

EXPLORANDO LA RESPONSABILIDAD CIVIL Y EL RIESGO EN EL PROYECTO DE LEY CHILENO SOBRE INTELIGENCIA ARTIFICIAL

EXPLORING CIVIL LIABILITY AND RISK IN THE CHILEAN DRAFT LAW ON ARTIFICIAL INTELLIGENCE

*Felipe Diez Ringeles**

RESUMEN: El presente trabajo pretende abordar el tratamiento de la responsabilidad civil y el riesgo en el proyecto de ley chileno sobre inteligencia artificial (IA) presentado por el Ejecutivo el 7 de mayo de 2024¹. Para dicho propósito, se expone y explora la regulación general del proyecto en la materia, efectuando un análisis crítico del mismo.

PALABRAS CLAVE: responsabilidad civil, riesgo, inteligencia artificial, sistemas de inteligencia artificial, legitimación pasiva.

ABSTRACTS: This work aims to address the treatment of civil liability and risk in the Chilean bill on Artificial Intelligence (AI) presented by the Executive on May 7, 2024. For this purpose, the general regulation of the project on the matter is exposed and explored, carrying out a critical analysis of it.

KEYWORDS: civil liability, risk, artificial intelligence, artificial intelligence systems, passive legitimation.

* Abogado. Magister en Derecho de la Empresa por la Universidad del Desarrollo y doctorando en Derecho por la misma universidad. Profesor de Derecho Civil, Universidad del Desarrollo. Correo electrónico: f.diez@udd.cl

¹ *Boletín* n.º 16821-19.

NOTAS PRELIMINARES

La inteligencia artificial, por la automatización de procesos que conlleva², importa el elemento central de la denominada “cuarta revolución industrial”³, especialmente por haber producido un efecto disruptivo en la sociedad y economía⁴, generando importantes desafíos para las ciencias, y en especial para el derecho. Entre los diferentes retos jurídicos, se encuentra el de la responsabilidad civil, especialmente por las características propias de los sistemas inteligentes, en que destaca su autonomía, es decir, que el sistema pueda tomar una “decisión” entre dos o más acciones posibles, basándose en sus propios datos⁵; su opacidad, vale decir, la dificultad de comprender y explicar cómo han tomado esas decisiones⁶; la interconexión, que dificulta identificar a los muchos otros actores que pueden haber intervenido en la producción del daño⁷ y, por último, su carácter abierto, lo que significa que requieren constantemente actualizaciones y mejoras⁸. Conforme a lo dicho, parece relevante explorar cómo este proyecto pretende incidir en la materia⁹ a través de:

- I. una regla general de responsabilidad por daños ocasionados por sistemas inteligentes;
- II. la clasificación de los sistemas de IA según el riesgo que entrañan y
- III. la llamada responsabilidad generada a partir de espacios controlados de pruebas para la IA.

² Véase SCHWAB (2016) pp. 19-28.

³ LLANO (2021) p. 26; MARTÍN-CASALS (2022) p. 102. Para una visión panorámica y elocuente sobre qué es la inteligencia artificial y su historia, véase el eminente trabajo de AMUNÁTEGUI (2021) pp. 13-51.

⁴ MARTÍN-CASALS (2022) p. 102; NAVAS (2022) p. 2.

⁵ AMUNÁTEGUI (2021) p. 54; ATIENZA (2022) p. 60; MARTÍN-CASALS (2022) pp. 115-116.

⁶ ATIENZA (2022) p. 58; MARTÍN-CASALS (2022) pp. 115-116.

⁷ ATIENZA (2022) pp. 57-58; MARTÍN CASALS (2022) pp. 115-116.

⁸ ATIENZA (2022) p. 62; MARTÍN CASALS (2022) p. 117.

⁹ Existen antecedentes de propuestas legislativas sobre inteligencia artificial en Chile. Así, la ley n.º 21383, publicada el 25 de octubre de 2021, modificó el numeral 1.º del art. 19 de la Constitución Política de la República, en el sentido de agregar lo que sigue: “El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella”. Asimismo, y en cumplimiento de dicha norma constitucional, actualmente existe otro proyecto de ley, *Boletín* n.º 15869-19, en primer trámite constitucional, que: “regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas, en sus distintos ámbitos de aplicación”. A la fecha de este trabajo, el referido proyecto, sigue en primer trámite constitucional.

I. REGLA GENERAL DE RESPONSABILIDAD CIVIL POR DAÑOS OCASIONADOS POR SISTEMAS INTELIGENTES (ART. 28)

El proyecto de ley, en el art. 28, dispone:

“La persona que sufra un daño como consecuencia de la utilización de un sistema de IA, podrá demandar civilmente y de forma conjunta respecto del operador:

- a) La cesación de los actos generadores de daño.
- b) La indemnización de los daños y perjuicios.
- c) La adopción de las medidas necesarias para evitar que prosiga la infracción.
- d) La publicación de la sentencia a costa del condenado, mediante anuncios en un diario a elección del demandante. Esta medida será aplicable cuando la sentencia así lo señale expresamente”.

Conforme a la disposición, los presupuestos de responsabilidad, son los siguientes:

- a) que una persona sufra un daño;
- b) que el daño sea consecuencia de la utilización de un sistema de inteligencia artificial;
- c) que la acción se dirija contra el operador.

En cuanto al daño, la ley no lo ha limitado en su clasificación o extensión, por lo que, en principio, conviene entender que se refiere a todo daño, cualquiera sea su naturaleza y cuantía, sin perjuicio que, naturalmente se trate de perjuicios directos, pues la disposición exige que este *sea consecuencia de la utilización de un sistema de IA*.

En cuanto a la utilización de un sistema de IA, es relevante precisar que se exige o basta “la utilización”, sin que sea necesario, por ejemplo, ser propietario del sistema, o tener alguno derecho sobre el mismo. En cuanto a los sistemas de IA, el proyecto lo define, en su art. 3 n.º 1, como aquel:

“Sistema basado en máquinas que, por objetivos explícitos o implícitos infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los distintos sistemas de IA pueden variar en sus niveles de autonomía y adaptabilidad tras su implementación”.

Luego, según la definición, para estar frente a un sistema inteligente, se requiere:

- a) que exista un sistema basado en máquinas;
- b) que el sistema, por objetivos explícitos o implícitos, infiera, a partir de la entrada que recibe¹⁰, cómo generar salidas (tales como: predicciones, contenidos, recomendaciones o decisiones);
- c) que las “salidas”, influyan en entornos físicos o virtuales.

Respecto a la definición de sistema inteligente, llama la atención que el proyecto defina los “sistemas de inteligencia artificial”, y no a la “inteligencia artificial”, propiamente tal (sin perjuicio que se haga referencia a esta en los antecedentes del proyecto¹¹), lo que puede responder, a que, en la actualidad, más que aludir simplemente a “inteligencia artificial”, se haga referencia a “sistemas de IA”¹², los que pueden ser comercializados o puestos en servicio, y que pueden ser concebidos como un producto, un servicio o, incluso, un híbrido entre ambos¹³. Asimismo, la definición no hace referencia al hecho de que los sistemas de IA son diseñados por seres humanos, prevención que si hace, por ejemplo, la Resolución del Parlamento Europeo sobre el régimen de responsabilidad civil en materia de inteligencia artificial¹⁴; por último, nos parece curioso que la definición haga referencia a las “entradas” y “salidas”, pero omita la referencia a los datos, materia prima de la IA¹⁵, ya sea respecto a su percepción, adquisición o interpretación de los mismos, lo que, si bien se puede “deducir” de los conceptos de “entrada” y “salida”, su omisión hace que la definición devenga en imprecisa. Sin perjuicio de lo anterior, lo que, si nos parece

¹⁰ La información o datos de entrada, ha sido definida en el art. 3 numeral 32 de la Propuesta de Reglamento de la Unión Europea por la se establecen normas armonizadas en materia de IA como: “aquellos datos proporcionados a un sistema de IA u obtenidos directamente por él a partir de los cuales se produce la información de salida”.

¹¹ En los antecedentes del proyecto, se define como: “un conjunto de sistemas basados en máquinas que infieren, a partir de información de entrada, determinada información de salida, que puede consistir en predicciones, contenidos, recomendaciones o decisiones capaces de influenciar espacios físicos o virtuales”: *Boletín* n.º 16821-19 p. 1.

¹² La precisión se efectúa en la Resolución del Parlamento Europeo acerca de un régimen de responsabilidad civil en materia de IA, de 20 de octubre de 2020, la cual, en su art. 3 letra a, advierte: “Todo sistema basado en programas informáticos o incorporado en dispositivos físicos que muestra un comportamiento que simula la inteligencia, entre otras cosas, mediante la recopilación y el tratamiento de datos, el análisis y la interpretación de su entorno y la actuación con cierto grado de autonomía, para lograr objetivos específicos”: PARLAMENTO EUROPEO (2020).

¹³ NAVAS (2022) p. 10.

¹⁴ En su art. 3, la define como, “el *software* que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de *objetivos definidos por seres humanos, generar información de salida* como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos en los que interactúan”.

¹⁵ Los principales elementos que integran la inteligencia artificial son los “datos” y “algoritmos”: COMISIÓN EUROPEA (2020a) p. 20.

prudente, es que la definición pretende ser amplia, lo que permite, hipotéticamente, resistir el desarrollo tecnológico y de mercado, pues, la IA es un concepto abierto cuya definición es difícil de lograr, dada su oscuridad¹⁶, indeterminación¹⁷ y constante evolución¹⁸.

Por último, para ejercer la acción, se exige que la demanda se dirija contra el operador. Esta precisión legislativa es relevante, pues uno de los grandes problemas de los daños ocasionados por sistemas inteligentes ha sido el poder determinar el sujeto o legitimado pasivo de la acción de responsabilidad, dado que el sistema inteligente es una cosa, y como enseña Georges Ripert: “Las cosas, puesto que carecen de vida, salvo que se trate de un animal, no pueden ser causa sino instrumento del daño”¹⁹, por lo que resulta fundamental determinar quién es el agente responsable en una cadena compleja y extremadamente técnica. En cuanto al operador, este es definido por el proyecto como “el proveedor, el implementador, el representante autorizado, el importador y el distribuidor” (art. 3 n.º 10). Asimismo, se define cada uno de los sujetos que lo comprenden; así, el proveedor es

“toda persona natural o jurídica u organismo del Estado *que desarrolle un sistema de IA* con miras a introducirlo en el mercado o ponerlo en servicio, a título gratuito u oneroso” (art. 3 n.º 4);

el implementador “toda persona natural o jurídica u organismo del Estado que utilice un sistema de IA [...]” (art. 3 n.º 5); el representante autorizado como:

“toda persona natural o jurídica domiciliada en Chile que haya recibido y aceptado el mandato por escrito de un proveedor de un sistema de IA para cumplir con las obligaciones establecidas en la presente ley en representación de dicho proveedor” (art. 3 n.º 7);

el importador:

“toda persona natural o jurídica domiciliada en Chile que introduzca en el mercado o ponga en servicio un sistema de IA que lleve el nombre o la marca comercial de una persona natural o jurídica establecida fuera del territorio nacional” (art. 3 n.º 8)

y distribuidor:

“toda persona natural o jurídica que forme parte de la cadena de suministro, distinta del proveedor o el importador, que comercialice

¹⁶ AMUNÁTEGUI (2021) pp. 13-14.

¹⁷ OROZCO (2022) p. 863.

¹⁸ ATIENZA (2022) p. 37.

¹⁹ RIPERT (2013) p. 213.

un sistema de IA en el mercado nacional sin influir sobre sus propiedades” (art. 3 n.º 9).

No obstante, que el “operador” comprenda distintos sujetos en la cadena de suministro (proveedor, representante, importador y distribuidor), y a quien lo utilice (implementador), genera un grave problema para la víctima, pues es claro que el legislador, con esta extensión de sujetos bajo el título común de “operador”, pretende ampliar la gama de legitimados pasivos para favorecer a la víctima, pero el efecto que en realidad produce es absolutamente el contrario, pues según los antecedentes del proyecto, el art: 28 regula:

“la acción de responsabilidad civil por culpa que podría derivarse de la generación de un daño provocado por la utilización de un sistema de IA”²⁰;

en dicho escenario, considerando que los sistemas inteligentes se caracterizan, como dijimos, por ser autónomos, en muchas oportunidades toman decisiones a partir de los datos de su entorno y, en ocasiones, en forma inexplicable, especialmente en tareas complejas, siendo difícil atribuir la culpa o negligencia a los sujetos que operan con ellos²¹, lo que importa entender que el actuar de dichos sistemas pueda ser imprevisible²². Así, la víctima, ante daños ocasionados por un sistema inteligente, podrá concluir, dado el tenor de la disposición, que el agente responsable (legitimado pasivo) es el “operador”, pero tendrá la enorme dificultad o imposibilidad²³ procesal y económica de precisar qué sujeto del “grupo”, reducido bajo el título de “operador”, fue el causante culpable del daño que ha sufrido.

Esta preocupación, que fue omitida por la deficiente técnica legislativa expuesta, sí fue tomada en cuenta, por ejemplo, por la Propuesta de Directiva Responsabilidad Extracontractual, en los términos que siguen:

“Las normas [...] que se basan en la culpa, no son adecuadas para tramitar las denuncias de responsabilidad civil por daños causados por productos y servicios en los que se recurre a la IA. Con arreglo a

²⁰ *Boletín* n.º 16821-19 p. 27.

²¹ ATIENZA (2022) pp. 60-61.

²² ARAYA (2020) pp. 261-262.

²³ Así como enseña Susana Navas, existen situaciones en que no puede acreditarse el proceso en virtud del cual recogiendo unos *in-puts* se obtienen otros *out-puts* concretos; de ahí que se aluda a la *black box* o a la “falta de transparencia de la IA”, refiriéndose a esta en dos sentidos: a) como la *black box*, que tienen las máquinas autónomas donde se recogen todos los datos relativos a su movimiento, actuación y decisión y b) a la *black box* como aquello que no se puede explicar del funcionamiento de la IA (opacidad), la cual puede tener incidencia en la formación del nexo causal y consiguientemente en la prueba por parte de la víctima: NAVAS (2022) pp. 21-22.

dichas normas, las víctimas deben demostrar que ha habido una acción u omisión ilícita por parte de una persona que ha causado el daño. Las características específicas de la IA, incluidas su complejidad, su autonomía y su opacidad (el denominado efecto de ‘caja negra’), pueden dificultar o hacer excesivamente costoso para las víctimas determinar cuál es la persona responsable y probar que se cumplen los requisitos para una demanda de responsabilidad civil admisible. En particular, al reclamar una indemnización, las víctimas podrían tener que soportar unos costes iniciales muy elevados y enfrentarse a procedimientos judiciales mucho más largos, en comparación con los casos sin relación alguna con la inteligencia artificial. Por lo tanto, las víctimas pueden verse disuadidas de intentar siquiera obtener una indemnización”²⁴.

El defecto legislativo, nos parece, se produce porque lo que hace el proyecto para solucionar el problema de la legitimidad pasiva es recurrir, erróneamente, a la regulación de la Propuesta por productos defectuosos, cuya responsabilidad es objetiva²⁵, y cuya acción puede dirigirse contra el “fabricante y otros operadores económicos” en la cadena de suministro, es decir:

“los diversos operadores económicos responden en cascada, es decir, unos en defecto de otros, con el objeto de garantizar que el perjudicado pueda reclamar a la persona más cercana en la cadena de suministro y, en todo caso, que no tenga que hacerlo con sujetos responsables situados fuera del territorio” (art. 4 de la Propuesta)²⁶

y a la Resolución del Parlamento Europeo sobre el régimen de responsabilidad civil en materia de inteligencia artificial, que propuso un régimen mixto, por un lado de responsabilidad objetiva para SIA autónomos de alto riesgo (art. 4²⁷) y, por otro de responsabilidad subjetiva, para los SIA que no sean de alto riesgo, aunque con la posibilidad de aplicar una presunción de culpa del operador en caso de incidentes repetidos graves, señalando como sujeto pasivo de la acción, al operador de un sistema de IA, que se justifica por el solo hecho de que “controla el riesgo asociado al sistema de IA”²⁸. Así, y como podremos concluir, la

²⁴ COMISIÓN EUROPEA (2022a) pp. 1-2.

²⁵ COMISIÓN EUROPEA (2022b) art: 9: “Los Estados miembros garantizarán que se exija al demandante que demuestre el carácter defectuoso del producto, los daños sufridos y el nexo causal entre el defecto y el daño”.

²⁶ MARTÍN-CASALS (2023) p. 81.

²⁷ La disposición reza: “El operador de un sistema de IA de alto riesgo será objetivamente responsable de cualquier daño o perjuicio causado por una actividad física o virtual, un dispositivo o un proceso gobernado por dicho sistema de IA”.

²⁸ PARLAMENTO EUROPEO (2020) p. 4.

lógica de extender al “operador” a distintos sujetos en la cadena de suministro, no parece lógica en un sistema de responsabilidad fundado en la culpa, más aún si se considera que el proyecto no contiene reglas que permitan presumir la culpa o causalidad de los sujetos que utilizan u operan con sistemas inteligentes.

En la misma línea, la problemática incrementa su intensidad si consideramos que el proyecto de ley no establece una responsabilidad solidaria o proporcional para los daños cometidos por los sujetos que comprenden al denominado “operador”, como ocurre con la Propuesta de Directiva sobre Productos Defectuosos, que, en su art. 11²⁹ contempla la posibilidad de que los sujetos que comprenden los diversos operadores económicos puedan, en caso de tener que responder de forma conjunta, ser obligados solidariamente a la reparación. En consecuencia, si dicha hipótesis se presentara en nuestro país (daño ocasionado por uno o más de los sujetos que comprenden el denominado “operador”), se tendría que recurrir a la regla del art. 2317 del *Código Civil*, pero con la dificultad de acreditar que el delito o cuasidelito fue cometido por dos o más de los sujetos mencionados, lo que importa volver al problema primitivo, es decir, que la víctima deba individualizar a los agentes, su acción conjunta y su “participación” culpable y causal en el daño.

Por lo anterior, nos parece cuestionable que el proyecto de ley se haya presentado, en la materia indicada, en los términos antes referidos, siendo una alternativa con miras a mejorar el mismo y procurar la efectiva indemnización de la víctima, mantener la responsabilidad fundada en la culpa, pero recurriendo a soluciones como las indicadas en la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre Responsabilidad Civil Extracontractual a la Inteligencia Artificial, que contempla una responsabilidad por culpa para daños causados por sistemas de IA (art. 1), abandonando la Propuesta de Resolución del Parlamento Europea adoptada en octubre de 2020 antes indicada (que establecía un régimen de responsabilidad objetiva para los sistemas de IA de alto riesgo (capítulo II)) y que establece, en favor de las víctimas, un derecho de acceso a la información que esté en poder de empresas y proveedores, y que resulta necesaria para su reclamación (art. 3: “exhibición de pruebas”)³⁰ y una “presunción iuris tantum de la relación de causalidad” en caso

²⁹ La disposición reza: “Los Estados miembros garantizarán que, cuando dos o más operadores económicos sean responsables de los mismos daños con arreglo a la presente Directiva, puedan ser considerados responsables conjunta y solidariamente”.

³⁰ Cabe señalar que la Propuesta de Directiva establece este mecanismo solo para los sistemas inteligentes de alto riesgo. Sin embargo, esto ha sido criticado por Miquel Martin-Casals, quien ha sostenido: “los retos que los sistemas de IA plantean a la prueba de los presupuestos de la responsabilidad son inherentes a la IA y dependen de la complejidad de la tecnología utilizada

de culpa (art. 4), la que, si bien debe ser probada (culpa), también puede ser presumida mediante el mecanismo que dispone el art. 3 de la Propuesta para el caso de que se incumpla la referida exhibición de pruebas³¹, lo que podría ser razonable y útil para afrontar la dificultad antes expuesta.

Por último, el art. 29 del proyecto, determina que el procedimiento aplicable en materia civil, es decir, para ejercer la acción de responsabilidad contemplada en el art. 28, será el procedimiento sumario, de conformidad con las disposiciones del título XI del libro III del *Código de Procedimiento Civil*.

II. SISTEMAS INTELIGENTES Y CLASIFICACIÓN SEGÚN SU RIESGO

La idea de clasificar a los sistemas inteligentes según su riesgo no es nueva. Así, por ejemplo, el día 19 de febrero de 2020, la Comisión Europea publicó el denominado *Libro Blanco sobre la inteligencia artificial –un enfoque europeo orientado en la excelencia y la confianza*³², en que estableció directrices políticas para enfrentar los diversos desafíos de la inteligencia artificial y analizó de qué forma. Europa evolucionaría en la materia:

“desde la repercusión de las nuevas tecnologías en la sociedad y el empleo, a las dudas que suscita la globalización, los problemas en materia de seguridad [...]”³³,

distinguiendo, para dichos objetivos, entre sistemas de bajo y alto riesgo³⁴. Asimismo, la Resolución del Parlamento Europeo de 2020 distinguió entre distintos sistemas, y definió el sistema inteligente de alto riesgo como:

“aquel cuyo potencial significativo en un sistema de IA que funciona de forma autónoma puede causar daños o perjuicios a una o más per-

por el sistema de IA y no, necesariamente, al riesgo que comportan, por lo que cabe preguntarse cuál puede ser la razón por la que la Propuesta limita tales normas de exhibición de pruebas a los sistemas de IA de alto riesgo”: MARTÍN-CASALS (2023) p. 73.

³¹ Para un estudio pormenorizado y elocuente de la Propuesta, véase MARTÍN-CASALS (2023).

³² La finalidad del *Libro Blanco*, según su propio texto, es formular alternativas políticas para alcanzar un doble objetivo: promover la adopción de la inteligencia artificial y de abordar los riesgos vinculados a determinados usos de esta nueva tecnología: COMISIÓN EUROPEA (2020a) p. 1.

³³ COMISIÓN EUROPEA (2017).

³⁴ El texto señaló que se busca generar un ecosistema de confianza exclusivo, velando por el cumplimiento de normas de la UE, especialmente las normas de protección de derechos fundamentales y los derechos de los consumidores, y en concreto con relación a los SIA que operan en la UE y presentan un riesgo elevado (p. 3).

sonas de manera aleatoria y que excede lo que cabe esperar razonablemente; la magnitud del potencial depende de la relación entre la gravedad del posible daño o perjuicio, el grado de autonomía de la toma de decisiones, la probabilidad de que el riesgo se materialice y el modo y el contexto en que se utiliza el sistema de IA”³⁵.

Asimismo, en la Propuesta de Reglamento por el que se establecen normas armonizadas en materia de IA (llamada Ley de Inteligencia Artificial), distingue, según las prácticas de inteligencia artificial, y los riesgos que los usos de la IA generan, en sistemas de riesgo inaceptable (art. 5), alto y bajo o mínimo³⁶.

En lo que respecta al proyecto de ley chileno, en su art. 5, clasifica los sistemas de inteligencia artificial según su riesgo en sistemas de:

- A) “riesgo inaceptable”
- B) “alto riesgo”
- C) “riesgo limitado” y
- D) “sin riesgo evidente”

En cuanto a los sistemas de riesgo inaceptable.

“Agrupa a sistemas de IA incompatibles con el respeto y garantía de los derechos fundamentales de las personas, por lo que su introducción en el mercado o puesta en servicio se encuentra prohibida” (art. 5 letra a.)

y se considera que estos son, conforme al art. 6 del Proyecto:

- a) los sistemas de manipulación subliminal;
- b) los que explotan vulnerabilidades de personas para generar comportamientos dañinos;
- c) sistemas de organización biométrica de personas basadas en datos personales sensibles;
- d) sistemas de calificación social genérica;
- e) sistemas de identificación biométrica remota en espacios de acceso público real;
- f) sistemas de extracción no selectiva de imágenes faciales;
- g) sistemas de evaluación de los estados emocionales de una persona.

En cuanto a los sistemas inteligentes de alto riesgo, son definidos en el art. 7 inc. 1 del proyecto de ley, bajo el siguiente tenor:

“Un sistema de IA se considerará de alto riesgo cuando presente un riesgo significativo de causar perjuicios para la salud, la seguridad, los derechos fundamentales protegidos por la Constitución Política de

³⁵ PARLAMENTO EUROPEO (2020) art. 3 letra c).

³⁶ COMISIÓN EUROPEA (2020b) arts. 6-7.

la República o el medioambiente, así como los derechos de los consumidores, con independencia de si se ha introducido en el mercado o se ha puesto en servicio, ya sea que el sistema de IA esté destinado a ser utilizado como componente de seguridad de un producto, o bien que sea en sí mismo dicho producto”.

Por su parte, el art. 3 n.º 2, define el riesgo como:

“la combinación de la probabilidad de que se produzca un daño a las personas naturales, su salud, seguridad o derechos fundamentales y la gravedad de dicho daño”

y, el art. 3 n.º 3, precisa que es riesgo significativo:

[...] aquel riesgo que resulta como consecuencia de la combinación de su gravedad, intensidad, probabilidad de ocurrencia y duración de sus efectos y su capacidad de afectar a una o varias personas naturales”,

cuyas reglas aplicables, son, conforme al art. 8 del proyecto:

- A) aquellas relativas al establecimiento de sistemas de gestión de riesgos;
- B) gobernanza de datos;
- C) documentación técnica;
- D) sistema de registros;
- E) mecanismos de transparencia;
- F) mecanismos de supervisión humana;
- G) precisión, solidez y ciberseguridad.

Asimismo, se comprenden medidas frente a contingencias (art. 9), y la obligación de un sistema de seguimiento posterior a la comercialización de IA de alto riesgo (art. 10).

Por otro lado, el art. 30, establece:

“un reglamento dictado por intermedio del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación establecerá el listado de sistemas de IA de alto riesgo y de sistemas de IA de riesgo limitado respecto de los cuales serán aplicables las reglas de los artículos 8 y 11, respectivamente”,

lo que parece pertinente, pues otorga flexibilidad y permite compatibilizar la regulación de los sistemas con el rápido avance tecnológico en la materia.

En cuanto a la definición indicada del proyecto chileno y la necesidad de precisar los sistemas de inteligencia artificial de alto riesgo mediante reglamentos, cabe señalar que el mecanismo es similar a la del art. 6 letra a) de la Propuesta, que establece normas armonizadas en materia de IA (Ley de Inteligencia Arti-

ficial), que define los sistemas de inteligencia artificial, y que recurre a los denominados “anexos”. Así, la Propuesta dispone:

“Un sistema de IA se considerará de alto riesgo cuando reúna las dos condiciones que se indican a continuación, con independencia de si se ha introducido en el mercado o se ha puesto en servicio sin estar integrado en los productos que se mencionan en las letras a) y b): a) el sistema de IA está destinado a ser utilizado como componente de seguridad de unos de los productos contemplados en la legislación de armonización de la Unión que se indica en el anexo II, o es en sí mismo uno de dichos productos; b) conforme a la legislación de armonización de la Unión que se indica en el anexo II, el producto del que el sistema de IA es componente de seguridad, o el propio sistema de IA como producto, debe someterse a una evaluación de la conformidad realizada por un organismo independiente para su introducción en el mercado o puesta en servicio. También se considerarán de alto riesgo los sistemas de IA que figuran en el anexo III”.

En cuanto a los anexos referidos por la Propuesta Europea, *el anexo II* se divide en dos secciones: la “A”, hace referencia a la lista de legislación de armonización de la Unión basada en el nuevo marco legislativo y la “B”, contempla una lista de otra legislación de armonización de la Unión. En lo que respecta al *anexo III*, este dispone:

“Los sistemas de IA de alto riesgo con arreglo al artículo 6, apartado 2, son los sistemas de IA mencionados en cualquiera de los ámbitos siguientes: 1. Identificación biométrica y categorización de personas físicas; 2. Gestión y funcionamiento de infraestructuras esenciales; 3. Educación y formación profesional; 4. Empleo, gestión de los trabajadores y acceso al autoempleo; 5. Acceso y disfrute de servicios públicos y privados esenciales y sus beneficios; 6. Asuntos relacionados con la aplicación de la ley; 7. Gestión de la migración, el asilo y el control fronterizo; 8. Administración de justicia y procesos democráticos”.

Además, para otorgar las necesarias actualizaciones en la materia, propias del avance tecnológico, el referido anexo (III) se puede modificar, conforme lo prescribe expresamente el art. 7 de la Propuesta, si se reúnen las dos condiciones siguientes:

- a) Los sistemas de IA estén destinados a utilizarse en cualquiera de los ámbitos que figuran en los puntos 1 a 8 del anexo III.
- b) Los sistemas de IA conlleven el riesgo de causar un perjuicio a la salud y seguridad, o el riesgo de tener repercusiones negativas *para los derechos fundamentales, cuya gravedad y probabilidad sean equivalentes o*

*mayores a las de los riesgos de perjuicio o de repercusiones negativos asociados a los sistemas de alto riesgo que ya se mencionan en el anexo III*³⁷.

Respecto a los sistemas de IA de riesgo limitado, el proyecto de ley chileno entiende que un sistema de IA es de riesgo limitado cuando “su uso presente un riesgo no significativo de manipulación, engaño o error, producto de su interacción con personas naturales” (art. 11), estableciéndose reglas de transparencia que obligan al proveedor o el usuario a que informen a las personas naturales expuestas a un sistema de IA, que están interactuando con este, salvo las excepciones indicadas en la disposición (art. 12). Por último, el art. 30 de la ley dispone que un reglamento dictado por intermedio del Ministerio de Ciencia, Tecnología, Conocimiento e Innovación establecerá el listado de sistemas de IA de alto riesgo y de sistemas de IA de riesgo limitado respecto de los cuales serán aplicables las reglas de los arts. 8 y 11, respectivamente.

En cuanto a los sistemas inteligentes sin riesgo evidente. Agrupa a todos los demás sistemas de IA que no entran en las categorías mencionadas en los literales precedentes.

Proyecto de ley chileno, y la importancia de la clasificación sistemas inteligentes según el riesgo que entrañen

Dicho lo anterior, la distinción según el riesgo del sistema inteligente, importa, en principio, para definir que grupos de sistemas inteligentes requieren cier-

³⁷ Para dicha evaluación (indicada en la letra b) el art. 7 sostiene que se tendrá en cuenta los criterios siguientes: a) la finalidad prevista del sistema de IA; b) la medida en que se haya utilizado o sea probable que se utilice un sistema de IA; c) la medida en que la utilización de un sistema de IA ya haya causado un perjuicio a la salud y la seguridad, haya tenido repercusiones negativas para los derechos fundamentales o haya dado lugar a problemas importantes en relación con la materialización de dicho perjuicio o dichas repercusiones negativas, según demuestren los informes o las alegaciones documentadas que se presenten a las autoridades nacionales competentes; d) el posible alcance de dicho perjuicio o dichas repercusiones negativas, en particular en lo que respecta a su intensidad y su capacidad para afectar a una gran variedad de personas; e) la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas dependan de la información de salida generada con un sistema de IA, en particular porque, por motivos prácticos o jurídicos, no sea razonablemente posible renunciar a dicha información; f) la medida en que las personas que podrían sufrir dicho perjuicio o dichas repercusiones negativas se encuentren en una posición de vulnerabilidad respecto del usuario de un sistema de IA, en particular debido a un desequilibrio en cuanto al poder o los conocimientos que ambos poseen, sus circunstancias económicas o sociales, o su edad; g) la medida en que sea fácil revertir la información de salida generada con un sistema de IA, habida cuenta de que no se debe considerar que la información de salida que afecta a la salud o la seguridad de las personas es fácil de revertir; h) la medida en que la legislación vigente en la Unión establezca: i) medidas de compensación efectivas en relación con los riesgos que conlleva un sistema de IA, con exclusión de las acciones por daños y perjuicios; ii) medidas efectivas para prevenir o reducir notablemente esos riesgos.

tas medidas o reglas que determina el proyecto, deben ser adoptadas por los operadores, con mayor o menor intensidad según fuere el caso, salvo que se trate de sistemas de riesgo inaceptable, cuyo uso está prohibido. No obstante, y desde la perspectiva de la responsabilidad civil, dicha distinción parece muy relevante, especialmente si consideramos que el art. 28 del mismo, según sus antecedentes, somete la responsabilidad civil a las reglas de la culpa probada. En este sentido, cobra relevancia, según hemos advertido en otro trabajo³⁸ que, si bien el *Código Civil* establece, en general, el sistema de la culpa probada, debiendo acreditar la culpa (o el dolo) al que alega la obligación de indemnizar³⁹, aquello importa dejar a la víctima en desventaja estratégica frente al demandado, pues esta puede carecer de instrumentos probatorios que están en poder del demandado, y en casos más complejos –como ocurre con los daños ocasionados por sistemas inteligentes– por la dificultad de estar en condiciones de probar la culpa del agente⁴⁰. Luego, cuando el perjudicado solicita la indemnización, las reglas de la responsabilidad subjetiva exigen acreditar que ha existido un acto u omisión culpable por parte de la persona potencialmente responsable del daño, así como el nexo causal entre dicho acto culposo y el daño. Por tanto, el problema resulta evidente, pues:

“[...] cuando la IA se interpone entre el acto u omisión de una persona y el daño, las características específicas de determinados sistemas de IA, como la opacidad, el comportamiento autónomo y la complejidad, pueden hacer excesivamente difícil, si no imposible, que el perjudicado satisfaga la carga de la prueba. En particular, puede resultar excesivamente difícil demostrar que un dato de entrada concreto del que es responsable la persona potencialmente responsable ha dado lugar a una información de salida específica de un sistema de IA que, a su vez, ha provocado el daño en cuestión”⁴¹.

Así, ante este tipo de dificultades, y considerando especialmente que el proyecto de ley no entrega solución a la problemática, debemos recordar que el derecho sustantivo de la responsabilidad civil contempla presunciones de culpabilidad, cuyo efecto es invertir el riesgo probatorio en favor de la víctima⁴², las que pueden ser agrupadas en tres categorías⁴³:

³⁸ DIEZ (2024).

³⁹ BARROS (2020) p. 147; DUCCI (1971) p. 84; VODANOVIC (2021) p. 906; Así se ha resuelto en CORTE SUPREMA (2020) rol 3579-1999, c. 3.

⁴⁰ VODANOVIC (2021) p. 952.

⁴¹ PARLAMENTO EUROPEO (2020) p. 19.

⁴² BARROS (2020) p. 149; DUCCI (1937) p. 90.

⁴³ RAMOS (2009) p. 56.

- a) por hecho propio (art. 2329);
- b) por hecho ajeno (arts. 2320, 2321 y 2322) y
- c) por el hecho de las cosas (arts. 2323, 2324, 2326, 2327 y 2328), todas ellas, con el fin de “[...] favorecer a la víctima, de atenuar en parte los inconvenientes de este sistema y de hacer más expedita la acción”⁴⁴.

En este sentido, y para los llamados sistemas inteligentes de alto riesgo, que son aquellos que presentan “riesgos significativos”, y que, por tanto, merecen mayor preocupación, es posible recurrir a la presunción por el hecho propio del art. 2329⁴⁵, que parece una alternativa adecuada⁴⁶, si entendemos dicha disposición como una regla de presunción de culpabilidad referida a las llamadas actividades peligrosas⁴⁷. Para lo que proponemos, lo primero que se debe precisar es que nuestro *Código Civil* no entrega elementos para una definición de actividad peligrosa, resultandos inútiles los intentos por encontrar su significado en los antecedentes históricos del mismo⁴⁸, por lo que la expresión ha debido ser acuñada por la doctrina y jurisprudencia. Así se ha entendido por Carlos DUCCI:

“[...] se trata de actividades o actuaciones cuya peligrosidad implica culpa por sí sola, sin necesidad de prueba al efecto, porque ella va implícita en el daño”⁴⁹;

en el mismo sentido, Mauricio Tapia ha sostenido que una actividad tiene esta calificación en aquellos casos en que:

⁴⁴ VODANOVIC (2021) p. 952.

⁴⁵ Para una visión general de la disposición y las distintas doctrinas sobre la misma véase, por todos: POLIT (2015) pp. 827-846.

⁴⁶ Especialmente en contraste con la del hecho ajeno, que requiere que el guardián y subordinado o dependiente sean capaces de delito y cuasidelito, y que la víctima pruebe la culpa de estos; y, más conveniente que la presunción por el hecho de las cosas, toda vez que, en nuestro derecho, a diferencia del francés, dichas reglas se encuentran restringidas para los casos antes enunciados: ALESSANDRI (2020) p. 283; DUCCI (1937) p. 96; No obstante, Carlos Amunátegui ha sostenido la posibilidad por hecho de los animales que recoge, en esencia, la vieja doctrina romana de la *actio de pauperiem*: AMUNATEGUI (2021) pp. 88-89.

⁴⁷ En este sentido: AEDO (2018) pp. 389-392; AEDO (2023) pp. 221-222, nota pie de página n.º 80; DUCCI (1937) pp. 45-46; DUCCI (1971) pp. 99-100; TAPIA (2009) p. 700; Con matices adhieren a esta interpretación Carolina Schielle y Josefina Tocornal, quienes sostienen: “esta presunción [entendidos ambos incisos del artículo 2329] debe operar solo en [...] actividades en donde el agente causante del daño le es exigible una diligencia especial por la naturaleza de las actividades que desempeña”: SCHIELLE y TOCORNAL (2010) p. 139. Así se ha resuelto en CORTE SUPREMA (2017) rol 41095-2016, c. 4; CORTE SUPREMA (2021) rol 18949-2018, c. 7.

⁴⁸ PIZARRO y MANTILLA (2013) p. 40.

⁴⁹ DUCCI (1971) p. 99.

“[...] involucra una elevada probabilidad de daños a terceros que puede ser estimada peligrosa o aquellas cuya probabilidad de causar daños a terceros es baja, pero que, de producirse su magnitud es considerable o afectan a un gran número de personas”⁵⁰.

En la misma línea, la Corte Suprema ha resuelto que una actividad es peligrosa, cuando:

“hay una peligrosidad desproporcionada derivada de la acción u omisión del agente, en términos tales que genere una probabilidad cierta de que ocurra un daño derivado de su actividad peligrosa [...]”⁵¹,

conceptos y definiciones que han sido similares en la doctrina y jurisprudencia comparada⁵².

En el referido sentido, es posible concluir que una actividad es peligrosa cuando existe una elevada probabilidad de que el riesgo se materialice o cuando la magnitud del daño puede ser de gran envergadura. En este sentido, podemos precisar que no existe “un común denominador para todas las actividades peligrosas, no hay una esencia de peligrosidad”⁵³, lo que

“[...] presenta una ventaja evidente frente a un sistema como el francés que consagra un régimen objetivo de responsabilidad por el hecho de las cosas [...]”⁵⁴,

⁵⁰ TAPIA (2009) p. 455.

⁵¹ CORTE SUPREMA (2021) rol 18949-2018.

⁵² Así se ha entendido por actividad peligrosa aquella “[...] que, una vez desplegada, su estructura o su comportamiento generan más probabilidades de daño de las que normalmente está en capacidad de soportar por sí solo un hombre común y corriente: TAMAYO (2007) p. 395; en Colombia, cuyo art. 2356 es idéntico a nuestro art. 2329, la jurisprudencia ha entendido por actividad peligrosa: “aquella que [...] aunque lícita, es de las que implican riesgos de tal naturaleza que hacen inminente la ocurrencia de daños”: PIZARRO y MANTILLA (2013) pp. 43-44); y en Francia, aquella susceptible: “[...] de causar un daño, inmediato o diferido, de fuerte intensidad a las personas, al medioambiente, o a los bienes, en razón netamente de la complejidad de su organización, de los instrumentos o elementos utilizados, o por su naturaleza misma”: MAZEAU (2010) p. 444.

⁵³ PIZARRO y MANTILLA (2013) pp. 44-46; no obstante, se ha criticado esta flexibilidad por dejar el asunto “[...] a la prudencia de los tribunales, los cuales, careciendo de una normativa adecuada, pueden dirimir los asuntos haciendo uso de una peligrosa libertad [...]”: MUNITA (2019) p. 146.

⁵⁴ PIZARRO y MANTILLA (2013) pp. 47-48; la crítica se funda en que su campo de aplicación se extiende a cualquier daño causado por cualquier cosa. Por esta razón, precisamente, la jurisprudencia francesa ha buscado expedientes para excluir ciertos daños que, en su entender, no merecen ser sometidos a un régimen tan estricto. Dentro de esta perspectiva se han excluido ciertos daños causados por cosas que se encontraban estáticas (...) o que no tuvieron contacto físico con la persona o bien que sufrió el daño.

permitiendo: “[...] aplicarse a los contenciosos [...] cuya órbita se active frente a situaciones no cubiertas por normas especiales”⁵⁵, como sucede con la responsabilidad civil derivada del uso de sistemas inteligentes de alto riesgo.

En este contexto, y teniendo presente la definición de sistema de alto riesgo entregado por el proyecto de ley, que atiende al “riesgo significativo” (art. 7 inc. 1), que, a su vez, responde a la “gravedad, intensidad, y probabilidad” (art. 3 n.º 3), es posible concluir que el uso de los sistemas de alto riesgo cumplen con los elementos necesarios para ser calificados como actividades peligrosas y, por tanto, recurrir a la regla del art. 2329 del *Código Civil* que, como hemos sostenido, comprende la presunción de culpa por el hecho propio ante las llamadas “actividades peligrosas”. Dicho concepto, que importa un concepto jurídico indeterminado, nos parece

“suficiente para que las nuevas circunstancias –como los daños ocasionados por sistemas inteligentes de alto riesgo– queden cubiertas legalmente, aunque no fueran las previstas en el momento en que se adoptaron tales normas”⁵⁶.

Por lo demás, la solución es útil, pues mantiene la culpa en la base de la responsabilidad –como lo sostiene el art. 28 del proyecto–, pero en el sentido de disponer la inversión de la carga probatoria de la culpa del autor y de ampliar el contenido del deber de diligencia⁵⁷, poniendo a cargo del demandado:

“[...] un riesgo mayor de asumir los costos de las posibles indemnizaciones, lo cual podría inducirlo a tomar medidas preventivas específicas y a trasladar y distribuir el riesgo a través de la contratación de seguros”⁵⁸.

Además, se debe tener presente que la calificación de una actividad como peligrosa no implica un juicio de valor y no está llamada a inhibir las conductas ni desincentivar actividades, pues es solo decidir que los daños que se generen en su desarrollo estarán regulados por un régimen de responsabilidad más severo⁵⁹.

Por último, y en cuanto a los efectos del art. 2329 entendido como presunción de culpabilidad por el hecho propio ante actividades peligrosas, se ha sostenido que este permite presumir tanto la culpa como la causalidad⁶⁰; en

⁵⁵ MUNTA (2019) p. 146.

⁵⁶ NAVAS (2022) p. 3.

⁵⁷ VISINTINI (1999) p. 415.

⁵⁸ PIZARRO y MANTILLA (2013) p. 48.

⁵⁹ *Op. cit.* p. 49.

⁶⁰ BARROS (2020) pp. 439-441; en contra, se ha sostenido, que la tiene por objetivo presumir únicamente la relación de causalidad: CORRAL (2013) pp. 226-227; p. 242.

este escenario, la víctima de un daño ocasionado por un sistema inteligente de alto riesgo bajo el tenor del art. 28 del proyecto de ley, podrá demandar indistintamente al “proveedor, el implementador, el representante autorizado, el importador y el distribuidor” (art. 3 n.º 10), presumiéndose la culpa y causalidad respecto de dicho sujeto pasivo.

Es más, para el caso que se atribuya responsabilidad al operador bajo el tenor del art. 2329, entendida como una regla relativa a las actividades peligrosas, y la víctima tenga la calidad de consumidor, resulta procedente, como ya ha advertido Carlos Amunátegui, la aplicación del art. 47 de la Ley n.º 19496⁶¹, que permite que quien ha resultado condenado (el operador) bajo condición de que tenga la calidad de consumidor, disponga de acción solidaria para repetir en contra del productor, importador y primer distribuidor o prestador del servicio, en su caso⁶².

Respecto a la ventaja para la víctima, en el caso de daños ocasionados por sistemas inteligentes de alto riesgo, esta se traduce básicamente en que la víctima no necesita probar la culpa del autor del daño –operador, en los términos del proyecto– ni la relación causal entre este y aquella; de forma que le bastará probar la existencia del hecho perjudicial y el daño, siendo el demandado quien deba acreditar su irresponsabilidad, ya sea porque no existió culpa, o porque hubo caso fortuito, imprudencia exclusiva de la víctima o de un tercero. En defecto de esta prueba debe ser condenado a la reparación⁶³.

⁶¹ AMUNÁTEGUI (2021) pp. 90-91; para una visión panorámica sobre los desafíos de la IA en materia de consumo, véase WALKER (2023).

⁶² Conforme sostienen en un elocuente trabajo Lilian San Martín y Jorge Larroucau, el juez cuenta con dos estrategias para el razonamiento probatorio en el análisis de la causalidad en la responsabilidad civil; el primero, es tener por acreditado el nexos causal mediante la prueba de la culpa y, el segundo, para los casos en que no sea posible efectuar esa conexión funcional entre la culpa y la causalidad –como puede ocurrir con los sistemas inteligentes– recurrir a otros criterios jurídicos como las presunciones; así, en la práctica judicial, lo normal será que la causalidad se acredite mediante la prueba de la negligencia, lo que resulta coherente con la conexión funcional entre la culpa y la causalidad; pero ante problema probatorios y epistémicos –como los indicados– esto se puede solucionar con criterios jurídicos diferentes a la culpa, como el referido: SAN MARTÍN y LARROUCAU (2021) p. 347; lo dicho, resulta coherente con lo sostenido por Enrique Barros, quien distingue entre casos en que es difícil probar con exactitud el hecho que desencadenó el vínculo causal de aquellos en que es en extremo difícil acreditarlo. Para los casos difíciles, la prueba se construirá sobre la base de presunciones, porque su demostración será necesariamente hipotética (por ejemplo, *causas múltiples o tecnológicas complejas*); sin embargo, en casos de extrema dificultad, el autor sostiene que se flexibiliza la exigencia probatoria, si el daño se produce por un hecho ocurrido con ocasión de la actividad del demandado, por lo que tendrá importancia la prueba basada en indicios probatorios que permitan construir una presunción *prima facie* de la relación causal entre la culpa y el daño, ya sea por la gravedad de la culpa o por el *aumento del riesgo* (basado en probabilidades); así, agrega el autor, las razones para asumir una presunción legal de culpa por el hecho propio (art. 2329) rigen también respecto de la causalidad: BARROS (2020) pp. 439-441.

⁶³ ALESSANDRI (2020) p. 216.

III. RESPONSABILIDAD GENERADA

A PARTIR DE ESPACIOS CONTROLADOS DE PRUEBAS PARA LA IA (ART. 21)

Por último, el art. 21 inc. 1, regula la llamada responsabilidad generada a partir de espacios controlados de prueba para la IA, bajo el siguiente tenor:

“Responsabilidad generada a partir de espacios controlados de pruebas para la IA. Los proveedores potenciales en los espacios controlados de pruebas para la IA responderán de cualquier perjuicio causado a terceros como resultado de la experimentación realizada en el espacio controlado de pruebas”.

De esta forma, para que se genere esta responsabilidad, es necesario:

- a.1) que el agente sea un “proveedor potencial”.
- a.2) que el daño se produzca a partir de un espacio controlado de prueba para la IA. En cuanto al espacio controlado, del art. 20, se puede desprender:

“es aquel, que la administración del Estado proporciona para fomentar la innovación y facilitar el desarrollo, la prueba y la validación de sistemas innovadores de IA en la esfera de sus competencias, durante un período limitado antes de su introducción en el mercado o su puesta en servicio, con arreglo a un plan específico acordado entre los proveedores potenciales y las autoridades creadoras de tales espacios”.

- a.3) que el perjuicio causado a terceros sea consecuencia del resultado de la experimentación realizada en el espacio controlado de pruebas.

Por último, cabe señalar que el origen de la disposición (art. 21 inc. 1) tiene su origen en el art. 53 de la llamada Ley de Inteligencia Artificial⁶⁴, que fue aprobada por la Eurocámara de la Unión Europea con fecha 13 de marzo de 2024⁶⁵, y que sostiene, en lo pertinente:

“Los participantes en los espacios controlados de pruebas para la IA responderán de cualquier perjuicio infligido a terceros como resultado de la experimentación realizada en el espacio controlado de pruebas [...]”⁶⁶

⁶⁴ COMISIÓN EUROPEA (2020b).

⁶⁵ La propuesta fue respaldada por la Eurocámara con 523 votos a favor, 46 en contra y 49 abstenciones. Disponible en www.europarl.europa.eu/news/es/press-oom/20240308IPR19015/la-eurocamara-aprueba-una-ley-historica-para-regular-la-inteligencia-artificial [fecha de consulta: 21 de mayo de 2024].

⁶⁶ COMISIÓN EUROPEA (2020b) p. 78.

y que el alcance de la responsabilidad en cuanto a la referencia de “cualquier perjuicio” tiene por objetivo:

“observar un estándar de diligencia suficiente en la utilización del espacio controlado de pruebas para la IA, se establecerá que los proveedores potenciales responderán de cualquier perjuicio causado a terceros como resultado de la experimentación realizada dentro del mismo”⁶⁷.

CONCLUSIONES

1. El proyecto de ley regula, entre otras materias, aspectos relativos a la responsabilidad, estableciendo una regla general de responsabilidad por daños ocasionados por sistemas inteligentes; clasificando a los mismos según el riesgo que entrañan y regulando la llamada responsabilidad generada a partir de espacios controlados de pruebas para la IA.
2. Acerca de la acción de responsabilidad que se contiene en el art. 28, se cuestiona que, estando la norma, según los antecedentes del proyecto, fundada en la culpa, esta señale como legitimado pasivo de la acción al “operador”, que cubre una amplia gama de potenciales sujetos responsables como: el proveedor, implementador, representante autorizado, importador y distribuidor, pues aquello resulta enormemente sensible a la hora de que la víctima deba acreditar la negligencia de los sujetos que operan con los sistemas inteligentes dadas las características propias de estos, más aún, considerando que el proyecto no contiene reglas relativas a presunciones de culpa o causalidad, ni reglas que permitan sostener que exista una responsabilidad solidaria o proporcional.
3. No obstante, y referente a la clasificación de los sistemas inteligentes según el riesgo que entrañan, el proyecto de ley los clasifica en sistemas de riesgo inaceptable, alto, limitado y sin riesgo evidente. En este sentido, precisamos que dicha clasificación, es pertinente para la responsabilidad civil, especialmente si consideramos que, en nuestro entender, el art. 2329 del *Código Civil* contempla una presunción de culpa y causalidad ante daños ocasionados por las actividades peligrosas, las que comparten sus elementos calificadores, es decir, la probabilidad de daño o la magnitud del mismo, con los sistemas inteligentes de alto riesgos, definidos bajo esos mismos parámetros en el pro-

⁶⁷ *Boletín* n.º 16821-19 p. 14.

yecto (art. 7), lo que permitiría, bajo dicha lógica, presumir la culpa (y causalidad) de los daños originados por sistemas inteligentes que sean operados por cualquiera de los sujetos que indica el proyecto, quien tendrá la carga de acreditar su irresponsabilidad.

4. Por último, se contempla la responsabilidad generada a partir de espacios controlados de pruebas para la IA (art. 21), en que el proyecto, según sus propios antecedentes, para “observar un estándar de diligencia suficiente”, estableció que los participantes en estos espacios respondan de “cualquier perjuicio infligido a terceros”.

BIBLIOGRAFÍA

- AEDO BARRENA, Cristián (2018): *Culpa aquiliana. Una conjunción de aspectos históricos y dogmáticos* (Santiago, Thomson Reuters).
- AEDO BARRENA, Cristián (2023): “Título xxxv. De los delitos y cuasidelitos” en Amunátegui Perelló, Carlos (ed.), *Comentario histórico-dogmático al libro IV del Código Civil de Chile* (Santiago, Tirant lo Blanch).
- ALESSANDRI RODRIGUEZ, Arturo (2020): *De la responsabilidad extracontractual en el derecho civil chileno* (Santiago, Editorial Jurídica de Chile).
- AMUNÁTEGUI PERELLÓ, CARLOS (2021): *Arcana Technicae, El derecho y la inteligencia artificial* (Valencia, Tirant lo Blanch).
- ARAYA PAZ, Carlos (2020): “Desafíos legales de la inteligencia artificial en Chile”, *Revista Chilena de Derecho y Tecnología* vol. 9 núm. 2: pp. 257-290.
- ATIENZA NAVARRO, María (2022): *Daños causados por inteligencia artificial y responsabilidad civil* (Barcelona, Atelier Libros Jurídicos).
- BARROS BOURIE, Enrique (2020): *Tratado de responsabilidad extracontractual* (Santiago, Editorial Jurídica de Chile, segunda edición actualizada).
- CORRAL TALCIANI, Hernán (2013): *Lecciones de responsabilidad civil extracontractual* (Santiago, Thomson Reuters).
- DIEZ RINGELE, Felipe (2024): “Daños ocasionados por sistemas inteligentes complejos y de alto riesgo ante la responsabilidad civil extracontractual ¿Quién responde? Dos propuestas desde la legislación civil vigente”, *XIX Jornadas Nacionales de Derecho Civil* (en prensa).
- DUCCI CLARO, Carlos (1937): *Responsabilidad civil extracontractual* (Santiago, Empresa Periodística El Imparcial).
- DUCCI CLARO, Carlos (1971): *Responsabilidad civil. Actividades peligrosas - Hechos de las cosas - circulación de vehículos* (Santiago, Editorial Jurídica de Chile).
- LLANO ALONSO, Fernando (2021): “Inteligencia artificial y derecho. El jurista ante los retos de la era digital”, en Llano, Fernando y Garrido, Joaquín (eds.), *Inteligencia artificial*

- y el derecho. *El jurista ante los retos de la era digital* (Navarra, Thomson Reuters Aranzadi).
- MARTÍN-CASALS, Miquel (2022): “Desarrollo tecnológico y responsabilidad extracontractual. A propósito de los sistemas de inteligencia artificial (IA)”, en Pérez Collados, José (coord.), *La cultura jurídica en la era digital. Cuadernos Digitales, Derecho y Nuevas Tecnologías* n.º 8 (Navarra, Editorial Aranzadi).
- MARTÍN-CASALS, Miquel (2023): “Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial”, *InDret* 3.2023: pp. 55-100. Disponible en <https://indret.com/wp-content/uploads/2023/07/1806.pdf> [fecha de consulta: 9 de mayo de 2024].
- MAZEAU, Laurene (2010): *La responsabilité des professionnels exploitants une activité a risque*, Thèse (Toulouse, Université Toulouse Capitole).
- MUNITA MARAMBIO, Renzo (2019): “Sobre el recurso a máximas generales aplicables a la indemnización por daños derivados de actividades peligrosas o de objetos (peligrosos o no)”, en Céspedes Muñoz, Carlos (coord.), *Estudios de derecho privado en memoria del profesor Nelson Vera Moraga* (Santiago, Thomson Reuters).
- NAVAS NAVARRO, Susana (2022): *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación* (Granada: Editorial Comares).
- OROZCO GONZÁLEZ, Margarita (2022): “Reflexiones acerca de la relación entre Inteligencia artificial y robótica”, en Ataz López, Joaquín y Cobacho Gómez, José (coords.), *Cuestiones clásicas y actuales del derecho de daños* (Navarra, Thomson Reuters Aranzadi).
- PIZARRO, Carlos y MANTILLA, Fabricio (2013): “La responsabilidad civil por actividades peligrosas: aplique primero y explique después”, *Revista de Derecho - Escuela de Postgrado* n.º 4: pp. 7-56.
- POLIT CORVALÁN, Joaquín (2015): “¿Qué ha dicho realmente la jurisprudencia sobre la presunción general de culpa por el hecho propio?”, en Vidal, Álvaro (coord.), *Estudios de derecho civil X* (Santiago, Thomson Reuters) pp. 827-845.
- RAMOS PAZOS, René (2009): *De la responsabilidad extracontractual* (Santiago, Editorial Jurídica de Chile, 5ª edición actualizada).
- RIPERT, Georges (2013): *La règle morale dans les obligations civiles* (Paris, LGDJ).
- SAN MARTÍN, Lilian y LARROUCAU, Jorge (2021): “El razonamiento probatorio para el análisis de la causalidad en la responsabilidad civil: estudio de la jurisprudencia chilena”, *Revista de Derecho Privado*, n.º 40 (Universidad Externado de Colombia): pp. 329-359.
- SCHIELE, Carolina y TOCORNAL, Josefina (2010): “Artículo 2329 del Código Civil: la interpretación por presunción por hechos propios existe en la jurisprudencia”, *Revista Chilena de Derecho* vol. 37 n.º 1: pp. 123-139.
- SCHWAB, Klaus (2016): *La cuarta revolución industrial* (Bogotá, El Tiempo Casa Editorial, S.A.).

- TAMAYO JARAMILLO, Javier (2007). *Tratado de responsabilidad civil*, tomo I (Bogotá: Legis).
- TAPIA RODRÍGUEZ, Mauricio (2009): “Contra una presunción general de culpa por el hecho propio”, en Pizarro Wilson, Carlos (coord.), *Estudios de Derecho Civil IV. Jornadas Nacionales de Derecho Civil*, Olmué (Santiago, Legal Publishing) pp. 689-705.
- VODANOVIC HAKLICKA, Antonio (2021): *Tratado de derecho civil. Fuente de las obligaciones. Parte especial: de las fuentes de origen no convencional* [basado en las explicaciones de clases de Arturo Alessandri y Manuel Somarriva], tomo III (Santiago, Ediciones Jurídicas de Santiago, segunda edición actualizada).
- VISINTINI, Giovanna (1999): *Tratado de la responsabilidad civil* (trad. Aída Kemelmajer de Carlucci, Buenos Aires, Editorial Astrea).
- WALKER SILVA, Nathalie (2023): “Algunos desafíos en materia de consumo”, en Walker Silva, Nathalie y Schiele, Carolina (eds.), *Estudios de Derecho del Consumidor IV, X Jornadas Nacionales de Derecho del Consumo. Facultad de Derecho, Universidad Andrés Bello* (Valencia, Tirant lo Blanch).
- ZURITA MARTÍN, Isabel (2021): Gestión de riesgos y responsabilidad civil de los robots, en Ataz, Joaquín y Cobacho, José (coords.), *Cuestiones clásicas y actuales del derecho de daños* (Navarra, Thomson Reuters Aranzadi).

Normas

Boletín n.° 16821-19, que “Regula los sistemas de inteligencia artificial”. Disponible en www.senado.cl/appsenado/templates/tramitacion/# [fecha de consulta: 9 de mayo de 2024].

Boletín n.° 15869-19, que “Regula los sistemas de inteligencia artificial, la robótica y las tecnologías conexas, en sus distintos ámbitos de aplicación” Disponible en www.camara.cl/verDOC.aspx?prmID=72777&prmTipo=FICHAPARLAMENTARIA&prmFICHATIPO=DIP&prmLOCAL=0 [fecha de consulta: 9 de mayo de 2024].

Código Civil Chile.

COMISIÓN EUROPEA (2017): “La Comisión presenta el Libro Blanco sobre el futuro de Europa: Vías para la unidad de la UE de 27 Estados miembros”. Disponible en https://ec.europa.eu/commission/presscorner/detail/es/IP_17_385 [fecha de consulta: 9 de mayo de 2024].

COMISIÓN EUROPEA (2020a): *Libro blanco sobre la inteligencia artificial – un enfoque europeo orientado a la excelencia y la confianza*. Disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065> [fecha de consulta: 9 de mayo de 2024].

COMISIÓN EUROPEA (2020b): *Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la unión*. Disponible en <https://eur-lex.europa.eu/resource.tml?uri=cellar:e0649735-a372->

11eb-958501aa75ed71a1.0008.02/DOC_1&format=PDF [fecha de consulta: 9 de mayo de 2024].

COMISIÓN EUROPEA (2022a): *Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial (Directiva sobre responsabilidad en materia de IA)*. Disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022PC0496&from=ES> [fecha de consulta: 9 de mayo de 2024].

COMISIÓN EUROPEA (2022b): *Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos*. Disponible en <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022PC0495&from=ES> [fecha de consulta: 9 de mayo de 2024].

Ley n.º 19496, “Establece normas sobre protección de los derechos de los consumidores”. Disponible en www.bcn.cl/leychile/navegar?idNorma=61438 [fecha de consulta: 10 de mayo de 2024].

Ley n.º 21383, “Modifica la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas”. Disponible en www.bcn.cl/leychile/navegar?idNorma=1166983 [fecha de consulta: 10 de mayo de 2024].

PARLAMENTO EUROPEO (2020): Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un régimen de responsabilidad civil en materia de inteligencia (2020/2014(INL)). Disponible en www.europarl.europa.eu/doceo/document/A-9-2020-0178_ES.html [fecha de consulta: 9 de mayo de 2024].

Jurisprudencia

CORTE SUPREMA (2017): rol 41095-2016, 15 de junio de 2017.

CORTE SUPREMA (2000): rol 3579-1999, 16 de octubre de 2000.

CORTE SUPREMA (2021): rol 18949-2018, 22 de febrero de 2021.