Estratificación de riesgos y prevención de daños derivados de la IA

por Fernando Alfredo Ubiría

Sumario: 1. Planteo. – 2. Captación conforme a las reglas generales del CCyC. – 3.Termómetro probabilístico y control de causalidad. – 4. Mapeo de riesgos (estratificación). – 5. Rol y virtualidad de los protocolos.

1. Planteo

La inteligencia artificial (IA) ha emergido como una potente herramienta de desarrollo disruptiva que, no solo desafía los límites técnicos, sino también los marcos jurídicos tradicionales, empezando –por ejemplo– por la falta de comprensión cabal del funcionamiento interno de los algoritmos conocidos como "cajas negras". ¿Qué hacer entonces con esta novedosa tecnología que además se encuentra en plena etapa expansión, causando perplejidad y desconcierto en el mundo entero ante la amenaza de escenarios distópicos?

Al atisbar su impacto en el derecho y vislumbrar la conjunción de factores que interactúan, nos interpela adaptar ciertas bases estructurales de la obligación como fenómeno jurídico-económico y –consecuentemente– del derecho de daños, ámbito dentro del cual la prevención alcanza un lugar protagónico.

En una época signada por la sociedad de consumo, cada vez más individualista, automatizada y desconectada, el desafío reside en alcanzar un equilibrio entre la innovación tecnológica, la protección de los derechos y la seguridad pública.

En efecto, por lo pronto, es un renovado sistema de derecho privado el que recibe a esta aún incipiente tecnología, pues ha evolucionado debido a la influencia del fenómeno constitucionalizador que permitió el demorado rediseño (aún en elaboración) que se centra en la dignidad del ser humano como principio fundante y que se construye desde la ética y la responsabilidad individual y social para dar respuesta en tiempos turbulentos.(1)

Cabe retrotraerse a las XI Jornadas Nacionales de Derecho Civil (Univ. de Belgrano, 1987) para recordar el notable aporte de la doctrina vernácula de la especialidad, que de *lege ferenda* sentó ciertas bases de vanguardia en materia de responsabilidad civil emergente de la informática: consideró que constituye una "actividad "riesgosa" en la que opera un fundamento de atribución objetivo, y que en el ámbito contractual el prestador, en principio, asume una obligación de resultado en que opera una obligación tácita de seguridad por el principio de buena fe(2).

Nos interpela formular algunos aportes constructivos, pues el incesante desarrollo tecnológico exige de manera persistente a la disciplina, que en lo inmediato lo canaliza a través de la elaboración de nuevos estándares de conducta (protocolos) cada vez más exigentes.

2. Captación conforme a las reglas generales del CCyC

El Código Civil y Comercial (CCyC) reformuló y expandió al sistema a partir de su propia identidad, desde su propia "lógica", pues en buena medida se logró gracias a la pérdida de centralidad de los presupuestos "culpabilidad" y "antijuridicidad", necesarios para encumbrar al "daño injusto" como verdadero epicentro.

En efecto, y sobre los principios *aterum non laedere* y buena fe consagrados plenamente en el nuevo texto codificado, se construye la necesaria cultura preventiva, que erige como regla de conducta epicéntrica el deber de prevención legal del art. 1710 del CCyC, aplicable tanto en el ámbito contractual como en el extracontractual(3).

El nuevo texto codificado presenta una ingeniería jurídica moderna, que a partir de los parámetros de la tipología "abierta" o "en blanco" que identifica a la normatividad de la disciplina, brinda una base regulatoria generosa y dúctil para captar de manera adecuada, en términos generales, innovaciones tecnológicas como la IA(4).

Dentro de este marco general, en las jornadas nacionales del año 2019 se ratificó el rumbo que se trazara en el lejano 1987, pues se concluyó –ahora de *lege lata*– que:

1) "una actividad es riesgosa cuando por su propia naturaleza, por los medios empleados o por las circunstancias de su realización, apareciera una significativa probabilidad de riesgo o peligro para terceros, ponderable conforme a una causalidad adecuada";

2) son ejemplos la utilización de algoritmos, las actividades cibernéticas, las plataformas digitales y los sistemas operados por la IA;

3) ante la dificultad de pronosticar el derrotero de estas actividades en el futuro, la interpretación debe ser dúctil, abierta, genérica y flexible, con capacidad de adaptarse porque se corresponde con el espíritu dinámico del CCyC y con el sistema de responsabilidad civil vigente(5).

Desde esta perspectiva, resulta menester incursionar en materia de "responsabilidad por el hecho de las cosas y de las actividades riesgosas" (arts. 1757/8, CCyC)(6), y en el marco de este trabajo es menester subrayar que el sistema impone de manera invariable la adopción de conductas evitatorias conforme a cierto estándar o patrón (es decir, de todo sujeto se espera siempre un determinado comportamiento).

Es oportuno recordar ya que, de manera muy rigurosa, la ley dispone que "No son eximentes la autorización administrativa para el uso de la cosa o la realización de la actividad, ni el cumplimiento de las técnicas de prevención" (art. 1757 *in fine*, CCyC) y que "En caso de acti-

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. Todos los artículos citados pueden consultarse en www.elderechodigital.com.ar.

(1) Ubiría, Fernando, *Derecho de daños en el Código Civil y Comercial de la Nación*, Abeledo Perrot, 2015, págs. 3/8.

(2) La fuerza de este claro posicionamiento alentó a modificar las bases estructurales de un sistema de responsabilidad que pasó de ser un mero mecanismo reparatorio a convertirse en el vigoroso y progresista sistema derecho de daños actual (Ubiría, Fernando, "Cambios de paradigmas en el Derecho de Daños. Hacia un nuevo salto de calidad", en *Estudios de Derecho Civil con motivo del Bicentenario*, El Derecho, 2011, pág. 363).

(3) Conclusión de *lege lata* de las JNDC desarrolladas en la Universidad Nacional de La Plata en el año 2017 (XXVI), comisión N° 4: "Derecho de daños: función preventiva y sancionatoria de la responsabilidad civil".

(4) La reformulación de los parámetros centrales de la especialidad tiene como objetivo impostergable brindar una respuesta eficaz, decisión de política legislativa que videncia la saludable influencia del derecho constitucional y el derecho internacional de los derechos humanos [Ubiría, Fernando, "Estado de Derecho y protección de derechos. Aporte desde la prevención de daños del derecho privado", en *Memorias de 40 años de democracia. Desafíos y logros*, Diego Molea y María Fernanda Vázquez (compiladores), UNLZ, 2023, pág. 174; *ídem*, "La prevención desde un doble ángulo: el deber legal de prevención y la tácita obligación de seguridad según el Código Civil y Comercial de la Nación", La Ley, 2018-B-1017].

(5) Conclusión de *lege lata* de las JNDC desarrolladas en la Universidad Nacional de La Plata en el año 2017 (XXVI), comisión N° 4: "Derecho de daños: función preventiva y sancionatoria de la responsabilidad civil".

(6) Colombo, Celeste, "¿La utilización de algoritmos es una actividad riesgosa?", La Ley, 08/11/2019, pág. 3; Pizarro, Daniel y Vallespinos, Gustavo, *Tratado de responsabilidad civil*, t. II, Parte Especial, Rubinzal Culzoni, 2018, págs. 308 y ss.; Zavala de González, Matilde y González Zavala, Rodolfo, *La responsabilidad civil en el nuevo Código*, Alveroni Ediciones, 2018, t. III, págs. 756/758; Alferillo, Pascual, *Código Civil y Comercial comentado. Tratado exegético*, La Ley, 3.ª ed., t. VIII, págs. 442/459.

vidad riesgosa o peligrosa responde quien la realiza, se sirve u obtiene provecho de ella, por sí o por terceros…" (art. 1758 *in fine,*CCyC).

Cabe entonces subrayar que el carácter riesgoso de una actividad lo determina la "significativa probabilidad de riesgo o peligro" para terceros, que debe ponderarse según criterios de "causalidad adecuada".

3. Termómetro probabilístico y control de la causalidad

De lo apuntado, surge notoria la centralidad alcanzada por el factor "probabilidad", es decir, por la "verosimilitud o fundada apariencia" (RAE) en que se presenta o fluye la "amenaza de daño", que por tanto –como "dato duro" (*fact*)– aporta luz desde variables mensurables, confiriendo fundamento a la exigibilidad de medidas preventivas.

Los algoritmos nos convierten en sujetos predecibles, conocen lo que aun nosotros mismos no sabemos que queremos, y es claro que pueden causar daños; no tienen voluntad por sí mismos y carecen de ética, desarrollan sus tareas sin animosidad ni prejuicios, pues son los seres humanos quienes –al crearlos– le transfieren inconscientemente sus sesgos[7].

Se trata de un análisis enmarcado en las reglas de la causalidad adecuada, en tanto se confiere trascendencia jurídica a las consecuencias dañosas que tienen lugar según el "curso natural y ordinario de las cosas" (art. 1727, CCyC).

El parámetro (criterio) de previsibilidad es el eje central de la causalidad jurídica y cimenta el juicio de imputación de responsabilidad; allí anida su fundamento al permitir discernir o identificar las probables consecuencias dañosas de una acción u omisión.

En esta línea, el "termómetro probabilístico" determina –por ejemplo– que en el diseño, utilización de algoritmos y de sistemas de inteligencia artificial deba –ante todo– velarse por su adecuado funcionamiento en términos de seguridad, lo que impone por parte del deudor obligacional una gestión de carácter proactiva. Por ejemplo, la elaboración y estricto cumplimiento de protocolos de evaluación periódica que implique análisis de riesgos, validación de resultados, monitoreo, etc., con un adecuado registro de actividades: medidas técnicas que demuestren la seguridad de los sistemas de IA utilizados en cumplimiento de los estándares más elevados y exigentes.

Desde este plano, resulta exigible la adopción de continuas mejoras en los procedimientos para asegurar el más elevado "control" o "dominio" de la causalidad de la praxis en cuestión que, consecuentemente, genera una mejora del *know how*, valioso activo intangible que robustece la previsibilidad de daños en el desarrollo de actividades peligrosas y que autoriza a aplicar un mayor rigor (estándar) en la ejecución prestacional: queda de manifiesto la interactuación de los presupuestos "daño injusto" y "causalidad adecuada", mientras que el riesgo provecho opera como fundamento de ponderación (que *fluye*, resulte o no exigible legalmente su comprobación).

Algunos ejemplos resultarán ilustrativos: los vehículos autónomos que operan con sistemas de IA presentan riesgos significativos como la posibilidad de fallas en la toma de decisiones en situaciones de emergencia, y así, un error en el procesamiento de datos puede causar un siniestro vial; en materia de diagnóstico médico automatizado, la IA también implica riesgos como un error en la interpretación de imágenes o en la evaluación de síntomas que puede llevar a diagnósticos incorrectos y a tratamientos inadecuados, con potenciales daños al paciente.

En tales casos, las medidas para gestionar profesionalmente dichos riesgos –entre otras– son: 1) evaluación y validación continua a través de la implementación de un proceso riguroso de pruebas de los sistemas de IA, simulando diversas situaciones y escenarios posibles para identificar y corregir posibles fallos; 2) supervisión humana que se considera esencial, incluye la posibilidad de intervenir y tomar el control en caso de que el sistema de IA cometa un error o enfrente una situación inesperada; 3) transparencia y explicabilidad para permitir entender y corregir el comportamiento del sistema en caso de falla, y también para aumentar la confianza en su funcionamiento; 4) cumplimiento normativo y estandarización a través de la adhesión a normativas internacionales, establecer criterios de seguridad específicos para cada aplicación de IA.

En definitiva, en la dinámica y simétrica interrelación objeto-prestación se encuentra una compleja tensión o conflicto: por un lado, la tutela del interés creditorio en cabeza de sujetos generalmente vulnerables; por el otro, el rigor o severidad exigible al deudor en orden a adoptar conductas evitatorias en el desarrollo de la actividad riesgosa.

4. Mapeo de riesgos (estratificación)

Las empresas que se valen de esta tecnología –eventualmente, conformantes de un *pool* de responsables concurrentes– como deudores obligacionales logran –por dicho camino– mejorar el circuito de producción y comercialización de sus productos y servicios: en este trance, practican un "mapeo de riesgos" de sus actividades, alcanzando una comprensión más acabada del negocio y de sus implicancias dañosas que están obligadas a gestionar eficazmente[8].

Los algoritmos procesan grandes volúmenes de datos para identificar patrones y tomar decisiones, por lo que la matemática –y en particular la estadística– juega un papel crucial en materia de causalidad, pues la gestión del riesgo en la IA se apoya en modelos probabilísticos que estiman la ocurrencia de eventos dañosos.

Por esta vía se incrementan la *expertise* y *know how* del negocio, y logran formular una mejor estratificación de los riesgos, una suerte de "semáforo de riesgosidad" que constituye base de gestión profesional de cualquier actividad productiva.

Un claro ejemplo de segmentación con base en tales criterios es la ley del Parlamento de la Unión Europea del 13/3/2024 para quienes desarrollan y/o utilizan sistemas de inteligencia artificial, pues categoriza los riesgos para imponer diferentes requisitos a cada clase (https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf):

1) riesgos inaceptables: se prohíben, por ejemplo, la manipulación subliminal que influye en las decisiones de voto sin el conocimiento del usuario, juguetes con asistentes de voz que podrían incitar a los niños a realizar acciones peligrosas;

2) riesgos altos: exigen certificación antes de salir al mercado, como sistemas de IA utilizados en infraestructuras críticas, por ejemplo: la gestión de tráfico, el suministro de energía o dispositivos médicos;

3) riesgos limitados: requieren la declaración de todo contenido generado por IA, como informar a los usuarios que están interactuando con un sistema de IA, por ejemplo: el caso de un *chatbot* que genera respuestas automáticas, o sistemas que manipulan imágenes o audio (como los *deepfakes*), que deben etiquetarse como contenido generado artificialmente;

4) riesgos mínimos: son sistemas de IA que presentan un riesgo bajo o nulo, como los filtros de *spam* o videojuegos impulsados por IA, que no están sujetos a regulaciones estrictas, aunque se recomienda seguir principios generales como la supervisión humana (https://legalsolutions.thomsonreuters.co.uk/blog/2024/08/08/ai-act-the-worlds-first-comprehensive-laws-to-regulate-ai/).

Es el "termómetro probabilístico" en la producción de daños el que determina –por ejemplo– que en el diseño, uso de algoritmos y sistemas de inteligencia artificial, ante todo deba velarse por su adecuado funcionamiento en términos de seguridad; por ello, exige una gestión de carácter proactiva, la elaboración de protocolos que determinen esquemas de evaluación periódica (análisis de riesgos, validación de resultados, monitoreo), con un adecuado registro de actividades: medidas técnicas que demuestren la seguridad de los sistemas de IA utilizados en cumplimiento de los estándares más elevados y exigentes.

Por lo demás, cabe considerar que también incide el "apetito de riesgo" empresario, fruto de una evaluación y

(7) Los algoritmos están caracterizados por su universalidad y su opacidad, es decir que están presentes en todos los ámbitos de nuestras vidas y permanecen ocultos. Es imposible saber dónde se encuentra cada algoritmo, qué hace y cuál es su objetivo verdadero, etc. Las grandes empresas de la *worldwide web* son remanentes a dar información de este tipo, so pretexto de que se debilitarían los procesos de IA (Colombo, Celeste, ob. cit., pág. 2).

(8) Domenech, María Mercedes, "Análisis periódico de riesgos de *compliance* y su impacto en un programa de integridad dinámico", en *Compliance, anticorrupción y responsabilidad penal empresaria,* La Ley, mayo de 2018, págs. 267/277; Ubiría, Fernando y Pérez, Matilde, "La herramienta del *compliance* como canal de cumplimiento de exigentes estándares preventivos para la gestión de actividades peligrosas o riesgosas", ponencia presentada en las XXVIII JNDC, Mendoza, 2022, comisión N° 3, en el marco del "Proyecto IUS de investigación" de la "Facultad de Derecho" de la "Pontificia Universidad Católica Argentina" (UCA).

decisión de negocio que, por tanto, fundamenta la consecuente imputación de las contingencias dimanantes: como reza el sabio proverbio, "donde está el beneficio, está la carga" (*ubiemolumentum, ibionus*).

5. Rol y virtualidad de los protocolos

El sistema obliga a desplegar la praxis (prestación) con dicho alcance riguroso que, por cierto, abarca desde el mismo diseño del producto o servicio lanzado al mercado.

Ahora cabe preguntarse si se producen daños a pesar de cumplimentarse los elevados estándares existentes (legales o fruto del *softlaw*): ¿podría concluirse que la propia víctima los debe absorber? Es decir, que si el deudor se atiene a los protocolos, su conducta alcanza entidad de "pago" y por tanto, apareja la extinción de la obligación.

Técnicamente, no resulta posible asignarle tamaña virtualidad, pues nos encontramos dentro de un esquema fuertemente objetivo, por lo que solo el *casus* reviste entidad eximitoria, y habida cuenta el complejo escenario actual en que se desenvuelve esta herramienta distópica, nos direcciona hacia el fangoso terreno de los "riesgos del desarrollo"[9].

Esta desafiante tensión o puja debe analizarse en el marco del derecho del consumidor, y vemos claro que, como principio sistémico, el uso de la IA siempre debe alinearse con la protección de derechos, pues –caso contrario– no pasaría de ser un postulado aspiracional meramente declarativo.

Llegados a este punto, evidentemente la aporía que se presenta excede el estrecho marco de nuestra especialidad y se abre hacia una dialéctica superior y más compleja, enriquecida por la politicidad del derecho y por la perspectiva economicista, factores que integran el complejo entramado del fenómeno jurídico[10].

Mientras nos preguntamos si hay margen para estas últimas disquisiciones, consideramos que no lo hay si es que efectivamente nos encontramos en el terreno de las actividades catalogadas como "riesgosas", en las que –como señaláramos– el amperímetro lo fija la "significativa probabilidad de peligro" para terceros, ponderable según criterios de causalidad adecuada, y la ley es clara al determinar que "No son eximentes la autorización administrativa para el uso de la cosa o la realización de la actividad, ni el cumplimiento de las técnicas de prevención" (art. 1757 *in fine,* CCyC).

En suma, el desafío de integrar la inteligencia artificial en el marco jurídico existente es significativo, pero no insuperable. La clave radica en desarrollar un derecho que se adapte a las innovaciones tecnológicas con la debida protección de los derechos. La función preventiva debe, por tanto, prevalecer para asegurar que los avances tecnológicos no se traduzcan en perjuicios para la sociedad.

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

(9) "La función preventiva de la responsabilidad civil constituye una herramienta útil en casos de riesgos del desarrollo a los fines de evitar el agravamiento o continuación del daño", "XXVIII JNDC" de Mendoza, 2022, comisión N° 3.

(10) Existen "nichos" de responsabilidad subjetiva en materia de responsabilidad civil emergente de la informática: por ejemplo, el caso de la actividad que desarrollan los buscadores de internet por afectación de derechos personalísimos (CSJN *in re* "Rodríguez, María Belén c/Google Inc. y otro s/Ds. y Ps.", 28/10/2014, ratificado en pronunciamientos posteriores); o de la actividad que desarrollan plataformas digitalesde intermediación comercial como Mercado Libre, por considerarse que intervienen como meros operadores técnicos y automáticos de datos u ofertas y demandas, sin "intermediación activa"(CNCom., Sala C, "Ferraro Antonio F. c/Car Group SA y Mercado Libre SRL", del 01/10/2019, publicado en RC J 12289/19, cita online: TR LALEY AR/JUR/38410/2019; *ídem*, "Kosten, Esteban c. Mercado Libre SRL s/ordinario", 22/03/2018, cita online: AR/JUR/1780/2018, comentado por Sebastián Cancio, "Comercio electrónico: la posición neutral de la plataforma y la negligencia del consumidor como eximentes de responsabilidad", LL cita online: AR/DOC/3872/2019).