cómplice de modelos de negocio que externalizan costos sobre la salud mental, la autonomía o la estabilidad financiera de los usuarios, y en esta materia resulta clave considerar al “principio de precaución” como un pilar central en la construcción jurídica, ya que persigue anticiparse a los problemas⁽⁵⁾.

En este marco y sin perjuicio de que resulta claro que nos encontramos ante un supuesto de “actividad riesgosa” en los términos de los arts. 1757 y 1758 del CCyCom., el carácter estructural y sistémico de los daños que se generan por esta vía excede dicha categorización, incluso en su formulación más amplia, resulta un tecnicismo que tiende a encubrir las dimensiones más profundas del fenómeno.

Aun reconociendo la amplitud y versatilidad del fundamento objetivo basado en el riesgo, la densidad del problema exige una mirada más profunda y conceptualmente rigurosa. Un enfoque diluido no alcanza para dar cuenta de su especificidad ni para ofrecer soluciones jurídicas a la altura del desafío.

NOTA DE REDACCIÓN: Sobre el tema ver, además, los siguientes trabajos publicados en EL DERECHO: Comercio electrónico y relaciones de consumo, por EMILIANO CARLOS LAMANNA GUINAZÚ, ED, 225-989; Estafa por medios electrónicos. Análisis del art. 173, inc. 16 (ley 26.388). Crítica. Manipulación informática. Estafas cometidas vía Internet, por GUSTAVO JUAN VANINETTI y HUGO ALFREDO VANINETTI, ED, 223-776; La protección de los datos personales en Internet: lineamientos que caben deducirse del fallo de la Corte Suprema, por ESTEBAN RUIZ MARTÍNEZ, ED, 260-861; Responsabilidad civil en internet: avance de las nuevas tecnologías de la información y asignaturas pendientes del sistema jurídico, por MARCELO OSCAR VUOTTO, ED, 261-860; Los contratos electrónicos de consumo en el derecho argentino, por JOHN GROVER DORADO (h.), ED, 270-641; Régimen jurídico de un sitio web. Identificación. Contenidos. Responsabilidades civiles derivadas de internet, por HORACIO FERNÁNDEZ DELPECH, ED, 273-799; Luces y sombras en un nuevo pronunciamiento de la Corte Suprema de Justicia de la Nación respecto de la responsabilidad civil de los buscadores de internet, por GUSTAVO ARIEL ATTA, ED, 275-521; El carácter de la responsabilidad del operador de sitio de e-commerce, por RITA CASTIGLIONI y NICOLÁS MOFFAT, ED, 278-25; El actuar de los “cazadores de ofertas” en la compraventa electrónica y la figura del abuso del derecho, por JUAN IGNACIO CRUZ MATTERI, ED, 304; Responsabilidad de las plataformas de comercio electrónico frente al consumidor, por MARÍA EUGENIA D’ARCHIVO, ED, 305. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(1) Los algoritmos están caracterizados por su universalidad y su opacidad, están presentes en todos los ámbitos de nuestras vidas y permanecen ocultos: es imposible saber dónde se encuentran, qué hacen y cuál es su objetivo verdadero, etc. Las grandes empresas de la *world wide web* son reticentes a dar información de este tipo, so pretexto de que se debilitarían los procesos de IA (Colombo, Celeste, “¿La utilización de algoritmos es una actividad riesgosa?”, LL 2019-F-678).

(2) Ubiría, Fernando, “Marco obligacional preventivo en materia de daños derivados de la IA”, en *Estudios de Derecho Privado en homenaje al profesor doctor Jorge H. Alterini*, La Ley Thompson Reuters, 2024, pág. 224.

(3) Ver –entre otros– el trabajo de Domenech, María Mercedes, “Análisis periódico de riesgos de *compliance* y su impacto en un programa de integridad dinámico”, en *Compliance, anticorrupción y responsabilidad penal empresarial*, La Ley, mayo 2018, págs. 267/277.

(4) Ubiría, Fernando, “Estratificación de riesgos y prevención de daños derivados de la IA”, en “Daños derivados de la inteligencia artificial”, edición especial de El Derecho, 23/9/2024, pág. 30. Por lo demás, desde el otro polo de la relación jurídica, la atribución de culpa frente a determinados riesgos no es neutra ni objetiva, obedece o se apoya sobre “patrones culturales” arraigados que tienden a preservar ciertos valores socialmente aceptados.

(5) En esta importante materia se destaca el trabajo de Matilde Pérez El principio de precaución y los riesgos del desarrollo, El Derecho, 2024.

3. El aporte de la “culpa estructural” como sustento axiológico y presupuesto de atribución de responsabilidad

Hace muchos años ya Atilio Alterini advirtió que “los contornos actuales de la responsabilidad civil son la resultante de enormes cambios derivados de la ‘estampida tecnológica’, de su incidencia en el pensamiento de nuestros contemporáneos, que aspiran a la evitación del daño y, en su caso, a que les sea reparado”⁽⁶⁾.

El sombrío escenario de lesividad descripto interpela con intensidad al progresista derecho de daños, que lejos de mostrarse obsoleto ofrece herramientas conceptuales idóneas: los fundamentos de corte subjetivo se erigen en un necesario “contrapeso”, permitiendo al sistema cumplir su función axiológica⁽⁷⁾.

En efecto, el Código Civil y Comercial al establecer criterios subjetivos y objetivos (art. 1721) deja en manos del intérprete la “incardinación”, tarea que cabe definir según de la “naturaleza de la obligación” y en función de las circunstancias de persona, tiempo y lugar (art. 1724).

En este campo, la culpa y el dolo constituyen el basamento más adecuado, ya que permiten identificar con nitidez que el origen del problema reside en una decisión consciente y deliberada: una política empresarial reprochable imputable directamente a la persona jurídica (art. 1763, CCyCom.). Aun cuando los algoritmos operen con autonomía y desarrollen aprendizajes propios, su punto de partida responde a elecciones humanas estratégicas, por tanto, los criterios subjetivos no actúan como un complemento accesorio (“a mayor abundamiento”) sino de manera autónoma.

La arquitectura sistémica se apoya en la culpabilidad *lato sensu* que tiene la profundidad y versatilidad suficientes para dotar de un adecuado fundamento axiológico al sistema preventivo legal en orden a imponer medidas de seguridad y control (arts. 1710 y 961, CCyCom.; arts. 5 y 6, LDC 24.240), mientras que en la dimensión reparatoria actúa como presupuesto de responsabilidad (arts. 1721, 1724/5 y 1728, CCyCom.).

Si un adolescente sufre ansiedad por el uso intensivo de TikTok, es más común que se culpe al joven o a sus padres (“nadie los obligó”) antes que al diseño mismo de la aplicación que lo indujo a ese uso excesivo, y lo mismo ocurre con pequeños inversores que pierden sus ahorros en Robinhood en tanto se los considera ingenuos o irresponsables, sin cuestionamiento alguno del diseño algorítmico que trivializa el riesgo para generar rentabilidad⁽⁸⁾.

Tales aplicaciones (y otras similares) configuran esquemas reprochables de daños previsibles, en muchos casos funcionales a su éxito comercial, configurando un canal de agresión o lesividad no accidental o excepcional sino sistémico⁽⁹⁾.

4. Quid sobre la virtualidad del cumplimiento de “protocolos”

Erigida la culpa como fundamento y criterio de atribución de responsabilidad en esta materia, al resultar vagos

(6) Alterini, Atilio, *Contornos actuales de la responsabilidad civil*, Abeledo, 1987, pág. N° 8.

(7) En la estrategia legislativa existe un *prius* que la UE encaró desde la “gestión del riesgo”, estableciendo una serie de deberes de conducta por parte de los desarrolladores y los responsables del despliegue del producto en el mercado, cuya violación u omisión a la postre es el fundamento de una culpa o de una causalidad presumida (Santarelli, Fulvio, “El camino hacia un sistema de responsabilidad civil de la Inteligencia Artificial. Signaturas pendientes”, La Ley del 23/09/2024, LL 2024-E-96, cita online: TR LALEY AR/DOC/2289/2024).

(8) Desde una perspectiva antropológica, cabe considerar que los riesgos derivados de ciertas plataformas digitales no son neutros ni se distribuyen al azar, su atribución se encuentra moldeada por patrones culturales que tienden a culpabilizar a las víctimas vulnerables antes que a cuestionar las estructuras empresariales que los inducen. Tales construcciones sociales cumplen una función estabilizadora del *statu quo* al preservar valores dominantes y desplazar la responsabilidad desde decisiones sistémicas hacia supuestas fallas individuales. En este marco el derecho debe asumir una función crítica: desnaturalizar esa distribución simbólica de la culpa y poner en evidencia los condicionamientos culturales que legitiman la impunidad de estos modelos de negocio.

(9) Silicon Valley es conocido por lanzar nuevos productos sin considerar necesariamente las implicaciones sociales o éticas: hay una gran prisa por innovar. No obstante, las empresas pueden ejecutar simulaciones regularmente para probar los resultados de sus algoritmos (Mascitti, Matías, “La insuficiencia de la causalidad como presupuesto de la responsabilidad civil en los daños producidos por la robótica y los sistemas autónomos”, en Revista de Derecho Privado N° 42, 2022, pág. 223).

y genéricos los mandatos legales por la naturaleza “abierto” de nuestra “normatividad”, al formularse la comparación entre la conducta obrada y la debida mediante cláusulas generales, principios abiertos y genéricos que desde luego carecen de precisión técnica suficiente, asumen relevancia creciente los “protocolos”, “manuales de buenas prácticas” u otros similares, mandatos formulados desde organismos internacionales o sectoriales que actúan como estándares de autorregulación del sector.

Cabe preguntarse si, en este preciso ecosistema digital, el estricto acatamiento de dispositivos de *soft law* podría considerarse (es decir, categorizar) como “actuación diligente y profesional”, y por tanto pago y extinción obligacional. La respuesta negativa parece imponerse.

En efecto, su cumplimiento no agota el juicio de valor que debe imperar en la materia; se requiere un análisis crítico sobre la verdadera legitimidad y real eficacia del estándar invocado: así la mera “recomendación” de pausar el uso como política resulta claramente insuficiente y abiertamente inconsistente con las estrategias algorítmicas de retención compulsiva; la laxitud con que TikTok permite abrir cuentas, en tanto que, aunque formalmente se establece un umbral etario mínimo de 13 años, no se implementa una verificación robusta de edad ni se exige consentimiento parental para validar el acceso; del mismo modo, los mecanismos de advertencia sobre riesgos financieros se tornan ineficaces cuando las propias aplicaciones otorgan recompensas visuales o sonoras cada vez que el usuario invierte, etc.

Se trata de simulacros de diligencia que no evitan ni mitigan los riesgos estructurales, antes bien constituyen mera apariencias que falsea el estándar requerido en procura de legitimar un modelo de negocios reprochable jurídicamente⁽¹⁰⁾.

5. La dificultad probatoria del nexo causal

El parámetro de la previsibilidad como eje central de la causalidad jurídica cimenta el juicio de imputación de responsabilidad, permite discernir o identificar las probables consecuencias dañosas de una acción u omisión y, en los entornos digitales donde los daños son consecuencia del diseño intencional de plataformas orientadas a la retención compulsiva del usuario, la prueba del nexo causal adecuado se torna especialmente ardua.

Cuando las plataformas estructuran sus servicios precisamente para saturar la atención, estimular la “dopamina digital” y generar consumo compulsivo, el sistema de responsabilidad no puede escudarse en la multicausalidad para eludir el reproche jurídico, debe asumir el desafío probatorio adaptando sus exigencias al carácter sistémico del riesgo involucrado.

Por ejemplo, en el caso de un adolescente con deterioro psicológico, estará precisado a probar no solo que utilizó intensivamente la aplicación, sino que ello constituye la causa adecuada del daño sufrido (art. 1726, CCyCom.), lo que representa un problema, pues la manipulación que opera a través del diseño algorítmico no es transparente ni lineal sino solapada, difusa y progresiva. Bajo formas placenteras y deseadas por el propio usuario y consentida por sus padres (lo que diluye la percepción de riesgo), se debilita la evidencia directa del daño y abre la puerta a múltiples concausas, es decir, a otros factores que pueden haber contribuido al mismo resultado dañoso, como –por ejemplo– antecedentes de trastornos emocionales, dinámicas familiares conflictivas, presiones escolares o sociales, acoso digital, aislamiento postpandemia, etc., variables que concurren para complejizar la acreditación del vínculo causal entre el uso de la plataforma y el daño⁽¹¹⁾.

(10) Cabe defender la transparencia como criterio de decisión de las organizaciones, por ejemplo, a través del incremento de la calidad de un producto y la reducción de los riesgos de daños. Defender este tipo de transparencia no es reducir o anular los controles, sino –en todo caso– no poner la fe en ellos o contentarse con el cumplimiento de un “check-list” (Preziosa, María Marta, “En defensa de la transparencia”, en Revista Cultura Económica, Año XLII, N° 107, junio 2024, pág. 88).

(11) Pretender que los padres deban contrarrestar este poder tecnológico equivale a imponerles una carga desproporcionada, no tienen acceso ni herramientas para desactivar la arquitectura algorítmica ni el conocimiento técnico necesario para neutralizar sus efectos. Los padres actúan muchas veces de buena fe al permitir el uso de aplicaciones que socialmente son legitimadas, masivamente difundidas y en apariencia inofensivas. La confianza en el entorno digital se vuelve un presupuesto razonable, y no puede derivarse de ello la eximición de responsabilidad de quien diseña deliberadamente el daño.

Esta situación exige un ajuste metodológico del estándar probatorio, pues no se trata de probar un vínculo mecánico, inmediato y exclusivo entre uso de plataforma y daño, sino de acreditar el diseño y la lógica funcional del servicio digital como generador de un riesgo previsible y relevante de daño. Aquí la causalidad puede presumirse a partir de criterios de razonabilidad, especialmente en casos de usuarios hipervulnerables⁽¹²⁾.

No cabe exigir una prueba imposible ni ideal, por lo que adquiere preponderancia la prueba indiciaria, la prueba estadística o los estudios de impacto psicofísico masivo, que tendrán valor en tanto demuestren que el diseño de la herramienta tiene capacidad efectiva y sistemática de lesionar, y que esa capacidad se desplegó en el caso concreto.

Es necesario un modelo dinámico y antiformalista de causalidad, orientado por criterios de razonabilidad, previsibilidad y verosimilitud científica.

6. Libertad de empresa vs. salud pública

El amplio reconocimiento económico y social de plataformas como TikTok o Robinhood demuestra que el problema de fondo trasciende lo estrictamente jurídico y se inscribe en una problemática de orden sociocultural.

Cabe desenmascarar un falso dilema: no se trata de elegir entre alentar el desarrollo económico o proteger los derechos, consideramos que el legítimo afán de lucro debe ejercerse dentro de los límites impuestos por la tutela de la dignidad humana, la autonomía personal, la salud y los intereses colectivos, por lo que la innovación tecnológica debe cumplir ciertos estándares éticos y jurídicos mínimos.

En efecto, no se propone aquí deslegitimar el éxito o la utilidad de estas plataformas, ni negar su aporte a la economía digital, sino en todo caso advertir que su sostenibilidad a largo plazo depende también de su compatibilidad con un modelo de desarrollo humano integral que requiere límites normativos claros, temática en la que nos interpela muy especialmente la tutela de los menores de edad⁽¹³⁾.

En esta gesta corresponde apuntalar la dimensión preventiva de la responsabilidad civil, ámbito disciplinar en el que la categoría culpa estructural adquiere un valor estratégico, pues visibiliza que el problema no reside en un “uso anómalo” de una tecnología sino en el diseño jurídicamente reprochable.

Con sustento en el fenómeno de constitucionalización del derecho privado, afirmamos que bajo el escudo de la “libertad de empresa” no se pueden amparar esquemas comerciales abiertamente lesivos para los usuarios y consumidores.

Por lo demás, es también relevante apuntar que la inercia estatal en esta materia no puede justificarse apelando a la “autorregulación del mercado”, sobre el Estado pesa un deber activo e indelegable de protección (art. 42, CN)⁽¹⁴⁾. La ausencia de una intervención regulatoria eficaz alienta

la reproducción de un modelo de negocio tóxico y compromete la legitimidad misma del Estado como garante de un mercado justo y humanamente viable⁽¹⁵⁾.

7. Conclusiones

a) La lógica algorítmica que sustenta a ciertas plataformas digitales como estrategia deliberada de captación y manipulación orientada al lucro exige un enfoque jurídico que priorice la tutela efectiva de los usuarios vulnerables frente al poder de estos actores del ecosistema digital.

b) La imputación debe erigirse sobre la decisión deliberada de adoptar un modelo de negocio que opera manipulando conductas desde el diseño. La responsabilidad surge no de lo que pudo preverse sino de lo que se eligió provocar.

c) La categoría culpa estructural aporta un marco axiológico idóneo para imputar responsabilidad en estos entornos.

d) El cumplimiento formal de protocolos no puede ser considerado actuación diligente, pues la propia estrategia comercial contradice su contenido; los estándares así concebidos devienen simulaciones ineficaces, pues no mitigan riesgos estructurales ni eximen de responsabilidad.

e) La naturaleza solapada y progresiva de los daños generados por ciertas arquitecturas digitales exige superar una visión mecanicista de la causalidad y ajustar el estándar probatorio para admitir el uso de presunciones razonables, indicios estadísticos y criterios de verosimilitud científica.

f) La libertad de empresa no puede erigirse en escudo de prácticas lesivas para la salud psicofísica, la autonomía y la estabilidad económica de los usuarios; el derecho debe establecer límites normativos claros y exigir una intervención estatal activa que proteja bienes jurídicos fundamentales frente a modelos de negocio incompatibles con un desarrollo humano sostenible.

La complejidad que presenta la temática no exime al derecho de su función orientadora, la transforma en un imperativo más urgente. En un ecosistema que convierte a la atención humana en mercancía y normaliza la manipulación algorítmica como estrategia de rentabilidad, corresponde interpelar las decisiones estructurales que configuran estos esquemas comerciales en resguardo de la tutela de los sujetos más vulnerables.

VOCES: DERECHO COMERCIAL - COMERCIANTE - ACTOS DE COMERCIO - CONTRATOS COMERCIALES - TECNOLOGÍA - INFORMÁTICA - INTERNET - CÓDIGO CIVIL Y COMERCIAL - RESPONSABILIDAD CIVIL - RESPONSABILIDAD SUBJETIVA - DAÑOS Y PERJUICIOS - OBLIGACIÓN DE SEGURIDAD - JURISPRUDENCIA - DERECHOS DEL CONSUMIDOR - OBLIGACIONES - COMUNICACIONES ELECTRÓNICAS - ABUSO DEL DERECHO - COMERCIO ELECTRÓNICO - MULTA - DAÑO PUNITIVO - E-COMMERCE

(12) En ciertos supuestos vinculados con productos defectuosos, se admite una presunción del nexo causal cuando el daño es normalmente compatible con el defecto, o incluso cuando el producto forma parte de una misma serie en la que ya se ha constatado un funcionamiento anómalo: esta lógica traslada el análisis desde el hecho puntual hacia patrones estructurales, por lo que resulta particularmente fecunda para abordar escenarios en los que las fallas algorítmicas emergen del diseño o del entrenamiento sistémico, antes que de una decisión humana singular (Santarelli, Fulvio, ob. cit., acáp. N° IV.2 *in fine*).

(13) Ver la completa obra de Bibiana Nieto *Derecho a la intimidad del niño. Alcances de su protección jurídica*, El Derecho, 2021; también, de la misma autora, “El sharenting y el ejercicio de la responsabilidad parental en una prudente resolución judicial”, El Derecho, cita Digital: ED-MMCLXXXII-128.

(14) Ubarri, Fernando, “Estado de Derecho y protección de derechos. Aporte desde la prevención de daños del derecho privado”, *Memorias de 40 años de democracia. Desafíos y logros*, Diego Molea

y María Fernanda Vázquez (compiladores), Universidad Nacional de Lomas de Zamora, 2023, pág. 174.

(15) Desde un ángulo convergente, cabe preguntarse acerca de una tutela de carácter penal (sin perjuicio de la administrativa) en orden a la formulación de una propuesta político criminal incriminadora, que debe erigirse a partir de dos pilares fundamentales: el criterio de precaución frente a riesgos muy importantes o sistémicos y el principio de responsabilidad pro víctima, que prioriza el control del riesgo ante la posibilidad de daños y riesgos que la literatura científica conecta al diseño adictivo de las redes sociales y plataformas; estos diseños adictivos deben ser considerados fuera del riesgo permitido con relación a los menores (sirve de paraguas el art. 5 del Reglamento IA de la UE), y corresponde centrarse muy particularmente en la responsabilidad de las plataformas que usan tales herramientas de IA para conseguir la atención y la constante y compulsiva conexión del usuario (González Tapia, Isabel, “Persuasión algorítmica y adicción tecnológica: las nuevas tabaquerías”, *Revista de Victimología* N° 19/2025, España, págs. 43-76).



XXX JORNADAS NACIONALES DE DERECHO CIVIL, CORRIENTES 25, 26 Y 27 DE SEPTIEMBRE DE 2025
10 AÑOS DE VIGENCIA DEL CÓDIGO CIVIL Y COMERCIAL DE LA NACIÓN



EL DERECHO