Universidad de Chile
Facultad de Derecho
Departamento de Derecho Comercial

INTELIGENCIA ARTIFICIAL EN LAS RELACIONES DE CONSUMO: OPORTUNIDADES Y DESAFÍOS

CAMILA ANTONELLA NAVARRETE GARCÍA
MARTÍN IGNACIO ZÚÑIGA DENEGRI

Profesor Guía: Claudio Magliona Markovicth

Santiago, Chile

2023

A nuestras familias y, especialmente, a nuestras madres, con todo el amor del mundo, porque sin ellas nada de esto habría sido posible.

A nuestros amigos y amigas, que nos acompañaron día a día y, también, noche tras noche.

Al equipo docente que guio la Memoria, por sus comentarios y sugerencias.

Y, finalmente, a nosotros mismos, por todo el esfuerzo y apoyo que nos brindamos durante este arduo proceso.

Hay dos buenas formas de poner a prueba una amistad: una es el paso del tiempo y la otra es realizar una Memoria en conjunto sin desistir en el camino.

"If a machine is expected to be infallible, it cannot also be intelligent".
– Alan Turing.

ÍNDICE

RESUMEN

El uso de sistemas de Inteligencia Artificial en actividades comerciales y empresariales es cada vez más recurrente. La incorporación de estas tecnologías en las relaciones de consumo genera cuantiosas oportunidades para el desarrollo de las mismas. Sin embargo, al mismo tiempo, debido a su particular funcionamiento, acarrea importantes desafíos en cuanto a la debida protección de los derechos de los consumidores. En tal sentido, la presente Memoria de Prueba examinará cómo el empleo de inteligencia artificial por parte de los proveedores repercute, tanto positiva como negativamente, en la autonomía, privacidad e integridad de los consumidores. Lo anterior, con el objetivo de descifrar los principales lineamientos que debe seguir una regulación que, junto con aprovechar las oportunidades que brinda el uso de inteligencia artificial en las relaciones de consumo, permita eliminar o disminuir significativamente los riesgos hacia los consumidores. Finalmente, se concluye que ha de fomentarse el uso de esta tecnología en la medida en que la normativa vigente en nuestro país sea complementada con ciertos estándares propuestos o consagrados internacionalmente.

PALABRAS CLAVES

Consumidores; Inteligencia Artificial; Autonomía; Privacidad; Responsabilidad; Transparencia; Algoritmos.

ABSTRACT

The use of Artificial Intelligence systems in commercial and business activities is becoming increasingly common. The incorporation of these technologies in consumer relationships generates significant opportunities for their development. However, at the same time, due their particular functioning, it presents substantial challenges in ensuring the proper protection of consumer rights. In this regard, this essay will examine how the utilization of artificial intelligence by providers impacts both positively and negatively on the autonomy, privacy, and integrity of consumers. This is done with the aim to decipher the main guidelines that should be followed by a regulation that, along with taking advantage of the opportunities offered by the use of artificial intelligence in consumer relations, allows eliminating or significantly reducing the risks for consumers. Finally, it is concluded that the use of this technology should be encouraged to the extent that the regulation in force in our country is complemented by certain standards proposed or enshrined internationally.

KEYWORDS

Consumers; Artificial Intelligence; Autonomy; Privacy; Liability; Transparency; Algorithms.

INTRODUCCIÓN

Los sistemas de Inteligencia Artificial (En adelante "**IA**") están revolucionando nuestra sociedad. Debido a su potencial y versatilidad, el campo de aplicación de la IA es muy amplio. Podemos apreciarla en nuestro día a día, cuando interactuamos con *chatbots* o utilizamos sistemas de geolocalización; así como en las labores más complejas y rebuscadas que se pueda imaginar, como las predicciones climáticas y el arte generativo.

En virtud de lo anterior, son cada vez más las empresas que incorporan tecnologías de IA en sus procesos de optimización, toma de decisión, control, venta, asistencia personal, entre otros. Un ejemplo concreto de esta tendencia se aprecia en el estudio AI Readiness 2023, desarrollado por el Instituto Data Science UDD y la Cámara Chilena Norteamericana de Comercio, el cual revela que, durante el año 2022, las empresas nacionales desarrollaron modelos basados en IA en una proporción diez veces mayor a la de la academia informática[1].

Así las cosas, actualmente es frecuente que estos sistemas -que en algún momento, no tan lejano, fueron una mera utopía- participen de las interacciones de consumo, ya sea en forma previa a que el proveedor establezca vínculos con el consumidor, durante la fase de comercialización o, incluso, actuando como componente del bien o servicio a vender[2].

La opinión de la comunidad –tanto general como académica– sobre este fenómeno es dual. Por un lado, se ha sostenido que la incorporación de la IA en las relaciones de consumo brinda un sinfín de oportunidades para el desarrollo de las mismas, por cuanto la captura y el procesamiento automatizado de datos permiten, entre otras cosas, ofrecer servicios personalizados a los consumidores, brindar asistencia virtual y reducir los costos de transacción[3].

Por otro lado, se ha destacado que ello supone importantes riesgos para los derechos de los consumidores, asociados, principalmente, al ejercicio de influencias indebidas sobre su

---

[1] INSTITUTO DATA SCIENCE UDD y AMCHAM CHILE. *AI Readiness. 2° Diagnóstico de la adopción de la inteligencia artificial IA de empresas en Chile.* [en línea], p. 8, <https://ingenieria.udd.cl/files/2023/06/2023-05-10-ai-readiness-2023.pdf> [consulta: 30 agosto 2023].

[2] ABRAHAM, M. y EDELMAN, D. *Customer Experience in the Age of AI.* [en línea] Harvard Business Review. March-April 2022. <https://hbr.org/2022/03/customer-experience-in-the-age-of-ai> [consulta: 30 agosto 2023].

[3] PUNTONI, Stefano, et al. *Consumers and artificial intelligence: An experiential perspective*. Journal of Marketing, 2021, vol. 85, no 1, p. 131-151. p. 132.

autonomía, a la vulneración de su privacidad y a la producción de discriminaciones arbitrarias en la toma de decisiones[4].

Atendido que los beneficios que produce la incorporación de IA en las relaciones de consumo resultan suficientemente significativos como para rehusar vedar su uso, pero, al mismo tiempo, los riesgos asociados son preocupantes, surge la pregunta de si es necesario regular la materia.

En términos generales, el acto de regular encuentra su motivación en proteger intereses públicos y/o evitar fallas de mercado[5]. En el caso del uso de IA en las relaciones de consumo, es claro que dichos fundamentos concurren, toda vez que esta tecnología, si bien ofrece grandes oportunidades de desarrollo, posee el potencial de conculcar garantías fundamentales de las personas, tales como la integridad física y psicológica, la dignidad humana, la libertad de expresión, entre otras[6].

Asimismo, los sesgos ínsitos a los algoritmos empleados por la IA pueden facilitar la colusión de precios y disminuir la transparencia de los mercados[7]; en tanto que el acceso y procesamiento de grandes volúmenes de datos puede constituirse en una barrera de entrada tecnológica, por ser un activo que, no obstante su utilidad, resulta complejo de replicar para las empresas que acaban de ingresar a un mercado[8].

Por consiguiente, a juicio de los autores, y siguiendo las propuestas de la Unión Europea y Estados Unidos, la incorporación de la IA en las relaciones de consumo se trata de un asunto que amerita regulación. Con todo, no puede obviarse que la imprevisibilidad y el carácter transfronterizo de la IA suponen severos desafíos para todo regulador[9], tanto más

---

[4] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 33 que Aprueba Circular Interpretativa sobre Protección de los Consumidores frente al uso de sistemas de Inteligencia Artificial en las relaciones de consumo. Santiago, Chile, 18 de enero de 2022.. 4-5pp.

[5] SACRISTÁN, Estela. *Teoría de la regulación (en especial, acerca de los fundamentos de la regulación*. Derecho PUCP. (76): 2016, p. 86.

[6] COMISIÓN EUROPEA, 2020. *LIBRO BLANCO sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza.* [en línea], p. 13, <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065> [consulta: 30 agosto 2023].

[7] EUROPEAN COMMISSION, 2019. *Ethics guidelines for trustworthy AI*, p. 25 [en línea], <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai,> [consulta: 30 agosto 2023].

[8] LABBÉ Figueroa, María. *Big Data: Nuevos desafíos en materia de libre competencia*. Revista chilena de derecho y tecnología. 9(1): 2020, p. 45.

[9] ZAROR, Danielle. *¿Por qué resulta tan problemático regular la tecnología?* En: AZUAJE Pirela, M (coord.). *Introducción a la ética y el derecho de la inteligencia artificial*. Madrid, Wolters Kluwer-La Ley, 2023. p. 240.

cuanto que esta nueva tecnología, en parte, desdibuja las distinciones conceptuales típicas del derecho del consumo y la responsabilidad civil[10].

En efecto, existe incertidumbre en la evolución de los avances tecnológicos, lo que impide al regulador asir completamente el fenómeno. Además, la IA cambia la forma en que se desarrollan las transacciones y, si se sigue un esquema tradicional de responsabilidad, no resulta claro quién debe responder en caso de que los productos o servicios con IA produzcan daños indeseados e impredecibles[11]. Por ello, es importante pensar en cómo ha de ser la regulación.

En Chile, sin perjuicio de las disposiciones genéricas de la Ley Nº 19.496[12] y la Ley Nº 19.628[13] que puedan resultar aplicables, no existe una regulación específica sobre la materia, salvo por la Circular Interpretativa del Servicio Nacional del Consumidor (En adelante "**SERNAC**") sobre "Protección de los consumidores frente al uso de sistemas de inteligencia artificial en las relaciones de consumo", que fue dictada a comienzos del año 2022[14].

No obstante, es difícil sostener que esta Circular Interpretativa pueda ser una regulación como tal, en circunstancias que resulta vinculante únicamente para los funcionarios de la institución. Por lo demás, según se explicará, el documento da excesiva importancia a analizar los derechos y deberes que resultan relevantes en este contexto, sin ahondar en las herramientas normativas que existen para garantizar su cumplimiento; de modo que, aun si tuviese una obligatoriedad mayor, no constituye una protección suficiente.

Dentro de los Proyectos de Ley que se han impulsado, cabe mencionar, en primer lugar, el Boletín 15869-19 que "Regula los Sistemas de Inteligencia Artificial, la Robótica y las Tecnologías Conexas en sus Distintos Ámbitos de Aplicación" (En adelante "Proyecto de ley sobre IA y Robótica"), el cual pretende:

---

[10] *Ibíd.*, p. 240.

[11] *Ibíd.*, p. 241.

[12] DFL 3. CHILE. Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021.

[13] Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999.

[14] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 33 que Aprueba Circular Interpretativa sobre Protección de los Consumidores frente al uso de sistemas de Inteligencia Artificial en las relaciones de consumo. Santiago, Chile, 18 de enero de 2022..

> "[E]*stablecer un área de soberanía digital para los sistemas de inteligencia artificial en que sea el Estado de Chile el que discuta las consideraciones éticas y jurídicas, además de regular los riesgos surgidos a propósito del desarrollo, distribución, comercialización y utilización de esta tecnología. Estableciendo límites, formalidades y requisitos de implementación y aplicación que sean aplicables, y su cumplimiento exigible, a toda persona –natural o jurídica- que desenvuelva su actuar con sistemas de inteligencia artificial.*"[15].

En segundo lugar, resulta importante hacer mención al Boletín 16271-03 (En adelante "**Proyecto de ley Sernac te Protege**"), que "*Mejora la protección de los derechos de las personas consumidoras en el ámbito de sus intereses individuales fortaleciendo al Servicio Nacional del Consumidor, y establece otras modificaciones que indica*"[16].

Aun cuando los objetivos principales de este Proyecto dicen relación con modernizar y ampliar las facultades del SERNAC, agilizar los procedimientos de reclamo y fijar un sistema de incentivos para evitar las sanciones[17], "*también busca actualizar la normativa vigente considerando las nuevas tecnologías y dinámicas existentes en las relaciones de consumo y la reiteración permanente de prácticas abusivas por parte de las empresas*"[18]. No se alude a la IA a lo largo del Proyecto, pero existen algunas disposiciones relevantes que podrían resultar aplicables en este contexto. Una de ellas es la que establece la responsabilidad de las plataformas que intermedian en el proceso de comercialización de bienes y servicios[19].

---

[15] CÁMARA DE DIPUTADOS (Chile). Proyecto de Ley que Regula los Sistemas de Inteligencia Artificial, la Robótica y las Tecnologías Conexas en sus Distintos Ámbitos de Aplicación. Boletín Nº 15.869-19, refundido con Boletín Nº 16.821-19. Valparaíso, Chile, 24 de abril de 2023.

[16] MINISTERIO de Economía, Fomento y Turismo (Chile). Proyecto de ley que mejora la protección de los derechos de las personas consumidoras en el ámbito de sus intereses individuales fortaleciendo al Servicio Nacional del Consumidor, y establece otras modificaciones que indica. Boletín N° 16.271-03. Santiago, Chile, septiembre del 2023.

[17] *Ibíd.*, pp. 9-14.

[18] *Ibíd*, p. 14.

[19] El Proyecto reforma el artículo 43 de la LPDC, estableciendo un nuevo precepto que indica que: "*El proveedor que actúe como intermediario en la comercialización de bienes o servicios responderá directamente frente al consumidor por el incumplimiento de las obligaciones contractuales, sin perjuicio de su derecho a repetir contra los que resulten responsables*".

En tercer lugar, resulta relevante mencionar el Proyecto de Ley que regula el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, que refunde los Boletines 11.144-07[20] y 11.092-07[21], el cual busca perfeccionar las normas relativas a la protección de los datos personales en el ordenamiento jurídico chileno.

Para ello, establece una serie de obligaciones para las empresas y organizaciones que manejan datos personales, tales como obtener el consentimiento explícito de los titulares de los datos, informar sobre el uso que se dará a los datos, garantizar la seguridad de los datos y permitir el acceso y rectificación de los mismos por parte de los titulares. Adicionalmente, crea la Agencia de Protección de Datos Personales, la cual tiene como objetivo supervisar y fiscalizar el cumplimiento de las obligaciones que se consagran y, además, sancionar a las empresas y organizaciones que no cumplan con la ley.

Con todo, según se explicará detalladamente en el tercer Capítulo de la presente Memoria, el nivel de protección de los consumidores ante el uso de IA continuaría siendo insuficiente aun en el evento de que se aprueben los mentados proyectos. En efecto, entre otros problemas, no se consagra un deber general de transparencia en el uso de la IA, ni tampoco un régimen de responsabilidad civil especial que facilite, por ejemplo, la identificación del agente responsable por los daños de la tecnología o la prueba del vínculo causal.

Por su parte, en derecho comparado, destaca especialmente la regulación de la Unión Europea y de Estados Unidos. En lo que respecta a la Unión Europea, en una primera instancia, no existían normas jurídicas concretas, pero la Comisión Europea trabajó en algunos documentos que plantean los lineamientos regulatorios a seguir en la materia, tales como el Libro Blanco sobre Inteligencia Artificial[22] y las Directrices Éticas para una IA fiable[23].

---

[20] MINISTERIO de Economía, Fomento y Turismo (Chile). Proyecto de ley que mejora la protección de los derechos de las personas consumidoras en el ámbito de sus intereses individuales fortaleciendo al Servicio Nacional del Consumidor, y establece otras modificaciones que indica. Boletín N° 16.271-03. Santiago, Chile, septiembre del 2023.

[21] MINISTERIO Secretaría General de la Presidencia (Chile). Proyecto de ley sobre Protección de Datos Personales. Boletín N° 11.092-07. Santiago, Chile, enero del 2017.

[22] COMISIÓN EUROPEA, 2020. *LIBRO BLANCO sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza.* [en línea], <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065> [consulta: 30 agosto 2023].

[23] EUROPEAN COMMISSION, 2019. *Ethics guidelines for trustworthy AI* [en línea], <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai,> [consulta: 30 agosto 2023].

En estos, se reconoce, entre otras cosas, que los consumidores son un grupo especialmente vulnerable[24]; que debe seguirse un principio de prevención del daño[25]; y que los sistemas empleados han de propiciar confianza para un consumo seguro[26]. Todo ello, teniendo presente que "*el marco regulador debe dejar margen para abordar su desarrollo* [el de la IA] *en el futuro*"[27].

Posteriormente, se han propuesto regulaciones más específicas que, al dar forma a las directrices propuestas, consagran algunos estándares cuya replicación resultaría interesante en nuestro medio. Este es el caso de la "Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial", que evita situaciones de responsabilidad difusa en el consumo[28]; y de la propia AI Act[29], que regula en detalle la seguridad de los sistemas de IA en el consumo y cómo puede aminorarse la probabilidad de conculcación de garantías fundamentales.

En cuanto a la regulación de Estados Unidos, la situación no ha sido tan diferente a lo ocurrido en la Unión Europea, en el sentido de que se trata de una materia incipiente, la cual ha comenzado a ser abordada hace no más de una década, pero con especial preocupación, atendida la exponencial importancia que ha ido desarrollando a medida que el estado de la ciencia evoluciona a pasos agigantados.

Al respecto, cabe destacar, por ejemplo, la *National AI Initiative Act,* de 2020; la *Executive Order 13960 on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, también de 2020; la *Digital Services Oversight and Safety Act,* de 2022; y, la *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, de 2023.

---

[24] *Ibíd*., p. 15.
[25] *Ibíd.*, p. 15
[26] COMISIÓN EUROPEA, op. cit., p. 12,
[27] *Ibíd*., p. 12. Corchetes agregados.
[28] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022.
[29] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021.

Asimismo, es necesario mencionar que actualmente se encuentran en trámite legislativo dos proyectos de ley especialmente relevantes en la materia: la *American Data Privacy and Protection Ac*t, que tiene como objetivo proporcionar derechos fundamentales de privacidad de datos a los consumidores, establecer mecanismos sólidos de supervisión y crear una aplicación significativa; y, la Algorithmic *Accountability Act*, la cual busca requerir evaluaciones de impacto de sistemas de decisión automatizados y procesos de decisión crítica aumentados.

Así, en este escenario, surge la pregunta de si es posible que en Chile se genere una regulación específica que recoja estándares internacionales y, junto con evitar o disminuir significativamente los riesgos hacia los consumidores –que persistirían incluso si se aprueban los proyectos de ley actualmente en tramitación–, asegure que las obligaciones y restricciones impuestas a los proveedores sean posibles de cumplir. Esa es la principal pregunta que persigue contestar la presente memoria.

Empero, si el objetivo es pensar en cómo ha de ser la regulación, es menester cumplir con un paso previo. No tiene sentido –o, al menos, no resulta satisfactorio– plantear una regulación si no se tiene plena conciencia de los efectos concretos del fenómeno a regular. En consecuencia, antes de abordar las herramientas regulatorias que posee o que puede consagrar nuestra normativa, se analizará cómo repercute el hecho de que los proveedores empleen IA en la autonomía, privacidad e integridad de los consumidores -que, para estos efectos, según se explicará, se estiman como los derechos más relevantes-.

En este orden de ideas, la presente memoria persigue responder íntegramente a dos preguntas, que corresponden a dos niveles de análisis distintos, pero complementarios. La primera de ellas es: ¿cómo afecta el empleo de IA por parte de los proveedores a los derechos de los consumidores que, a la luz de las particularidades de esta tecnología, resultan más relevantes? Y, una vez respondida dicha interrogante, la siguiente pregunta será: ¿cuál es la forma adecuada de regular esta materia, teniendo en cuenta las herramientas ya previstas en nuestra normativa y aquellas consagradas o propuestas en derecho comparado?

Al respecto, se parte de la hipótesis de que la introducción de IA en las relaciones de consumo beneficia sobremanera a los consumidores, y, aunque conlleva también importantes peligros, estos pueden ser solucionados parcialmente por la normativa actual vigente y

propuesta en nuestro país y, en forma total, por una futura regulación que recoja ciertos estándares consagrados o propuestos internacionalmente. En tal sentido, la respuesta normativa deseable es una que acepte que la IA es una herramienta a la que no deben renunciar los proveedores y, al mismo tiempo, la regule adecuadamente para resolver sus desafíos.

En aras de comprobar dicha hipótesis, y encauzar en forma ordenada, completa y satisfactoria las respuestas a las interrogantes planteadas, este ensayo comprenderá cuatro Capítulos. Cada Capítulo, a su vez, tendrá subsecciones en las que se tratarán en forma específica ciertos temas.

En el primer Capítulo se abordarán brevemente, a modo de marco teórico, las dos instituciones en que se basa esta memoria: las relaciones de consumo y la IA. En primer lugar, se tratará el concepto, regulación y modernización de las relaciones de consumo y, en segundo lugar, la definición de IA, sus usos y ciertos términos relacionados. Lo anterior, con el propósito de asentar las bases conceptuales que resultan fundamentales para entender esta Memoria.

En el segundo Capítulo se explicará por qué la autonomía, la privacidad y la integridad de los consumidores son derechos que se ven afectados por la introducción de IA en las relaciones de consumo. Luego, se analizará, en forma específica y detallada, cómo es que esta tecnología repercute, tanto positiva como negativamente, en dichos derechos. Ello, en primer lugar, para demostrar que no resulta dable prohibir ni restringir severamente su uso; y, en segundo lugar, para dar cuenta de los riesgos a los que debe atender el regulador.

En el tercer Capítulo se analizará la normativa chilena que resulta aplicable en relación a la protección de los consumidores frente al uso del IA. En una primera parte, se examinará en qué medida la ley chilena actual puede responder a los riesgos que se identifiquen hacia los derechos estudiados en el Capítulo anterior, con el fin de demostrar que, sobre todo en la Ley Nº 19.496 (En adelante "**LPDC**"), se prevén herramientas genéricas que permiten disminuir o eliminar adecuadamente la mayor parte de los riesgos, mas existen otros que no pueden ser resueltos en forma satisfactoria.

Posteriormente, en una segunda parte, se proporcionará una mirada crítica sobre el rol y alcance de tres Circulares dictadas por el SERNAC acerca de temáticas que giran en torno

a la protección de los consumidores y los riesgos que las tecnologías implican. En tercer lugar, se abordarán las modificaciones que introducen ciertos Proyectos de Ley en tramitación que buscan modificar la legislación vigente en torno a la protección de los consumidores, la IA y el tratamiento de datos personales. A modo de cierre, se realizará un breve análisis crítico acerca de aquellos riesgos que no logran ser abordados en completitud por la normativa nacional actual.

Finalmente, en el cuarto y último Capítulo, se realizará un análisis de ciertos estándares desarrollados mediante diversos Reglamentos y Directivas de la Unión Europea y, también, Leyes Federales y Órdenes Ejecutivas de Estados Unidos, con el propósito de explicitar la manera en que ambos ordenamientos han dado respuesta a ciertos desafíos pendientes en nuestro medio, en base a lo revisado en el Capítulo III.

Luego, se hará una comparación entre ambas normativas extranjeras y se examinará si es posible arribar a una combinación de reglas, criterios e interpretaciones que permitan resolver satisfactoriamente los desafíos pendientes. La Memoria concluirá con una sección que delimitará el contenido de este eventual futuro régimen y propondrá la forma específica en que debe introducirse en Chile.

CAPÍTULO I. CONCEPTOS GENERALES EN TORNO A LA IA Y A LAS RELACIONES DE CONSUMO

I. Relaciones de consumo

A. Concepto y ámbito de protección

No existe una definición unánime y transversal respecto de lo que es una relación de consumo. Ello se debe, en buena medida, a que todas las legislaciones se encargan de precisar el ámbito de aplicación de la normativa de consumo, de modo que la doctrina, en lugar de construir un concepto de relación de consumo, opta por realizar una identificación de aquellos aspectos que forman parte de su esencia y constituyen un común denominador de los ordenamientos[30].

Así, se ha señalado que la configuración de una relación de consumo siempre exige la concurrencia de un aspecto subjetivo y un aspecto objetivo. El aspecto subjetivo se refiere a que las partes de la relación han de ser un consumidor y un proveedor[31], mientras que el aspecto objetivo alude a que se comercialice un bien, producto o servicio destinado al consumo masivo, y que se cobre un precio o tarifa a cambio[32].

Nuestro ordenamiento sigue la misma lógica. Sin embargo, el aspecto objetivo queda comprendido dentro del aspecto subjetivo. Vale decir, cuando la legislación chilena precisa qué se entiende por consumidor y por proveedor –aspecto subjetivo–, se incorpora como parte de las definiciones la necesidad de que el vínculo recaiga sobre un bien o servicio destinado al consumo final, mediando un acto jurídico oneroso –aspecto objetivo–. Por ello, en la práctica, basta con constatar que una de las partes tiene la calidad de consumidor y la otra de proveedor para estar ante una relación de consumo[33].

Al efecto, el artículo 1 Nº 1 de la LPDC dispone que son consumidores o usuarios "*las personas naturales o jurídicas que, en virtud de cualquier acto jurídico oneroso, adquieren, utilizan, o disfrutan, como destinatarios finales, bienes o servicios. En ningún caso podrán ser*

[30] BARRIENTOS, Francisca. *Lecciones de derecho del consumidor*. Santiago, Thomson Reuters, 2019. 3p.
[31] *Ibíd.*, p. 3.
[32] *Ibíd.*
[33] *Ibíd.*

considerados consumidores los que de acuerdo al número siguiente deban entenderse como proveedores"[34].

De la definición anterior se colige que, para estar en presencia de un consumidor, es necesario que: (i) este sea una persona natural o jurídica que no pueda ser catalogada como proveedor; (ii) realice un acto jurídico oneroso; y (iii) en virtud de dicho acto adquiera, utilice o disfrute, como destinatario final –esto es, para su propio consumo –un bien o servicio.

Por su parte, el artículo 1 Nº 2 de la LPDC indica que son proveedores "*las personas naturales o jurídicas, de carácter público o privado, que habitualmente desarrollen actividades de producción, fabricación, importación, construcción, distribución o comercialización de bienes o de prestación de servicios a consumidores, por las que se cobre precio o tarifa*"[35]. En dicha definición destaca que el proveedor: (i) puede ser cualquier tipo de persona natural o jurídica; (ii) debe realizar alguna actividad –del catálogo amplio que se contempla– en relación al bien o servicio; (iii) realiza dicha actividad en forma habitual; (iv) cobra a cambio un precio o tarifa.

Como puede apreciarse, el aspecto objetivo de la relación de consumo es absorbido por el aspecto subjetivo, por cuanto tanto la definición de consumidor como la definición de proveedor refieren a los dos elementos del aspecto objetivo, a saber: (i) que la relación gire en torno a un bien o servicio destinado al consumo final; y (ii) que haya un acto jurídico oneroso o se pague un precio o tarifa.

Con todo, cabe precisar que la doctrina nacional, en forma bastante mayoritaria, ha entendido suprimida la exigencia de que medie un acto jurídico oneroso o se cobre un precio o tarifa para adquirir la calidad de consumidor y de proveedor –respectivamente–[36]. Puede

[34] DFL 3. CHILE. Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021. Artículo 1 Nº 1.

[35] *Ibíd*. Artículo 1 Nº 2 LPDC.

[36] Los esbozos iniciales de esta tesis pueden apreciarse en: MOMBERG Uribe, Rodrigo. *Ámbito de Aplicación de la Ley No 19.496 Sobre Protección de los Derechos de los Consumidores*. Revista de Derecho (Valdivia). 17: 2004, p.51, en donde el autor sostiene que los actos que sirven de antecedente a la eventual adquisición del bien o servicio se encuentran protegidos por la normativa. La postura avanzó hasta concebir que el acto jurídico oneroso y el pago de un precio ya no constituyen requisitos de las definiciones. Para un mayor detalle sobre la gran acogida dogmática que posee la postura actualmente, véase, por todos: ISLER, Erika. P*lataformas digitales y relación de consumo en Chile: un desafío actual*. En su: *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. 1ºed. Chile, Rubicón Editores, 2023. 193p.

arribarse a tal conclusión a partir de la aplicación del principio pro consumidor consagrado en el artículo 2 ter de la LPDC[37], así como a través de la racionalidad sistémica del cuerpo normativo, que contiene varias disposiciones protectoras que no exigen contrato ni cobro alguno para su aplicación[38]. De este modo, se entiende que la legislación cubre también a los "clientes potenciales"[39] y, en general, a todos quienes interactúen con plataformas digitales de los proveedores[40].

En ese mismo sentido, es menester tener presente que la relación de consumo no supone necesariamente la existencia de una relación contractual. La normativa resulta aplicable aun cuando no se haya suscrito un contrato. Adicionalmente, aplica respecto de toda la cadena de consumo, incluyendo no solo a vendedores directos, sino también a fabricantes, importadores y distribuidores –en la medida en que puedan ser catalogados como proveedores–[41].

B. Justificación y regulación

En términos generales, la creación de un estatuto especializado destinado a proteger al consumidor halla su explicación en que el vínculo de consumo es asimétrico, en el sentido de que una de las partes se encuentra en una posición mucho más fuerte que la otra. En efecto, esta relación supone un desvanecimiento del principio de igualdad entre los contratantes que caracteriza el derecho común, puesto que el consumidor cuenta con un menor nivel de información y poder de negociación que su contraparte proveedora[42].

---

[37] DFL 3. CHILE. Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021. "*Artículo 2 ter.- Las normas contenidas en esta ley se interpretarán siempre en favor de los consumidores, de acuerdo con el principio pro consumidor, y, de manera complementaria, según las reglas contenidas en el párrafo 4° del Título Preliminar del Código Civil*".

[38] ISLER, Erika. P*lataformas digitales y relación de consumo en Chile: un desafío actual*. En su: *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. 1ºed. Chile, Rubicón Editores, 2023. 193p.

[39] BARRIENTOS, Francisca. *Lecciones de derecho del consumidor*. Santiago, Thomson Reuters, 2019. 13p.

[40] ISLER, op. cit., 193p. Sobre este punto, cabe precisar que, incluso si no se entiende suprimido el requisito de que exista un acto jurídico oneroso o se cobre un precio o tarifa, la conclusión seguiría siendo válida, por cuanto, cuando el consumidor interactúa con las plataformas, le da acceso a sus datos personales. Y dado que los datos poseen un valor, ese solo intercambio impide catalogar como gratuito el acto. Véase: MOMBERG URIBE, Rodrigo; MORALES ORTIZ, Maria Elisa. 2019. *Las cláusulas relativas al uso y tratamiento de datos personales y el artículo 16 letra g) de la Ley 19.496 sobre Protección de los Derechos de los Consumidores*. Revista chilena de derecho y tecnología 8(2): 157-180. pp. 176.

[41] BARRIENTOS, Francisca. *Lecciones de derecho del consumidor*. Santiago, Thomson Reuters, 2019. 4-5pp.

[42] ISLER, Erika. *Derecho del consumo. Nociones fundamentales*. Valencia, Tirant lo Blanch, 2021. 65-66pp.

Ello se evidencia, principalmente, en la masificación de la contratación por adhesión. En este tipo de contratos, el proveedor redacta la totalidad del contenido contractual habiendo meditado cada cláusula, en tanto que el consumidor solo podrá leerlo al momento de celebrar la operación[43]. No obstante, incluso si el contrato fuese negociado o no existiese contrato, lo cierto es que el proveedor, al dedicarse de manera profesional a la actividad económica que incide en el bien o servicio del que será destinatario el consumidor, dispone de experiencia y conocimientos que no están al alcance de su contraparte, de suerte que se erige como el único capaz de entender todo lo que está en juego y, a la postre, tutelar completamente sus intereses[44].

De ahí que se haga necesaria la constitución de un Derecho del Consumidor. En palabras del eximio profesor y ex Director del SERNAC, don Francisco Fernandez Fredes, este corresponde a un:

> "[C]*onjunto de normas jurídicas y de mecanismos previstos en el ordenamiento, dirigidos a tutelar o resguardar ciertos intereses que se consideran relevantes en atención al hecho de que el consumidor , sujeto aislado o individualmente determinado que concurre al mercado, lo hace en una situación de inferioridad o desventaja respecto a los proveedores de bienes o prestadores de servicios que acuden a él organizados como empresas, y, por consiguiente, asumiendo determinados riesgos dentro de una concepción de organización ad hoc para injerir profesionalmente en la producción, distribución o comercialización de bienes o servicios*"[45].

En nuestro ordenamiento, dicho régimen se consolida en la LPDC, que contempla varios derechos en favor de los consumidores y obligaciones que han de adoptar los proveedores. Sin embargo, aun cuando este marco aplique en forma especial y prioritaria, debe entenderse sin perjuicio de la eventual supletoriedad del derecho común en materias no

[43] MOMBERG, Rodrigo. *El control de las cláusulas abusivas como instrumento de intervención judicial en el contrato*. Revista de derecho (Valdivia). 26(1): 2013, p. 18.
[44] ZÚÑIGA Denegri, Martín. *Principio de préstamo responsable. Naturaleza y fuentes legales en el ordenamiento jurídico chileno.* Revista de Derecho Económico. 79(2): 2022, p. 103.
[45] FERNÁNDEZ Fredes, Francisco. *La regulación de la actividad económica y los derechos del consumidor. La experiencia chilena*.Temas de Derecho del Consumidor, 1997, pp. 13 y 14.

reguladas –a fin de evitar situaciones de desprotección–[46]. Además, ha de tenerse presente el rol complementario de la Ley Nº 19.628, a propósito de la protección de los datos personales de los consumidores[47].

En cuanto a la regulación prevista en la LPDC, es relevante destacar que, junto con ciertos derechos de los consumidores que aplican en situaciones específicas (ej: acceso al precio, garantía legal, etc.), existen derechos básicos que actúan a modo de marco general, principio informante y criterio interpretativo de toda la normativa de consumo[48]. Dichos derechos están consagrados en diversos literales del artículo 3º de la LPDC y refieren a la libre elección del bien o servicio; al acceso a una información veraz y oportuna; a la proscripción de la discriminación arbitraria; a la seguridad en el consumo; al derecho a la reparación e indemnización adecuada; y, a la educación de un consumo responsable[49].

Con todo, sin desconocer su vocación programática, conviene precisar que existen fundamentos suficientes para sostener que su alcance no se agota en ello. En efecto, la infracción directa a estos derechos básicos bien puede ser reclamada autónomamente –vale decir, sin necesidad de reconducirla a otro precepto más específico– en sede judicial.

Lo anterior se colige del tenor literal de los artículos 50[50] y 24 de la Ley Nº 19.496, que indican, respectivamente, que las acciones que deriven de la LPDC son procedentes ante la afectación del ejercicio de "cualquiera de los derechos de los consumidores"[51], y que las infracciones a lo dispuesto en esta legislación —sin distinguir— serán sancionadas por defecto con multa de 300 UTM[52].

La relevancia de dicha aclaración reside en que, según se explicará, algunos de estos derechos juegan un rol protagónico a propósito de la introducción de la IA en las relaciones de

---

[46] BARAONA, Jorge. *La regulación contenida en la Ley 19.496 sobre protección de los derechos de los consumidores y las reglas del Código Civil y Comercial sobre contratos: Un marco comparativo*. Revista chilena de derecho. 41(2): 2014, p. 382.

[47] DFL 3. CHILE. Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021. Artículo 15 bis, en relación con los artículos 58 y 58 bis.

[48] ISLER, Erika. *Derecho del consumo. Nociones fundamentales*. Valencia, Tirant lo Blanch, 2021. 244p.

[49] DFL 3. CHILE, op. cit. Artículo 3, letras a) a f), respectivamente.

[50] Véase: ISLER, Erika. *Derecho del consumo. Nociones fundamentales*. Valencia, Tirant lo Blanch, 2021. 247p.

[51] DFL 3. CHILE, op. cit. Artículo 50.

[52] *Ibíd*. Artículo 24.

consumo. Si bien su aplicación también podría resultar atingente a propósito de la consecución de otras disposiciones más específicas, es posible que existan hipótesis en las que se vulneren derechos básicos sin infringir ningún otro precepto. De ser así, los consumidores deben tener presente que ello no les impide accionar.

C. Modernización de las relaciones de consumo y consumo digital

La creación de un estatuto protector especial para los consumidores constituyó un gran avance en orden a brindar confianza en el consumo y propender a un equilibrio en las relaciones comerciales. Sin embargo, la aparición y masificación del uso de nuevas tecnologías exige la adopción de un paradigma más moderno. Así como en el siglo XX el fenómeno del consumo masivo desafió el principio civil de igualdad de los contratantes, en el siglo XXI la despersonalización, la intermediación digital y la relativización de los espacios importan repensar los conceptos de consentimiento, contrato, venta, oferta y aceptación[53].

Actualmente, las plataformas digitales, el *marketplace*, la asistencia virtual automatizada y las compras electrónicas asumen un rol protagónico en las relaciones de consumo. Aunque ello ha permitido agilizar las compras, reducir costos de transacción y dar cabida a intercambios beneficiosos que antaño habrían sido inconcebibles[54], también ha transformado el comportamiento de los consumidores y la forma en que estos interactúan con los proveedores[55]. Por consiguiente, parte del régimen inicial ha debido ser ajustado para responder a los desafíos que supone la introducción de estas tecnologías.

En ese sentido, la LPDC ha incluido algunos preceptos que regulan la contratación a distancia –contemplando un derecho a retracto– y el empleo de medios electrónicos[56]. Asimismo, durante el año 2021 se promulgó un Reglamento de Comercio Electrónico que trata

[53] ISLER, Erika. P*lataformas digitales y relación de consumo en Chile: un desafío actual*. En su: *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. 1ºed. Chile, Rubicón Editores, 2023. 189-190pp.

[54] GUAÑA-MOYA, E., QUINATOA-AREQUIPA, E, PÉREZ-FABARA, M. *Tendencias del uso de las tecnologías y conducta del consumidor tecnológico*. Ciencias Holguín, 23(2): pp. 16-17, 2017.

[55] GRETZEL, U., FESENMAIER, D, O'LEARY, J. *The transformation of consumer behaviour.* Tourism business frontiers: Consumers, products and industry, 9: pp. 9-15, 2006. En el mismo sentido, LALALEO, F., BONILLA, D., ROBLES, R. *Tecnologías de la Información y Comunicación exclusivo para el comportamiento del consumidor desde una perspectiva teórica.* Retos: Revista de Ciencias de la Administración y Economía, 11(21): pp. 147-164, 2021.

[56] Véase: MINISTERIO DE ECONOMÍA, FOMENTO Y TURISMO (Chile). *DFL 3, que fija texto refundido, coordinado y sistematizado de la Ley Nº 19.496, que establece normas sobre protección de los derechos de los consumidores.* Santiago, Chile, 2021. Artículos 3, 3 bis, 3 quáter, 12 A, 17 D, entre otros.

con mayor detalle las obligaciones de los proveedores y los derechos de los consumidores en las relaciones de consumo remotas[57].

En concreto, el citado Reglamento tuvo por objeto "*fortalecer la transparencia y calidad de la información que se entrega a los Consumidores en Plataformas de Comercio Electrónico respecto de las características, prestaciones esenciales, precio de los productos y servicios que se ofertan y toda otra información relevante para incentivar la toma de decisiones debidamente informada, con miras a la adquisición de productos o contratación de servicios*"[58].

Como puede observarse, se hace especial énfasis en los deberes de información. Las reformas a las LPDC han ido en esa misma línea. El problema es que no basta con ello. A mayor ahondamiento, el régimen aplicable a las plataformas digitales continúa siendo difuso, por cuanto, si es que estas no reúnen los requisitos para ser catalogadas como proveedores, no se genera una relación de consumo y, por ende, no resulta aplicable la normativa protectora prevista en la LPDC[59].

De igual manera, debe tenerse presente que muchas de las tecnologías que se incorporan a las relaciones de consumo pueden resultar de difícil comprensión para los consumidores. Como consecuencia de lo anterior, estos adquieren una capa de vulnerabilidad adicional a la que poseen por el solo hecho de ser consumidores.

En efecto, ya no solo deben lidiar con ser la parte débil de la relación, sino que, además, han de enfrentar los desafíos que supone el uso de nuevas tecnologías –que, por lo demás, suelen ser empleadas a beneficio del proveedor–. Atendido que en tal cometido se exponen una mayor cantidad de asimetrías informativas y vulneración de sus derechos, se les concibe como "consumidores tecnológicos hipervulnerables"[60]. Si bien parte de los deberes de información pueden ayudar a disminuir dichas asimetrías, hay riesgos en contra de la privacidad, autonomía e integridad que sugieren la adopción de medidas especiales.

---

[57] MINISTERIO de Economía, Fomento y Turismo (Chile). Decreto 6 que Aprueba Reglamento de Comercio Electrónico. Santiago, Chile, 23 de septiembre de 2021.

[58] *Ibíd.* Artículo 1.

[59] ISLER, Erika. P*lataformas digitales y relación de consumo en Chile: un desafío actual*. En su: *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. 1ºed. Chile, Rubicón Editores, 2023. 192p.

[60] LÓPEZ Díaz, Patricia. E*l consumidor hipervulnerable como débil jurídico en el derecho chileno: una taxonomía y alcance de la tutela aplicable*. Latin american legal studies, 10(2): 2022, p. 402.

Más allá de las Circulares Interpretativas del SERNAC a las que se hizo referencia a la Introducción –y que no abordan todos los desafíos–, no existe mayor regulación respecto de la incidencia específica que el uso de nuevas tecnologías puede tener en los derechos de los consumidores. Esto resulta aún más preocupante si se tiene en consideración la masificación de sistemas de IA, que poseen un funcionamiento complejo, utilizan muchos datos de los consumidores y pueden actuar en forma autónoma e imprevisible.

Así las cosas, se hace imperiosa la revisión de los estándares de protección previstos en favor de los consumidores. La presente Memoria pretende descifrar cómo podría ajustarse el régimen a la luz de la introducción de IA en las relaciones de consumo. Ya habiendo realizado una aproximación teórica al derecho del consumidor, se abordará brevemente el fenómeno de la IA.

II. Inteligencia Artificial

A. Definición y conceptos claves

El término "Inteligencia artificial" fue acuñado por primera vez en 1956 por John McCarthy, Marvin Minsky, Nathaniel Rochester y Claude Shannon en una conferencia en Dartmouth College. McCarthy definió la IA como "*la ciencia y la ingeniería de hacer máquinas inteligentes, especialmente programas informáticos*"[61], señalando, además, que la "*inteligencia artificial sería una máquina que se comporta de formas que se llamarían "inteligentes" si un humano se comportara así*"[62].

Ahora bien, el concepto ha ido evolucionando y perfeccionándose con el tiempo. Algunas décadas después, se planteó que, cuando se habla de IA, se hace referencia a un sistema artificial que interactúa autónoma y flexiblemente con su entorno, de manera

[61] *Dartmouth Artificial Intelligence Conference* (1º, Hanover, New Hampshire, Estados Unidos, 1956). Inteligencia Artificial, Dartmouth College, 1956.
[62] *Ibíd*.

apropiada para sus circunstancias y sus metas, aprendiendo de su experiencia y tomando decisiones apropiadas dadas sus limitaciones perceptuales y computacionales[63].

La definición anterior resulta atingente. Sin embargo, en la actualidad el concepto de IA se ha abordado desde una perspectiva más funcional. En efecto, cuando se habla de IA:

> "*Se alude a un sistema que cumpla con tres principios: autonomía, adaptabilidad e interactividad. La autonomía es la capacidad para actuar de forma independiente y tomar sus propias decisiones; adaptabilidad es la capacidad de aprender de las propias experiencias, sensaciones e interacciones para reaccionar con flexibilidad a los cambios del entorno; e interactividad es la capacidad de un agente de percibir e interactuar con otros agentes, sean humanos o artificiales, con sus propias metas y capacidades*"[64].

Así las cosas, la IA tiene una serie de rasgos característicos que la hacen única y que le permiten realizar tareas que normalmente requieren inteligencia humana. Algunas de estas características son: capacidad de reacción ante la información disponible en el entorno; memoria y aprendizaje a partir de la experiencia; razonamiento y resolución de problemas; automatización de procesos; interacción humano-máquina; aprendizaje profundo (*Deep Learning*); creatividad; y, capacidad de trabajar en conjunto y compartir información.

De esta manera, en base a la caracterización ya señalada del concepto de IA, en la sección siguiente se analizarán tres conceptos fundamentales para entender el funcionamiento de esta herramienta y poder analizar su comportamiento en las relaciones de consumo: datos, algoritmos y *machine learning.*

B. Conceptos relevantes

1. Datos

[63] POOLE, David, MACKWORTH, Alan, GOEBEL, Randy. *Computational intelligence: a logical approach*. Nueva York, Oxford University Press, 1998. 1p.
[64] LLAMAS, Jersain, et al. *Enfoques regulatorios para la Inteligencia Artificial (IA)*. Revista chilena de derecho, 2022, vol. 49, no 3, p. 31-62. p. 32.

Los datos son información que se recopila y se almacena en un formato estructurado o no estructurado, los cuales pueden ser de diferentes tipos, como texto, imágenes, audio, video, entre otros. En el contexto de la IA, los datos son esenciales para entrenar los algoritmos de aprendizaje automático y mejorar su precisión y eficiencia con el tiempo. En otras palabras, los datos constituyen la materia prima utilizada para automatizar el proceso de aprendizaje en el que los sistemas son entrenados para realizar predicciones[65].

El análisis de datos es una parte fundamental de la IA, ya que permite a los algoritmos detectar patrones y correlaciones en los datos, lo que, a su vez, les posibilita hacer predicciones o tomar decisiones. La IA utiliza técnicas de análisis de datos, como el aprendizaje automático y el procesamiento del lenguaje natural, para comprender y procesar grandes cantidades de datos y tomar decisiones basadas en patrones y reglas establecidas.

Conceptos relacionados al concepto de "datos":

1) Datos personales

Conforme al artículo 2 letra f) de la Ley Nº 19.628[66], los datos personales son datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables[67]. Para que un dato sea considerado un dato personal no es necesario que se vincule de manera directa y autocontenida a una persona específica. Así las cosas, mientras la información se pueda reconducir a una persona específica nos encontramos ante un dato de carácter personal.

2) Datos sensibles

Conforme al artículo 2 letra g) de la Ley Nº 19.628, los datos sensibles son aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen

[65] FERRANTE, Enzo. *Inteligencia artificial y sesgos algorítmicos: ¿Por qué deberían importarnos?*. Buenos Aires, Nueva sociedad, 2021, no 294, p. 27-36. p.30.

[66] Se previene al lector que, sin perjuicio de tener como base la Ley Nº 19.628, más adelante se abordará el Proyecto de Ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, el cual se encuentra en tramitación.

[67] Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999. Artículo 2 letra f).

racial, las ideologías y opiniones políticas, las creencias religiosas, los estados de salud físicos o psíquicos y la vida sexual[68].

3) Dato estadístico

Conforme al artículo 2 letra e) de la Ley Nº 19.628, un dato estadístico es un dato que, en su origen, o como consecuencia de su tratamiento, no puede ser asociado a un titular identificado o identificable[69].

4) Dato caduco

Conforme al artículo 2 letra d) de la Ley Nº 19.628, un dato caduco es un dato que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiese norma expresa, por el cambio de los hechos o circunstancias que consigna[70].

5) Registro o banco de datos

Conforme al artículo 2 letra m) de la Ley Nº 19.628, registro o banco de datos es un conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos[71].

6) Responsable del registro o banco de datos

Conforme al artículo 2 letra n) de la Ley Nº 19.628, responsable del registro o banco de datos es toda persona natural o jurídica privada, o el respectivo organismo público, a quien compete las decisiones relacionadas con el tratamiento de los datos de carácter personal[72].

7) Titular de los datos

[68] *Ibíd.* Artículo 2 letra g).
[69] *Ibíd*. Artículo 2 letra e).
[70] *Ibíd*. Artículo 2 letra d).
[71] *Ibíd*. Artículo 2 letra m).
[72] *Ibíd*. Artículo 2 letra n).

Conforme al artículo 2 letra ñ) de la Ley Nº 19.628, es titular de los datos toda persona natural a la que se refieren los datos de carácter personal[73].

8) Tratamiento de datos

Conforme al artículo 2 letra o) de la Ley Nº 19.628, se denomina "tratamiento de datos" a cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma[74].

2. Algoritmos

Los algoritmos corresponden a un conjunto metódico de pasos que pueden emplearse para hacer cálculos, resolver problemas y alcanzar decisiones. Un algoritmo no es un cálculo concreto, sino el método que se sigue cuando se hace el cálculo[75].

Conceptos relacionados al concepto de "algoritmo":

1) Sesgos algorítmicos

En palabras de la investigadora Cecilia Danesi, un sesgo algorítmico acaece cuando un sistema de IA hace una predicción que genera una situación injusta o un trato desfavorable para una persona o grupos de personas. Para ponderar esa circunstancia, debemos confrontarla con los principios éticos de la IA, o bien con el ordenamiento jurídico en sentido amplio. El ejemplo clásico es una predicción que trae como resultado una discriminación o un trato desigual prohibido por la ley[76].

2) Auditoría algorítmica

[73] *Ibíd*. Artículo 2 letra ñ).
[74] *Ibíd*. Artículo 2 letra o).
[75] HARARI, Yuval Noah. *Homo Deus. Breve historia del mañana*. Buenos Aires, Ed. Debate, 2015. 100p.
[76] DANESI, Cecilia. *El imperio de los algoritmos: IA inclusiva, ética y al servicio de la humanidad*. Buenos Aires, Galerna, 2022. 113p.

La auditoría algorítmica podría definirse como el proceso de evaluación sistemática de un algoritmo para identificar y corregir sesgos, errores y problemas éticos. El objetivo es garantizar que el algoritmo sea justo y equitativo[77]. Así, la auditoría constituye un mecanismo para comprobar que los algoritmos son diseñados, desarrollados y utilizados de acuerdo con la norma jurídica vigente para garantizar que los principios éticos y jurídicos se reflejan en los sistemas de IA que toman decisiones sobre todos nosotros y, gracias a ellas, se hace la IA más transparente, explicable y eficaz[78].

3) Discriminación algorítmica

La discriminación algorítmica refiere a la situación en la que los algoritmos utilizados en el aprendizaje automático y la inteligencia artificial generan resultados injustos o sesgados para ciertos grupos de personas[79]. Los algoritmos pueden incluir sesgos que discriminan a ciertos grupos de personas, ya sea de manera sutil o evidente, influyendo en los más diversos ámbitos. De este modo, es posible que un individuo o colectivo reciba un tratamiento injusto como consecuencia de la toma de decisiones algorítmica automatizada[80].

4) Equidad algorítmica

Se refiere a la idea de que los algoritmos utilizados en el aprendizaje automático y la IA deben ser justos e imparciales en sus resultados, independientemente de ciertas variables que se consideran irrelevantes o no deben ser tomadas en cuenta[81].

---

[77] KASSIR, Sara. *Algorithmic Auditing: The Key to Making Machine Learning in the Public Interest*. [en línea] IBM Center for The Business of Government. Viewpoints. Winter 2019/2020. <https://www.businessofgovernment.org/sites/default/files/Algorithmic%20Auditing.pdf> [consulta: 10 septiembre 2023]

[78] MOTA, Eva y HERRERA, Esther. 2023. *Auditoría algorítmica en la inteligencia artificial en el sector público.* [en línea] Revista Digital Instituto de Investigaciones y Estudios Contables - FCE UNLP (17) <https://revistas.unlp.edu.ar/proyecciones/article/view/14782> [consulta: 09 septiembre 2023].

[79] KÖCHLING, Alina y WEHNER, Marius. *Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development*. Business Research 13(3): p, 796. 2020.

[80] KNIGHT, Will. *Microsoft is creating an oracle for catching biased AI algorithms*. [en línea] MIT Technology Review. 25 de mayo, 2018 <https://www.technologyreview.com/2018/05/25/66849/microsoft-is-creating-an-oracle-for-catching-biased-ai-algorithms/> [consulta: 10 septiembre 2023],

[81] VERMA, Sahil y RUBIN, Julia. *Fairness definitions explained* [en línea]. Proceedings of the International Workshop on Software Fairness, FairWare'18, May 2018, pp. 1-7 <https://dl.acm.org/doi/10.1145/3194770.3194776> [consulta: 10 septiembre 2023].

5) Transparencia algorítmica

La transparencia algorítmica alude a la apertura o visibilidad del proceso de toma de decisión de los algoritmos. Ello implica que se muestre "*qué datos se utilizan, cómo se utilizan, quiénes los utilizan, para qué los utilizan y cómo se llega a partir de los datos a tomar las decisiones que afectan a la esfera vital de quien reclama esta transparencia* [en este caso, los consumidores]"[82]. En otras palabras, la transparencia es la habilidad para hacer visible los componentes de un sistema de IA[83].

6) Explicabilidad

Conforme a la definición propuesta por la UNESCO, la explicabilidad alude a hacer inteligibles los resultados de los sistemas de IA. La XAI[84] también hace referencia a la comprensibilidad de los datos, procesos y comportamientos de los distintos bloques algorítmicos y a cómo cada uno de ellos contribuye al resultado del sistema. Así, la explicabilidad está estrechamente relacionada con la transparencia, ya que los procesos y sub-procesos que conducen a los resultados deberían ser comprensibles, trazables y apropiados para el contexto[85].

3. Machine learning

En español, "aprendizaje automático", el *machine learning* es una disciplina de la informática que se enfoca en el desarrollo de algoritmos y modelos que permiten a las máquinas aprender a partir de datos, sin ser explícitamente programadas para hacerlo. Se ha definido como "el estudio sistemático de algoritmos y sistemas que mejoran su conocimiento o desempeño con experiencia"[86].

---

[82] SANGÜESA, Ramón. *Inteligencia artificial y transparencia algorítmica: It's complicated.* BiD: textos universitaris de biblioteconomia i documentació. 41: 2018, p.2. Corchetes agregados.

[83] DE ZÁRATE, Luis. *Explicabilidad (de la Inteligencia artificial).* Eunomía. Revista en Cultura de la Legalidad. (22):2022, p. 334.

[84] Sigla de "*Explainable Artificial Intelligence*".

[85] UNESCO. 2021. *Recommendation on the ethics of artificial intelligence.* [en línea], p. 12 <https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa> [consulta: 11 septiembre 2023].

[86] FLACH, Peter. *Machine learning: the art and science of algorithms that make sense of data*. Nueva York, Cambridge University Press, 2012. 23p.

Los algoritmos de *machine learning* se entrenan con un conjunto de datos de entrenamiento para aprender a resolver un problema específico. A partir de ese entrenamiento, los algoritmos pueden hacer predicciones o tomar decisiones en nuevos datos.

Entre las características y funcionalidades del *machine learning* nos encontramos con que los algoritmos de esta disciplina aprenden a partir de datos, en lugar de ser programados explícitamente; pueden automatizar tareas que normalmente requieren inteligencia humana; pueden mejorar su precisión y rendimiento a medida que se les proporciona más datos; y, pueden detectar patrones y correlaciones en los datos, lo que les permite hacer predicciones o tomar decisiones, entre otras cosas.

Conceptos relacionados al concepto de "machine learning":

1) *Aprendizaje profundo o deep learning*

El Deep Learning o aprendizaje profundo, es una técnica de aprendizaje automático perteneciente al campo de la inteligencia artificial (IA), en específico al subcampo del Machine learning o aprendizaje automático. Los algoritmos de Deep Learning se caracterizan por el uso de arquitecturas jerárquicas capaces de aprender abstracciones de alto nivel. Estas arquitecturas están formadas por capas de unidades de procesamiento apiladas, y se denominan redes neuronales artificiales dado que su funcionamiento trata de emular el de las células del sistema nervioso de los seres vivos[87].

2) *Redes neuronales*

Una red neuronal es un modelo matemático que trata de imitar el funcionamiento y estructura de una red neuronal biológica. De manera que, al igual que una red neuronal biológica está formada por la unión de millones de neuronas, la red neuronal artificial está formada por la unión de neuronas artificiales en diferentes capas[88].

[87] PEÑA Lorenzo, José María. *Aplicación de técnicas de aprendizaje profundo (deep learning) para la detección de objetos en Industria 4.0*. Tesis (Máster en Ingeniería de Telecomunicación). Valladolid, España, Universidad de Valladolid, Escuela Técnica Superior de Ingenieros de Telecomunicación, 2022. 23p.

[88] SANCHO CAPARRINI, Fernando. 2015. *Redes neuronales: una visión superficial* [en línea}. Dpto. deficiencias de la computación e inteligencia artificial - Universidad de Sevilla, p. 4 <http://www.cs.us.es/~fsancho/?p=inteligencia-artificial-2022-23> [consulta: 13 septiembre 2023].

En palabras más simples, las redes neuronales son modelos de aprendizaje profundo inspirados en la estructura y funcionamiento del cerebro. Se utilizan para tareas de procesamiento de imágenes, procesamiento de lenguaje natural y más.

3) Big data

Es un término subjetivamente acuñado por la sociedad de conocimiento para denotar el uso de “grandes datos”. Consiste en un sistema complejo de absorción, interacción y proceso de grandes cantidades de datos que deben ser procesados, abarcando además de un elevado volumen o magnitud de los mismos, una variabilidad de fuentes y aspectos que permiten su procesamiento[89].

C. Datos, algoritmos y machine learning: regulación de la IA

Ahora bien, luego de abordar una gran parte de los conceptos más relevantes relacionados con la IA cabe preguntarse por qué, efectivamente, resultan relevantes para el asunto en cuestión. La respuesta reside en que esta investigación busca analizar las repercusiones de la IA en las relaciones de consumo y la posible regulación, lo cual solo es posible si se dimensiona, en forma previa, en qué consiste la tecnología a estudiar.

En el contexto de la IA, es importante entender que los datos, los algoritmos y el machine learning son los componentes principales que permiten su funcionamiento, en tanto la regulación de la IA no es posible la comprensión de los mismos. Los datos son la materia prima con la que se trabaja; los algoritmos son los encargados de procesar los datos; y el machine learning es el que hace que la IA sea efectivamente "inteligente" sin requerir mayor intervención humana después de ser entrenada.

En otras palabras, en función de los datos, la IA puede analizar y procesar grandes cantidades de información en diferentes formatos, permitiendo a los algoritmos identificar patrones y tomar decisiones basadas en esos datos. A su vez, el machine learning posibilita a los algoritmos aprender de manera autónoma y mejorar su rendimiento a medida que se les

[89] BORJA, M. y PÉREZ, M. *Big data: un análisis documental de su uso y aplicación en el contexto de la era digital*. Rev. Prop. Inmaterial 28: p. 273, 2019.

proporciona más información. De ahí que, desarrollar los tres elementos descritos resulta esencial para entender las diversas aplicaciones de la IA en la actualidad.

La IA se ha convertido en una tecnología versátil con una amplia variedad de aplicaciones prácticas, tales como la atención al cliente mediante asistentes virtuales, la medicina, la robótica, el arte y la administración de justicia, entre otros campos. Estas capacidades de la IA tienen un impacto significativo en las empresas, ya que pueden revolucionar sus operaciones al aumentar la eficiencia, reducir costos y mejorar las experiencias de los clientes y/o consumidores. Esta tecnología puede automatizar tareas que antes requerían intervención humana, lo que permite una mayor agilidad y productividad en las empresas[90].

Sin embargo, junto con los beneficios, la IA también plantea desafíos y preocupaciones importantes. La privacidad de los datos es un tema crítico, ya que el uso de grandes cantidades de información personal implica la necesidad de salvaguardar la confidencialidad y protección de los datos de los usuarios. Además, la ética en la toma de decisiones y la responsabilidad de los algoritmos se convierten en temas de discusión, puesto que las decisiones automatizadas pueden tener implicaciones sociales y éticas[91].

[90] INSTITUTO DATA SCIENCE UDD y AMCHAM CHILE. *AI Readiness. 2° Diagnóstico de la adopción de la inteligencia artificial IA de empresas en Chile.* [en línea], p. 7, <https://ingenieria.udd.cl/files/2023/06/2023-05-10-ai-readiness-2023.pdf> [consulta: 30 agosto 2023].
[91] *Ibíd.*, p. 7

CAPÍTULO II. IA EN LAS RELACIONES DE CONSUMO

Los avances de la era digital han adquirido bastante protagonismo en las relaciones de consumo. En efecto, actualmente, muchos bienes y servicios cuentan con tecnologías de IA o son comercializados con ayuda de ella[92].

Dado el carácter de confianza inherente a las transacciones, la creciente incorporación de nuevas tecnologías en las relaciones de consumo produce suspicacia, máxime si es que su funcionamiento resulta de difícil comprensión para la ciudadanía[93]. Sin embargo, más allá de las legítimas preocupaciones, lo cierto es que la automatización y optimización de procesos genera grandes oportunidades tanto para los proveedores como para los consumidores.

Una de las ventajas más destacables es la posibilidad de que los proveedores brinden recomendaciones personalizadas de bienes y servicios a los consumidores, basándose en las preferencias que han hecho explícitas en sus compras previas[94]. Junto con ello, la IA, mediante *chatbots* o asistentes de voz, puede orientar a los consumidores en su proceso de compra, en forma rápida, eficiente y, lo mejor de todo, ¡sin restricciones de horario![95]. De este modo, se da bastante dinamismo a la interacción, lo que permite a ambas partes ahorrar costos y tiempo[96].

Existen también otras ventajas que, si bien benefician directamente al proveedor -por facilitar sus tareas o responsabilidades-, se traducen también en mayor bienestar para los consumidores. Un claro ejemplo es la posibilidad de que se implementen programas de *compliance* eficientes[97] y/o se sistematicen datos de forma tal que se reduzca la probabilidad

---

[92] THE EUROPEAN CONSUMER ORGANISATION (BEUC), 2019. *AI RIGHTS FOR CONSUMERS*. [en línea], <https://www.beuc.eu/sites/default/files/publications/beuc-x-2019-063_ai_rights_for_consumers.pdf> [consulta: 01 julio 2023].

[93] SALESFORCE. *Business Adopting AI Risk a 'Trust Gap' with Customers – Salesforce Repor*t. [en línea] <https://www.salesforce.com/news/stories/customer-engagement-research-2023/> [consulta: 30 agosto 2023].

[94] WERTENBROCH, Klaus, et al. 2020. *Autonomy in consumer choice.* [en línea] Marketing letters, 31: 429-439. <https://link.springer.com/article/10.1007/s11002-020-09521-z> [consulta: 17 octubre 2023]. p. 431.

[95] ANDRÉ, Quentin, et al. Consumer choice and autonomy in the age of artificial intelligence and big data. Customer needs and solutions, 2018, vol. 5, p. 28-37. p. 28.

[96] SARTOR, Giovani, 2020. *New aspects and challenges in consumer protection*. [en línea], p. 10. <https://policycommons.net/artifacts/1336949/new-aspects-and-challenges-in-consumer-protection/1944500/> [consulta: 01 julio 2023].

[97] KINGSTON, John. *Using artificial intelligence to support compliance with the general data protection regulation*. Artificial Intelligence and Law. 25 (4): 2017, pp. 430-431.

de generar daños[98]. Adicionalmente, la IA permite que exista una mayor innovación con los bienes o servicios que se comercializan, por lo que aumenta la variedad de la oferta[99].

Con todo, "*la proliferación de los sistemas de IA implica también diversos desafíos de cara al debido resguardo de los derechos de los consumidores*"[100]. Tal como se adelantó en la Introducción, esta tecnología puede resultar lesiva para las personas, ya sea por amenazar directamente sus derechos o por acrecentar ciertas fallas de mercado.

En concreto, existe un gran riesgo de que los sistemas de IA, al momento de ayudar u orientar al consumidor, ejerzan influencias indebidas sobre su voluntad, impulsándolo a tomar decisiones que de otro modo no habría tomado[101]. Además, el solo hecho de que el proveedor tenga a su disposición información sistematizada sobre el comportamiento de compra de los consumidores, le permite elaborar perfiles a sus espaldas, lo que acrecienta aún más las asimetrías de información propias de la relación de consumo y genera problemas de privacidad[102].

Otro riesgo característico de esta tecnología es que puede dar origen a hipótesis de responsabilidad difusas. Con ello, se alude a aquellas situaciones en que la IA ocasiona daños impredecibles, respecto de los cuales, en principio, no resulta claro quién debe responder[103]. También es posible que los sesgos de los algoritmos conduzcan a discriminaciones arbitrarias, tomando decisiones prejuiciosas o infundadas[104].

A continuación, se examinará el modo específico en que la utilización de IA en las relaciones de consumo puede potenciar y/o poner en riesgo tres elementos clave en el ámbito

---

[98] CHAMATROPULOS, Demetrio. *Inteligencia artificial, prevención de daños y acceso al consumo sustentable*. XXVI Jornadas Nacionales de Derecho Civil (La Plata, septiembre 2017). 26: 2017, p. 5.

[99] THE EUROPEAN CONSUMER ORGANISATION (BEUC), 2019, *AI RIGHTS FOR CONSUMERS.* [en línea], <https://www.beuc.eu/sites/default/files/publications/beuc-x-2019-063_ai_rights_for_consumers.pdf> [consulta: 01 julio 2023]

[100] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 33 que Aprueba Circular Interpretativa sobre Protección de los Consumidores frente al uso de sistemas de Inteligencia Artificial en las relaciones de consumo. Santiago, Chile, 18 de enero de 2022.. 4p.

[101] WERTENBROCH et al., op. cit., p. 431.

[102] EUROPEAN COMMISSION, 2019. *Ethics guidelines for trustworthy AI*, p. 15 [en línea], <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai,> [consulta: 04 julio 2023].

[103] ARAYA Paz, Carlos. *Desafíos legales de la inteligencia artificial en Chile*. Revista chilena de derecho y tecnología. 9 (2): 2020, pp. 278-279.

[104] FERRANTE, Enzo. *Inteligencia artificial y sesgos algorítmicos: ¿Por qué deberían importarnos?*. Buenos Aires, Nueva sociedad, 2021, no 294, p. 27-36. p. 30.

del derecho del consumo: la autonomía, la privacidad y la integridad de los consumidores; exponiendo, en términos generales, las soluciones que admite cada uno de los problemas que se presenten.

Asimismo, al momento de analizar cada elemento, se distinguirá, en la medida en que resulte pertinente, entre, por una parte, la relación entre la recopilación de datos y el derecho examinado; y, por otra parte, cómo afecta al respectivo derecho el uso que la IA da a esa información. Esto último dice relación con la mecánica de los algoritmos y del *machine learning* (en su conjunto, el "funcionamiento de la IA").

En base a la bibliografía consultada y al análisis efectuado por los autores de esta Memoria, se estima que la autonomía, la privacidad y la integridad son los derechos de los consumidores que cobran más relevancia en la interacción con la IA, por cuanto esta tecnología repercute principalmente en tres esferas: (i) la toma de decisión del consumidor (autonomía); (ii) el acceso a datos del consumidor (privacidad); y (iii) el bienestar físico y psicológico del consumidor (integridad).

Se hace presente que la delimitación del objeto de estudio es sin perjuicio de que la IA pueda ocasionar efectos menores en otros derechos de los consumidores. Sin embargo, en esta ocasión el resto de los derechos no serán analizados, pues se estima que una sobrerrepresentación de los efectos ocasionados en los mismos puede desviar el foco de las políticas regulatorias.

I. Autonomía del consumidor

En el ámbito del derecho del consumidor, la autonomía se define como la capacidad de los consumidores para tomar y ejecutar decisiones por sí mismos, libres de influencias externas[105]. En nuestro ordenamiento jurídico, la autonomía se consagra, esencialmente, en el artículo 3 letra a) LPDC, que refiere al derecho a la libre elección del bien o servicio.

[105] WERTENBROCH et al., op. cit., p. 430.

La autonomía puede ser entendida desde dos perspectivas distintas: “autonomía real” y “autonomía percibida”. La autonomía real refiere al grado de independencia efectivo con que un consumidor puede tomar y promulgar sus propias decisiones; mientras que la autonomía percibida es la percepción subjetiva del consumidor de ser capaz de tomar y ejecutar decisiones por su propia voluntad[106].

Autonomía y datos

Mediante el uso de sistemas de IA, los proveedores pueden acumular un sinfín de datos de los consumidores, lo que les permite conocer sus preferencias y brindarles recomendaciones personalizadas[107]. Ello resulta especialmente valorable, considerando que, en ocasiones, la complejidad y variedad de la oferta de los mercados actuales deriva en que los consumidores no sepan qué productos se ajustan más a sus intereses, de modo que no pueden tomar decisiones verdaderamente libres[108].

En ese sentido, la sistematización de patrones de consumo puede ser una herramienta valiosa para que el consumidor ejerza su autonomía, puesto que, de este modo, es capaz de conocerse a sí mismo sin necesidad de incurrir en métodos de autoinspección –que, por lo demás, pueden resultar poco efectivos–[109].

Sin embargo, el hecho de que la IA funcione en base a datos acumulados genera una gran limitación. En concreto, es difícil que esta tecnología detecte todos los cambios de comportamientos del consumidor, así como sus motivaciones valóricas no explícitas en el acto de consumo. Estas motivaciones o preferencias valóricas se denominan metapreferencias[110].

A modo de ejemplo, piénsese en un ex-alcohólico que, luego de 20 años, decide cambiar sus hábitos. Naturalmente, querrá dejar de consumir alcohol y priorizará otros productos. Eso constituye un cambio de comportamiento que responde a una metapreferencia: no querer consumir más alcohol. No obstante, a pesar de que el consumidor esté convencido

[106] *Ibíd*., p. 431.
[107] *Ibíd*., p. 431.
[108] ANDRÉ, Quentin, et al. Consumer choice and autonomy in the age of artificial intelligence and big data. Customer needs and solutions, 2018, vol. 5, p. 28-37. p. 34.
[109] *Ibíd*., p. 29.
[110] *Ibíd.*, p. 34.

de llevar adelante un nuevo estilo de vida, los datos acumulados indicarán que sigue siendo un cliente potencial de alcohol. Mientras así sea, se corre el riesgo de que no se identifiquen correctamente sus intereses y se le aliente a repetir decisiones que desea evitar, privándolo de la capacidad de mejorar su propio carácter[111].

Con todo, cabe advertir que, en último término, el si se potencia o no la autonomía no depende tanto del hecho de que se posean datos sobre el consumidor, sino, antes bien, de cómo la IA pueda procesar la información y los patrones de consumo mediante algoritmos y *machine learning*. En ello se enfocará el análisis.

Autonomía y funcionamiento de la IA

Una vez que los sistemas de IA acumulan la información de los consumidores, la "trabajan" mediante algoritmos de recomendación, enfoques de orientación, publicidad dirigida y asistencia personalizada en la venta[112]. Por ejemplo, piénsese en plataformas de *streaming* de contenido audiovisual, como Netflix, Youtube y Spotify. Estas aplicaciones utilizan algoritmos de IA para recomendar películas, series o canciones a los usuarios, en función de sus preferencias y patrones de consumo previos.

Dichas técnicas aumentan la autonomía percibida de los consumidores, ya que les ayudan a encontrar los productos y servicios que se ajustan mejor a sus intereses[113]. Así, brindan a los consumidores una sensación de autorrealización y empoderamiento en el proceso de compra[114]. Sin embargo, ello trae como consecuencia adversa un riesgo concreto hacia la autonomía real de los consumidores, puesto que, aun cuando, en los hechos, la decisión pueda ajustarse a sus intereses, está siendo tomada con la ayuda de agentes externos que pueden aprovecharse de la vulnerabilidad de los usuarios para ejercer influencias encubiertas[115].

Ahora bien, es importante destacar que la aproximación anterior admite matices en ambos sentidos. En efecto, puede advertirse, por un lado, que, dado que los algoritmos

[111] *Ibíd*., p. 34.
[112] WERTENBROCH et al., op. cit., p. 432.
[113] *Ibíd*., p. 430.
[114] *Ibíd*., p. 431.
[115] *Ibíd.*, p. 431.

reducen los costos de búsqueda y ayudan a los consumidores a enfrentar sus disyuntivas de elección[116], vuelven más probable la realización de su verdadera voluntad, por lo cual potencian su autonomía real –y no solo la percibida–, eliminando toda clase de obstáculos que, normalmente, impiden al consumidor tomar una decisión adecuada.

Sin embargo, por otro lado, el hecho de que, existiendo tantas opciones en los mercados actuales, los algoritmos dirijan preferentemente hacia aquellas que se condicen con comportamientos o elecciones anteriores, dificulta a los consumidores conocer nuevas ofertas disponibles. En consecuencia, los consumidores no siempre quedarán satisfechos con sus decisiones ni habrá autonomía percibida[117], máxime si es que sus elecciones previas no fueron motivadas por patrones exteriorizables, sino por valores que resultan inaccesibles para el algoritmo[118].

De este modo, existen beneficios y riesgos tanto para la autonomía real como para la autonomía percibida. Ahora bien, podría sostenerse que todos los problemas de autonomía son parcialmente superables, en la medida en que el algoritmo actúe únicamente en interés de los consumidores y estos consientan libremente en ser orientados en su proceso de decisión.

Dicho planteamiento, *a priori,* cobra algo de sentido, si se tiene en cuenta que, según demostró un reconocido estudio, las personas poseen una confianza especial en los consejos brindados por algoritmos, hasta el punto de que les parecen mejores que los que podría brindar una persona experta[119]; de ahí que, naturalmente, podrían confiarle sus intereses.

Empero, sostener que, por el mero hecho de que los consumidores consientan libremente en que la IA tome decisiones por ellos, se solucionan los problemas de autonomía, no resulta satisfactorio. Lo anterior, no sólo porque existan otros estudios que indican que las

---

[116] ANDRÉ, Quentin, et al. Consumer choice and autonomy in the age of artificial intelligence and big data. Customer needs and solutions, 2018, vol. 5, p. 28-37. p.28.

[117] GRAFANAKI, Sofía. *Autonomy challenges in the age of big data*. Fordham Intell. Prop. Media & Ent. LJ. 27(4): 2016, p. 843.

[118] ANDRÉ, Quentin, et al. Consumer choice and autonomy in the age of artificial intelligence and big data. Customer needs and solutions, 2018, vol. 5, p. 28-37. p. 34.

[119] LOGG, Jennifer. M., MINSON, Julia. A., MOORE, Don .A., 2019. *Algorithm appreciation: People prefer algorithmic to human judgment.* Organizational Behavior and Human Decision Processes. 151: pp. 90-103, mar. 2019.

personas desconfían de la IA[120], sino también porque la complejidad de diseño de los sistemas de IA lleva a que los algoritmos sean opacos, de manera que, si para el proveedor es difícil entender sus procedimientos, con mayor razón lo será para el consumidor, cuyo consentimiento –en que la IA tome decisiones por él–, por lo mismo, estaría viciado[121].

Asimismo, aun cuando el consentimiento no sea viciado, lo cierto es que la autonomía del consumidor para dirigir sus actos de consumo es valiosa por sí misma, y no resulta válida una renuncia o limitación *ex-ante*, ni ética[122] ni jurídicamente[123]. A ello se agrega que: (i) las metapreferencias seguirán siendo difíciles de identificar mientras el consumidor no las comunique expresamente; (ii) pretender que los intereses del consumidor sean custodiados por la IA supone caer en un paternalismo problemático; y (iii) en última instancia, sería necesario asegurar que el algoritmo permita una elección libre real y no aparente[124], puesto que, de lo contrario, se transgrediría el principio ético de "respeto a la autonomía humana" que debe observarse en el uso y aplicación de IA[125].

Lo anterior no quiere decir que estos problemas sean insalvables y que el único modo de evitarlos sea prohibir el uso de la IA en las relaciones de consumo. Por el contrario, no solo pueden solucionarse, sino que conviene hacerlo, con el fin de aprovechar las grandes oportunidades que la IA brinda en orden a facilitar la toma de la decisión de consumo.

Un examen más detallado demuestra que se pueden resolver, al menos parcialmente, todos ellos. Sin embargo, se requiere identificar complicaciones concretas y emplear técnicas

---

[120] YEOMANS, Michael, et al. *Making sense of recommendations*. [en línea] Journal of Behavioral Decision Making, Feb-2019, Vol. 32, n° 4, p. 403-414 <https://onlinelibrary.wiley.com/doi/abs/10.1002/bdm.2118> [consulta: 17 septiembre 2023].

[121] BATHAEE, Yavar. *The Artificial Intelligence Black Box and the Failure of Intent and Causation*. Harvard Journal of Law & Technology (Harvard JOLT). 31 (2): 2018, p. 897.

[122] CORTINA, Adela. *Por una ética del consumo*. Madrid, Taurus, 2002. 241p. A mayor abundamiento, se ha demostrado que para los consumidores resulta valioso percibir sus procedimientos de decisión como autónomos, aun cuando no logren llegar a la decisión correcta. Véase: ANDRÉ et al, op. cit, p. 33.

[123] Ley Nº 19.496. CHILE. *Establece Normas sobre Protección de los Derechos de los Consumidores.* Ministerio Secretaría General de la Presidencia, Santiago, Chile, 07 de febrero de 1997. Artículo 4: "*Los derechos establecidos por la presente ley son irrenunciables anticipadamente por los consumidores"*.

[124] GRAFANAKI, op. cit, p. 855.

[125] EUROPEAN COMMISSION, 2019. *Ethics guidelines for trustworthy AI*, p. 15 [en línea], <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai,> [consulta: 04 julio 2023]. En virtud de este principio, "*Los sistemas de IA no deberían subordinar, coaccionar, engañar, manipular, condicionar o dirigir a los seres humanos de manera injustificada. En lugar de ello, los sistemas de IA deberían diseñarse de forma que aumenten, complementen y potencien las aptitudes cognitivas, sociales y culturales de las personas*".

de solución menos ingenuas. Para efectos esquemáticos, se agruparán los problemas expuestos en tres categorías.

En primer lugar, el riesgo de aprovechamiento y de ejercicio de influencias indebidas sobre el consumidor. Ello está estrechamente vinculado con la explotación intencional de sesgos cognitivos y la utilización de estrategias de diseño conocidas como "*dark patterns*". Los sesgos cognitivos son patrones predecibles de comportamiento que los seres humanos emplean en forma inconsciente y automática al momento de tomar decisiones[126]. Estos patrones pueden ser aprovechados por los proveedores para influir en el comportamiento de los consumidores. Dentro del comercio electrónico, la forma más común de hacerlo es a través de "*dark patterns*"[127].

Los "*dark patterns*"' son tácticas de diseño empleadas por las plataformas para manipular a los usuarios, llevándolos a adoptar cursos de acción que de otra manera no hubieran tomado[128]. El uso de estos patrones engañosos se vuelve más patente a medida que los procedimientos se automatizan, toda vez que el gran manejo de datos de los sistemas de IA, junto con su capacidad de procesamiento y análisis, facilita la restricción o dirección del entorno de elección e información disponible. De este modo, el proveedor puede forzar ciertos comportamientos en desmedro del consumidor, ya sea directa o indirectamente[129].

En segundo lugar, y relacionado con lo anterior, el hecho de que la IA –y, por ende, el proveedor– tenga injerencia en las decisiones del consumidor supone cierto grado de paternalismo. Ello es problemático, desde luego, en razón de que las asimetrías de información impiden que el proveedor sepa con exactitud qué es lo mejor para el consumidor; pero, también, por cuanto el proveedor queda en una posición de ventaja peligrosa.

En efecto, el proveedor puede emplear *dark patterns* con mayor facilidad para "'empujar" a los consumidores a desarrollar determinadas conductas, así como presentar o

[126] SUNSTEIN, Cass y THALER, Richard. *Un pequeño empujón*. 1ª ed. Madrid, Taurus, 2017. 15p.
[127] WALDMAN, Ari. *Cognitive biases, dark patterns, and the 'privacy paradox*'. Current Opinion in Psychology. 31: 2020, p. 107.
[128] *Ibíd*, p. 105. Traducción libre de: " (...) *design tricks platforms use to manipulate users into taking actions they might otherwise have not".*
[129] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 33 que Aprueba Circular Interpretativa sobre Protección de los Consumidores frente al uso de sistemas de Inteligencia Artificial en las relaciones de consumo. Santiago, Chile, 18 de enero de 2022.. 9p.

enmarcar la información de manera que refuerce esa dirección[130]. Cuando esto último se hace con el fin de ayudar o guiar a los consumidores, mediante el uso de elementos de interfaz de usuario, se está ante el fenómeno del "*digital nudging*"[131].

Según sostiene la literatura especializada, el *digital nudging* en sí no es algo malo, en tanto en cuanto se realice en forma leve, transparente e inteligente. De hecho, los *nudge* pueden ser una herramienta útil para evitar perjuicios a los consumidores en mercados complejos, siempre y cuando, en la práctica, el consumidor siga teniendo todas las opciones de consumo disponibles[132] . Empero, lo que sí es peligroso, es la posición de poder en la que queda el proveedor, que no solo puede ser usada para ayudar o guiar, sino también para explotar sesgos cognitivos a su favor o generar emociones negativas en el consumidor[133]. Ese es el real inconveniente al que se busca hacer referencia.

En tercer lugar, resulta problemática la dificultad de los algoritmos para identificar metapreferencias. Como se explicó, las metapreferencias son preferencias aspiracionales o valóricas que, pese a motivar el acto de consumo, no siempre están explícitas en él[134]. La naturaleza de los algoritmos impide que dichos valores puedan ser detectados y tratados adecuadamente.

Los primeros dos problemas pueden ser solucionados, en cierta medida, mediante la implementación de deberes de información por parte de los proveedores, así como a través de la transparencia y el control en el uso de la IA[135]. La transparencia alude a que exista una apertura de las operaciones, consideraciones, intenciones y comportamientos de la IA, con el fin de que aquellos actores que se ven afectados por su uso (en este caso, los consumidores) puedan monitorear el desempeño y funcionamiento de la tecnología[136]. Por su parte, el control

---

130 SUNSTEIN, Cass y THALER, Richard. *Un pequeño empujón*. 1ª ed. Madrid, Taurus, 2017. 54p.

131 WEINMANN, Marcus, SCHNEIDER, Christoph, BROCKE, Jan Vom. *Digital nudging*. Business & Information Systems Engineering, 58, p. 433, oct. 2016.

132 Para más detalles sobre el buen uso del digital nudging, véase: *Smart nudging: How cognitive technologies enable choice architectures for value co-creation* por Cristina Mele "et al". Journal of Business Research, 129, pp. 949-960.

133 PANTANO, Eleonora y SCARPI, Daniele. *I, robot, you, consumer: Measuring artificial intelligence types and their effect on consumers emotions in service*. Journal of Service Research 25(4): p. 595, 2022.

134 ANDRÉ, Quentin, et al. Consumer choice and autonomy in the age of artificial intelligence and big data. Customer needs and solutions, 2018, vol. 5, p. 28-37. p. 34.

135 MIK, Eliza. *The erosion of autonomy in online consumer transactions*. Law, Innovation and Technology. 8(1): 2016, p. 32.

136 FELZMANN, Heike, et al. *Towards transparency by design for artificial intelligence.* Science and Engineering Ethics, 26(6):3333-3361, 2020. p. 3336.

implica que exista una regulación administrativa, institucional y/o legal en el empleo de IA, que se asocia comúnmente a la vigilancia humana[137].

Todo lo anterior ayudaría a disminuir la probabilidad de que los proveedores hagan mal uso de su posición y ejerzan influencias indebidas sobre la voluntad de los consumidores, por cuanto existiría publicidad respecto de los sistemas utilizados y se supervisaría el comportamiento de los proveedores. Esto, al menos en principio, los llevaría a abstenerse de utilizar algoritmos que manipulen la toma de decisiones.

No obstante, es importante tener presente que la IA es opaca, en el sentido de que el funcionamiento de sus algoritmos es tan complejo que sus operaciones se presentan como una verdadera "caja negra" incomprensible para el humano promedio[138]. Ello, sumado a que los proveedores suelen emplear *dark patterns* en el diseño de interfaz de la IA, dificulta severamente la calidad de la explicabilidad, transparencia y control[139]. En otras palabras, sería complejo cumplir a cabalidad con los deberes de información y transparencia en el uso de la tecnología, de modo que la autonomía de los consumidores no siempre quedaría bien resguardada.

Por tanto, la prevención de riesgos debe, necesariamente, complementarse con otros deberes de comportamiento del proveedor y de los agentes que crean la tecnología, como el deber de profesionalidad y la transparencia por diseño, respectivamente. Se volverá sobre esto en los dos capítulos siguientes, al momento de analizar las herramientas que prevé nuestra legislación y que se han propuesto en el extranjero para resolver los desafíos planteados por el uso de IA en las relaciones de consumo.

Por su parte, el tercer problema (identificación de metapreferencias) no se asocia al mal o buen uso de la IA, sino a las limitaciones ínsitas de los algoritmos. De ahí que la solución a su respecto sea de naturaleza distinta. Dado que la esencia del problema radica en que los

---

[137] HUESO, Lorenzo Cotino. *Riesgos e impactos del Big Data, la inteligencia artificial y la robótica: enfoques, modelos y principios de la respuesta del derecho*. Revista general de Derecho administrativo. (50): pp.15-18, 2019.
[138] BATHAEE, Yavar. *The Artificial Intelligence Black Box and the Failure of Intent and Causation*. Harvard Journal of Law & Technology (Harvard JOLT). 31 (2): 2018, p. 892.
[139] CHROMIK, Michael, et al. *Dark Patterns of Explainability, Transparency, and User Control for Intelligent Systems.* [en línea] IUI workshops, 2019 <https://www.medien.ifi.lmu.de/pubdb/publications/pub/chromik2019iuiworkshop/chromik2019iuiworkshop.pdf> [consulta: 28 noviembre 2023]: pp. 3-5.

algoritmos no cuentan con información sobre las aspiraciones del consumidor ni sus deseos de cambio, una solución idónea podría ser que los sistemas de IA, mediante asistencia virtual, consulten al consumidor si es que desea hacer explícitas sus valores o aspiraciones, advirtiéndole que, si bien es algo voluntario, puede resultar de gran ayuda para evitar daños y efectos contraproducentes. De este modo, se respetaría tanto la autonomía como la privacidad de los consumidores.

II. Derecho a la vida privada y protección de datos personales

En Chile el derecho a la vida privada se encuentra consagrado en diversos cuerpos normativos, tanto nacionales como internacionales, de los cuales cabe hacer especial mención a los dos más importantes: (i) la Constitución Política de la República, la cual contempla expresamente en su artículo 19 Nº 4 que "*La Constitución asegura a todas las personas: 4º El respeto y protección a la vida privada y a la honra de la persona y su familia*"[140]; y, (ii) la Ley Nº 19.628, sobre Protección de la Vida Privada[141], que aborda de manera específica materias relacionadas con la protección de datos personales y la vida privada de los ciudadanos.

El derecho a la vida privada y la protección de datos personales están estrechamente relacionados y se complementan mutuamente. Aunque son conceptos distintos, se superponen en el ámbito de la protección de la información personal de los individuos. Por un lado, según ha señalado la Corte Interamericana de Derechos Humanos,

> *"La protección a la vida privada abarca una serie de factores relacionados con la dignidad del individuo, incluyendo por ejemplo la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus propias relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior. La efectividad del ejercicio del derecho a la vida privada es decisiva para la posibilidad de ejercer la autonomía*

[140] MINISTERIO Secretaría General de la República (Chile). Decreto 100, que fija el texto refundido, coordinado y sistematizado de la Constitución Política de la República de Chile. Santiago, Chile, 2005. Artículo 19 Nº4.
[141] Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999.

personal sobre el futuro curso de eventos relevantes para la calidad de vida de la persona. La vida privada incluye la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás, y es una condición indispensable para el libre desarrollo de la personalidad"[142].

Por su parte, el derecho a la protección de datos personales, también conocido como "autodeterminación informativa"[143], "*nos otorga a las personas la facultad de controlar nuestros datos personales, disponer y decidir sobre esos datos y su uso*"[144]. En otras palabras, se refiere a las medidas y regulaciones destinadas a salvaguardar la información que identifica a una persona o la hace identificable. Esto incluye datos como nombres, direcciones, números de teléfono, identificadores biométricos, información financiera, historial médico, entre otros.

Así las cosas, el objetivo principal de la protección de datos personales es garantizar la facultad del individuo de decidir básicamente por sí sólo sobre la difusión y utilización de sus datos personales[145]. Al respecto, el Tribunal Constitucional español ha señalado que la autodeterminación informativa se distingue de la privacidad e intimidad en cuanto el primero

> "[A]*tribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales*", incluyendo "*el derecho a que se requiera el previo consentimiento para la recogida y uso de datos personales, el derecho a saber y ser informado sobre el destino y uso de rectificar y cancelar dichos datos. En definitiva, el poder de disposición sobre los datos personales*"[146].

De esta manera, la relación entre ambos derechos se basa en que el derecho a la privacidad abarca la esfera más amplia de la intimidad y el control sobre la propia información

---

[142] CIDH, Caso Artavia Murillo y Otros ("Fecundación in vitro") vs. Costa Rica, Sentencia de Fondo (Excepciones Preliminares, Fondo, Reparaciones y Costas), de 28 de noviembre de 2012, párr. 143.
[143] CONTRERAS, Pablo. *El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena*. Estudios Constitucionales. 18(2): 2020, p.87.
[144] ARELLANO LÓPEZ, Christian Alberto. 2020. *El derecho de protección de datos personal*es. [en línea] Biolex, 12(23): 163-174. <https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-55452020000200009> [consulta: 15 septiembre 2023]. p.169.
[145] CONTRERAS, op. cit., p. 104.
[146] STCE, 254/1993, FJ. 7.

personal, mientras que la protección de datos se enfoca específicamente en la seguridad y el manejo adecuado de los datos personales.

En el ámbito del Derecho de Protección a los Consumidores, el derecho a la vida privada y la protección de datos personales juegan un papel fundamental, en tanto, aunque el enfoque principal de esta área del derecho es garantizar los derechos de los consumidores en general, también se reconocen y protegen los derechos relacionados con la vida privada y los datos personales de los consumidores.

A su respecto, por ejemplo, nos encontramos con la guía de Principios Actualizados sobre la Privacidad y la Protección de datos personales[147] publicada por la Organización de los Estados Americanos (En adelante "**OEA**") en el año 2021. Estos principios incluyen la finalidad legítima, la calidad de los datos, el consentimiento, la seguridad, la transparencia, la responsabilidad y la accesibilidad.

Protección de datos personales en los sistemas de IA

Como se ha señalado previamente, el derecho de protección de datos personales le confiere al titular del dato el poder de decisión sobre el tratamiento de su información, desde que se recaba hasta que se destruye. Este derecho cobra vida a través de los denominados derechos ARCO, consistentes en los derechos de: acceso, rectificación, cancelación y oposición frente al tratamiento de datos personales[148].

Los sistemas de IA reciben cantidades ingentes de datos, muchos de los cuales son de carácter personal. De hecho, algunos de los dispositivos basados en IA son recolectores masivos de datos personales que se infiltran de manera imperceptible en nuestra vida cotidiana. Es decir, no todos los datos que se recogen cuentan con conocimiento y consentimiento de los interesados.

---

[147] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), 2021. *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales* [en línea]. <https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf> [consulta: 09 julio 2023].

[148] MENDOZA, Olivia. *El derecho de protección de datos personales en los sistemas de inteligencia artificial.* REVISTA IUS. 15(48): 2022, p. 15.

A esto hay que añadir el hecho de que los sistemas de IA procesan de manera cada vez más compleja toda esta información personal y consiguen resultados a menudo impensables a partir de algunos datos desagregados y/o anónimos. Por todo ello, la protección de datos es uno de los retos que suelen señalarse en el caso de los sistemas de IA[149].

La IA puede emplear la tecnología para extraer conclusiones a partir de datos por medio de algoritmos de una manera independiente de la voluntad humana, y puede provocar, por ello, riesgos en los derechos de los consumidores que deben ser conjurados. Con las tecnologías que incorporan la IA, las máquinas pueden actuar y aprender por medio de una combinación de algoritmos cuya finalidad es asemejarse en todo lo posible a las capacidades del ser humano.

Los algoritmos no sólo emplean datos personales de los sujetos, sino que a partir de estos datos se pueden elaborar más volúmenes de datos que aportan una información sobre el individuo totalmente desconocida para este último. Respecto de este tipo de datos habrá que determinar cómo se aplican el consentimiento, el derecho a la información, el principio de finalidad o el ejercicio de los derechos de la ciudadanía[150].

Es indispensable que todos y cada uno de los sistemas de inteligencia artificial que sean empleados o comercializados en el mercado respeten a cabalidad la legislación vigente acerca de la protección de datos personales, de forma de encuadrar su actuación dentro de los límites que establece la ley[151].

Con todo, se requiere una regulación específica en la materia, la cual debe ser accesible y previsible, que exista un equilibrio entre el objetivo legítimo perseguido y la interferencia en la vida privada de los consumidores[152], y la configuración de mecanismos específicos para que los Estados supervisen el cumplimiento de los alcances de este derecho humano en la IA (principio de escrutinio) y habilitar nuevas manifestaciones del derecho de protección de datos personales para que los consumidores tengan mecanismos concretos de defensa frente a las consecuencias de los tratamientos de datos a través de IA (mecanismos

[149] FERNÁNDEZ-ALLER, Celia y SERRANO, María. *¿Es posible una Inteligencia artificial respetuosa con la protección de datos?* Doxa. Cuadernos de Filosofía del Derecho (45): p. 2, 2022.
[150] *Ibíd*., p. 5.
[151] *Ibíd*., p. 5.
[152] *Ibíd*., p. 7.

de reclamación, de no identificación y de no tratamiento de datos en sistemas de IA)[153]. Algunos de dichos fines pueden lograrse al hacer aplicación del principio de transparencia, que será analizado en el tercer capítulo.

Elaboración de perfiles

En directa relación con lo anterior, es menester referirnos a lo que se conoce como "perfilamiento" o, en inglés, "*profiling*", consistente en la posibilidad de extraer patrones de comportamiento y perfiles personales[154].

En la actualidad, las empresas pueden acceder a una cantidad ingente de datos, gracias a lo que se conoce como *big data,* y además, pueden procesarlos de forma automática o semi-automática, todo ello gracias al *machine learning,* lo que les permite no solo crear perfiles detallados de los consumidores, sino también adaptar estratégicamente los precios y las ofertas en función de estos perfiles personalizados[155], lo que acrecienta aún más las asimetrías de información propias de la relación de consumo y genera problemas de privacidad[156].

Asimismo, la elaboración de perfiles socava la capacidad de las personas para ejercer el control sobre sus datos personales, aumenta el riesgo de discriminación -utilizando información sensible- y de manipulación que podría afectar a cuestiones y procesos políticos, al acentuar vulnerabilidades y emociones negativas afectando a la autonomía, la libertad e, incluso, la salud psicológica[157].

De esta manera, la cantidad enorme de información que circula sobre cada una de las personas en distintas plataformas y bases de datos, que, en principio, parece insignificante, termina por permitir a quienes recolectan estos datos la creación de perfiles altamente detallados, que, al final, pueden conocernos mejor de lo que nos conocemos nosotros mismos.

---

[153] MENDOZA, op. cit., p. 24.

[154] CRAIG, T. y LUDLOFF, M. E. *Privacy and Big Data: The Players, Regulators, and Stakeholders.* Newton, Massachusetts, O'Really Media, 2011. p. 6.

[155] *Ibíd*.

[156] EUROPEAN COMMISSION, 2019. *Ethics guidelines for trustworthy AI*, p. 15 [en línea], <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai,> [consulta: 04 julio 2023].

[157] EUROPEAN DATA PROTECTION BOARD. Directrices 8/2020 sobre la focalización de los usuarios de medios sociales, Versión 2.0, adoptadas el 13 de abril de 2021, p. 7.

Paradoja de la privacidad

Sin perjuicio de lo anteriormente expuesto, hemos de tener en consideración una cuestión sumamente importante y que afecta directamente la privacidad de los consumidores: la "paradoja de la privacidad". La paradoja de la privacidad explica que, por un lado, los individuos muestran preocupación por la privacidad de su información, pero, por otro lado, suelen revelar dicha información por pequeñas recompensas[158]. En otras palabras, esta "paradoja" radica en que, aunque muchas personas son conscientes de los riesgos para la privacidad, siguen compartiendo información personal en línea -principalmente a sistemas de IA-.

Esta paradoja representaría un comportamiento irracional de los consumidores, lo cual rompe con uno de los supuestos fundamentales de la teoría microeconómica referido a que el individuo toma sus decisiones de manera racional[159]. Ello se debe, en parte, a la comodidad, el sentido de comunidad y la presión social para estar presentes en las plataformas digitales. Además, las políticas de privacidad a menudo son complejas y poco claras, lo que dificulta que los usuarios comprendan completamente cómo se utilizarán sus datos.

Ahora bien, al contrario de lo que se tiende a pensar, el porqué de la paradoja de la privacidad no radica exclusivamente en el comportamiento de los consumidores, sino que existe una multiplicidad de factores que influyen en ello, entre los cuales se encuentra, por ejemplo, la falta de información[160].

Se han realizado múltiples investigaciones con el propósito de comprender a cabalidad esta paradoja, mas no existe una respuesta unívoca que la explique. A su respecto, Hargittai & Marwick han señalado que:

> *"[L]a presencia simultánea de desconocimiento del riesgo y uso de comportamientos protectores de la privacidad sugiere que la paradoja de la*

[158] KOKOLAKIS, Spyros. *Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon*. Computers & Security. 64: 2017, p.3.
[159] MANTILLA Gonzales de la Cotera, Eduardo Javier. *La paradoja de la privacidad de la información en los servicios de Internet*. Tesis (Maestría en Investigación en Ciencias de la Administración). Lima, Perú. Universidad ESAN, Graduate School of Business, 2019, p. 15.
[160] *Ibíd.*, p. 15.

privacidad no puede atribuirse únicamente a la falta de comprensión o a la falta de interés en la privacidad.

En cambio, los comentarios de los participantes sugieren que los usuarios tienen una sensación de apatía o cinismo acerca de la privacidad en línea. Creen que las violaciones a la privacidad son inevitables y la exclusión no es una opción. Explicamos esta apatía utilizando el constructo de privacidad en red (Marwick & boyd, 2014), que sugiere que en entornos sociales altamente interconectados, la capacidad de los individuos para controlar la propagación de su información personal se ve comprometida por violaciones tanto tecnológicas como sociales de la privacidad. La privacidad no es un proceso individual, sino un esfuerzo colectivo que requiere la cooperación de aquellos con quienes existe conexión en las redes sociales, así como las posibilidades tecnológicas de los propios sitios web que manejan estas plataformas. Entendiendo esto, los adultos jóvenes recurren a una variedad de estrategias sociales imperfectas, pero creativas, para mantener control y agencia sobre sus datos personales"[161].

De esta manera, entonces, existen muchísimos factores que influyen en que los consumidores tomen decisiones que afectan su derecho a la privacidad, supeditándolo a otros intereses, a su juicio, "superiores" (por ejemplo, agilizar la compra), ya sea por desconocimiento o porque, en realidad, ya se encuentran "rendidos" ante el inminente tratamiento de sus datos[162].

Esta paradoja se ve acrecentada en el contexto de la IA. La IA, especialmente el aprendizaje automático y el análisis de grandes cantidades de datos, depende en gran medida de tener acceso a una amplia gama de información para funcionar de manera eficaz y producir resultados precisos. Sin embargo, esto crea un conflicto entre la necesidad de utilizar datos

[161] Traducción libre de: HARGITTAI, Eszter y MARWICK, Alice. *"What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy.* International Journal of Communication 10(0): p. 3752, 2016.

[162] ANIC, Ivan-Damir, ŠKARE, Vatroslav y KURSAN, Ivana. 2019. *The determinants and effects of online privacy concerns in the context of e-commerce.* Electronic Commerce Research and Applications, 36 (100868), pp.7-9 (100868).

personales para alimentar los modelos de IA y la preservación de la privacidad de los individuos cuyos datos están siendo utilizados[163].

La recopilación masiva de datos personales para el entrenamiento de algoritmos de IA plantea preocupaciones significativas en términos de privacidad y seguridad. Cuando los datos recopilados contienen información personal sensible, como historiales médicos, información financiera o datos de ubicación, existe el riesgo de que esta información pueda ser utilizada de manera inadecuada o caer en manos equivocadas.

Para abordar la paradoja de la privacidad en la IA podrían utilizarse diversos enfoques, tales como técnicos, legales y éticos, atendida la multidimensionalidad de la problemática. Algunas estrategias que se podrían utilizar son, por ejemplo, la incorporación de prácticas de privacidad en todas las etapas del desarrollo de la IA para minimizar la cantidad de datos personales utilizados y asegurarse de que se protejan adecuadamente; el desarrollo un marco normativo que proteja la privacidad y asegure el uso ético de la IA en diferentes contextos; y la utilización técnicas de aprendizaje federado y técnicas de procesamiento en el dispositivo para limitar la cantidad de datos personales que se comparten centralmente, entre otros.

Sin perjuicio de ello, los riesgos pueden disminuirse, en buena medida, a través del deber de informar veraz y oportunamente y del principio de transparencia, que serán analizados en la primera sección del tercer Capítulo (“Herramientas consagradas en la Ley para resolver los desafíos planteados por el uso de la IA en las relaciones de consumo”).

III. Integridad del consumidor

Mediante la expresión “integridad del consumidor”, se busca abarcar todos los derechos que corresponden al consumidor en orden a evitar cualquier tipo de perjuicio y peligro, ya sea físico, psicológico, material o ambiental, que pueda surgir como consecuencia de su participación en una relación de consumo. Así, quedan comprendidos la seguridad en el consumo (artículos 3º

[163] SMITH, Gary. *Artificial Intelligence and the privacy paradox of opportunity, Big Data and the Digital universe.* En: 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (2019). pp. 150-153.

letra d), 45 y 46 LPDC), la proscripción de la discriminación arbitraria (artículo 3º letra c) LPDC) y el derecho a la adecuada y oportuna reparación e indemnización (artículo 3º letra e) LPDC).

Según ha señalado la abogada experta en Derecho de los Consumidores, Érika Isler, "*[El] derecho a la seguridad en el consumo tiene por objeto resguardar la integridad del consumidor -material o jurídico-, propendiendo a que los bienes y servicios que se transan en el mercado, sean inocuos y no generen daño para su persona o bienes*"[164]. Con todo, cabe precisar que, según se desprende del artículo 3 letra d) LDPC, la seguridad en el consumo protege no solo la integridad física, psíquica y material del consumidor, sino también el medio ambiente[165].

Por su parte, la proscripción de la discriminación arbitraria impide que el proveedor establezca tratos diferenciados entre consumidores de forma caprichosa, desproporcionada, injustificada o no razonable[166]. El objeto de esta prohibición es resguardar la integridad psíquica y la dignidad de los consumidores[167].

Por último, el derecho a adecuada y oportuna reparación e indemnización constituye una manifestación del principio de reparación integral[168], en tanto garantiza, por mandato expreso del legislador, "que el consumidor quede indemne respecto de "todos los daños" que le hayan ocasionado, sean materiales o morales[169].

La interacción entre los sistemas de IA y estos derechos es variada. Por un lado, los algoritmos de analítica predictiva pueden ser utilizados para prevenir daños a los consumidores con un alto grado de acierto. En efecto, cuentan con el potencial de anticipar cursos de acción y activar mecanismos protectores "*mucho antes de que un daño se produzca*

---

164 ISLER, Erika. *Derecho del consumo. Nociones fundamentales*. Valencia, Tirant lo Blanch, 2021. 228p.

165 Ello se debe a que el legislador entendió que los daños al medio ambiente suponen también riesgos indirectos hacia la integridad de los consumidores, en el sentido de que es "*el consumidor quien termina pagando*". Véase: BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. *Historia de la Ley N° 19.496*. [en línea] <https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6746/>, pp. 73-74. [consulta: 12 septiembre 2023].

166 ISLER Soto, Erika. *Aproximación al derecho a la no discriminación arbitraria en el régimen de la Ley 19.496.* Revista de Derecho Público (4): 2016, pp. 103-104.

167 *Ibíd.*, p. 103.

168 *Ibíd.*, p. 236.

169 DFL 3. CHILE. Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021. Artículo 3 letra e).

efectivamente"[170], por lo que pueden generar condiciones de comercialización que sean menos propensas al riesgo. Lo mismo ocurre con los algoritmos de *machine learning*, cuya funcionalidad permite, por ejemplo, ejercer un control sobre cláusulas contractuales potencialmente abusivas[171].

Adicionalmente, la capacidad de la IA para automatizar procesos y reducir costos puede incentivar[172] al proveedor a adaptarse a las nuevas demandas y agregar valor sustentable a sus productos, sin que esto implique un aumento de los precios[173]. De este modo, se fomentaría la protección al medio ambiente y se reducirían las externalidades negativas de los mercados.

No obstante, por otro lado, las limitaciones y los sesgos de los algoritmos suponen serios riesgos para la integridad psíquica de los consumidores[174]. Los peligros pueden ser de dos tipos: (i) vinculados al desconocimiento de metapreferencias[175] o (ii) vinculados a discriminaciones arbitrarias[176].

Además, si bien es cierto que los sistemas de IA pueden ser utilizados para prevenir daños, también es posible que ocasionen menoscabos físicos y psicológicos al consumidor. Cuando dichos daños llegan a materializarse, se produce una situación problemática desde el punto de vista de la responsabilidad civil extracontractual, puesto que, en la mayoría de los casos, el consumidor enfrentará grandes dificultades de prueba y no sabrá quién es la persona

[170] CHAMATROPULOS, op. cit., p. 5.
[171] LIPPI, Marco, et al. CLAUDETTE: an automated detector of potentially unfair clauses in online terms of service. [en línea] Artificial Intelligence and Law, Feb-2019, vol. 27, pp. 117-139 <https://link.springer.com/article/10.1007/s10506-019-09243-2> [consulta: 04 octubre 2023]. pp. 128-130.
[172] Se plantea la afirmación en términos de "puede incentivar", porque, aun cuando exista doctrina al respecto, no se puede asumir que el proveedor siempre canalizará estos ahorros en ayudar al entorno.
[173] CHAMATROPULOS, op. cit., pp. 6-7.
[174] COMISIÓN EUROPEA, 2020. *LIBRO BLANCO sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza.* [en línea], p. 14, <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065> [consulta: 07 julio 2023].
[175]ANDRÉ, Quentin, et al. Consumer choice and autonomy in the age of artificial intelligence and big data. Customer needs and solutions, 2018, vol. 5, p. 28-37. p. 34.
[176] ZUIDERVEEN, Frederik, 2018. *Discrimination, artificial intelligence, and algorithmic decision-making* [en línea], pp. 10-14. Council of Europe, Directorate General of Democracy, <https://pure.uva.nl/ws/files/42473478/32226549.pdf> [consulta: 08 julio 2023].

o entidad potencialmente responsable por los daños[177]. Ello podría afectar el derecho a la debida reparación e indemnización.

A ello cabe agregar las complicaciones que, en nuestro medio, enfrenta el régimen de responsabilidad infraccional cuando el proveedor comercializa productos o servicios que incorporan IA, y estos, pese a no presentar fallas técnicas patentes, ejercen acciones autónomas e imprevisibles que causan daños al consumidor[178].

Así las cosas, los sistemas de IA pueden ayudar a evitar daños (principalmente físicos) y generar incentivos para ayudar al medio ambiente; pero, al mismo tiempo, pueden poner en riesgo la integridad psíquica de los consumidores y dar lugar a situaciones de responsabilidad difusa –tanto en el ámbito civil como en el infraccional–. Se abordará cada problema y sus posibles soluciones.

En lo relativo al desconocimiento de metapreferencias, se hace remisión al ejemplo expuesto al momento de analizar la autonomía del consumidor. Como se explicó, el hecho de que los algoritmos no tengan en cuenta las aspiraciones o valores de los consumidores puede derivar en un "*data mining*" lesivo, al incentivar el desarrollo de conductas que el consumidor en algún momento quiso potenciar, pero actualmente desea evitar.

Los siguientes apartados centrarán la atención en la discriminación arbitraria y en la responsabilidad difusa, por ser problemas que aún no se han analizado. Se explicarán ambas expresiones, se darán algunos ejemplos y se analizará la relevancia de estos riesgos en relación con la integridad de los consumidores.

Discriminación arbitraria

El libre albedrío en el uso de la IA se justifica con una frase: "no existe regulación", lo cual, si bien pareciera ser cierto en principio, no lo es, puesto que no es necesaria una norma específica que prohíba discriminar a través del uso de sistemas de IA. Ya tenemos, bien

[177] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022. Considerandos 17 y 28.

[178] ARAYA Paz, Carlos. *Desafíos legales de la inteligencia artificial en Chile*. Revista chilena de derecho y tecnología. 9 (2): 257-290, 2020. pp. 278-279. El autor indica que la situación es compleja, porque no se puede subsumir dicha hipótesis directamente en el régimen de responsabilidad del artículo 23 LPDC.

enraizado, un derecho humano que veda absolutamente la discriminación en cualquiera de sus formas[179]. Asimismo, como se explicó, en materia de consumo existe una norma específica que también lo prohíbe.

Ahora bien, lo anterior no significa que, en la práctica, no exista discriminación arbitraria en desmedro los consumidores. Si bien es cierto que los algoritmos, por definición, discriminan datos, la esencia del problema se encuentra en que tal discriminación se produzca de forma arbitraria, en tanto los modelos de IA pueden adquirir un sesgo que los lleve a presentar un rendimiento dispar en grupos caracterizados por distintos atributos demográficos, lo que redunda en un comportamiento desigual o discriminatorio[180].

En virtud de lo anterior, en esta materia se entiende que la discriminación es esencialmente arbitraria cuando proviene de sesgos algorítmicos, vale decir, sistemas cuyas predicciones benefician a un grupo de individuos frente a otro, resultando así injustas, desiguales o no razonables[181].

Si bien cuando hablamos de "sesgos algorítmicos" pareciera ser que el problema son los algoritmos, ello no es así. Los algoritmos no son discriminatorios *per se*: la tecnología es neutral y nosotros somos quienes transferimos nuestros valores a todo lo que hacemos, incluyendo los algoritmos[182], lo cual puede ser de forma intencionada o, incluso, inconsciente o sin quererlo.

Al respecto, vale mencionar que existen tres maneras en las cuales los sesgos se transfieren a los algoritmos. En primer lugar, los programadores, esto es, las personas que se encargan de la creación y actualización de los sistemas de inteligencia artificial, quienes, en tanto personas, poseen sus propios prejuicios. En segundo lugar, los datos de entrenamiento, es decir, aquellos datos que se utilizan en el proceso de formación y/o creación de los sistemas, los cuales, si no han sido bien seleccionados, pueden ser inadecuados, sobre o infra representativos o insuficientes, por ejemplo. Finalmente, en tercer lugar, los sesgos pueden

[179] DANESI, op. cit., p. 31.
[180] FERRANTE, op. cit, p. 33.
[181] *Ibíd*., p. 29
[182] DANESI, op. cit., p. 135.

prevenir del aprendizaje, el cual se produce por las interacciones que hace el sistema con el entorno una vez puesto en circulación[183].

De esta manera, los sesgos algorítmicos provenientes de las tres fuentes mencionadas anteriormente pueden tener un gran impacto en temas como la privacidad o agravar sesgos sociales como los existentes respecto a razas, género, sexualidad o etnias, entre otros, y pueden repercutir en los algoritmos teniendo como origen influencias culturales, sociales, o institucionales debido a limitaciones técnicas de su diseño. En relación a esta materia, a continuación se abordarán tres ejemplos de discriminación arbitraria que se encuentran latentes en la actualidad: de precios, de género y racial.

i. Discriminación de precios

Si bien la discriminación de precios no es algo nuevo, esta se ha acrecentado muchísimo con la masificación del comercio en línea, pues los algoritmos pueden utilizar información personal para definir los precios de los productos o servicios basándose, entre otros factores, en la capacidad de pago o "precio de reserva" de los consumidores, es decir, teniendo como consideración principal lo que el cliente estaría dispuesto a pagar por un determinado producto[184].

Gautier, Itto y Van Cleynenbreugel han señalado que la discriminación de precios consiste en cobrar a diferentes consumidores precios diferentes por productos iguales o similares[185], maquinación que es de mucho más fácil acceso en la actualidad, atendida la cantidad masiva de información –incluyendo datos personales– que circula en línea y que día a día sigue creciendo a ritmos inconmensurables.

En concreto, el conflicto radica en que los algoritmos de IA tienen la capacidad de crear perfiles personalizados de los consumidores en base a sus datos personales, contenido que consumen en línea, ubicación, hábitos de compra, entre otros, y, posteriormente, incorporarlos

[183] *Ibíd.*, pp. 152-158.
[184] JUÁREZ, Isabel Antón, et al. Marketplaces que personalizan precios a través del big data y de los algoritmos: ¿esta práctica es legal en atención al derecho de la competencia europeo?. Cuadernos de derecho transnacional, 2021, vol. 13, no 1, p. 42-69. p.52.
[185] Op. cit.

en aplicaciones de marketing o fijación de precios para precios personalizados (y recomendaciones de productos personalizadas)[186].

En otras palabras, las empresas pueden acceder a una cantidad ingente de datos, gracias a lo que se conoce como *big data,* y además, pueden procesarlos de forma automática o semi-automática, todo ello gracias al *machine learning,* lo que les permite no solo crear perfiles detallados de los consumidores, sino también adaptar estratégicamente los precios y las ofertas en función de estos perfiles personalizados.

ii. Discriminación contra la mujer

Un segundo ejemplo de discriminación arbitraria en que el uso de sistemas de IA puede influir sustancialmente es la discriminación de género, en tanto pueden estar contaminados con sesgos algorítimicos que reflejen estereotipos de género, lo cual puede dar lugar a resultados discriminatorios en desmedros de las mujeres.

Según señala la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer ("CEDAW"), la discriminiación contra la mujer denota "*toda distinción, exclusión o restricción basada en el sexo que tenga por objeto o por resultado menoscabar o anular el reconocimiento, goce o ejercicio por la mujer, independientemente de su estado civil, sobre la base de la igualdad del hombre y la mujer, de los derechos humanos y las libertades fundamentales en las esferas políticas, económicas, social, cultural y civil o en cualquier otra esfera"*[187].

En el mundo que vivimos hoy, lamentablemente, la violencia de género aún no ha sido erradicada y, más aún, ha surgido en nuevos ámbitos, tal como la violencia de género algorítmica, que nace al amparo de la inteligencia artificial, los algoritmos en los que esta se basa y los sesgos que se producen en el tratamiento de los datos[188].

---

[186] *Ibíd*.

[187] ORGANIZACIÓN DE NACIONES UNIDAS (ONU). 1979. Convención sobre la eliminación de todas las formas de discriminación contra la mujer. [en línea] <https://www.oas.org/dil/esp/convencion_sobre_todas_las_formas_de_discriminacion_contra_la_mujer.pf> [consulta: 12 de octubre de 2023].

[188] PETRILLO, P. *Las violencias invisibles: sesgo algorítmico, discriminación y violencia algorítmica de género.* Diario La Ley, 2022, 86(94), 1-5. p.3.

Así las cosas, los sistemas de IA pueden estar contaminados con sesgos algorítmicos que reflejen estereotipos de género, lo cual puede dar lugar a resultados discriminatorios en desmedro de las mujeres. Esto puede ocurrir, por ejemplo, en procesos de selección de personal, donde los algoritmos pueden estar programados para favorecer a los hombres en detrimento de las mujeres.

La discriminación de género en la IA también puede manifestarse en la falta de diversidad en los equipos de desarrollo de estos sistemas. Si los equipos de desarrollo están compuestos principalmente por hombres, es posible que los sesgos de género se vean reflejados en los algoritmos y en los resultados que producen. Por lo tanto, es importante fomentar la diversidad en los equipos de desarrollo de IA y promover la inclusión de mujeres y personas de otros géneros.

iii. Discriminación racial

Un tercer ejemplo importante de discriminación arbitraria en la cual los sesgos algorítmicos pueden influir de manera sustancial es la discriminación racial. Los sesgos algorítmicos pueden manifestarse en varios contextos relacionados con la raza, como el sistema de justicia penal, el acceso a crédito, el empleo y la vivienda, entre otros.

Respecto de lo que ocurre en el caso del sistema de justicia penal, es bastante común que los mecanismos de IA creados para realizar predicciones de reincidencia resulten, finalmente, discriminatorios. Estos sistemas se emplean, a grandes rasgos, para evaluar el riesgo de que los individuos que han sido condenados por delitos vuelvan a delinquir en el futuro. Sin embargo, lo que resulta problemático de todo esto recae en qué características y factores se consideran para realizar esta evaluación, ya que existe el riesgo de caer en el derecho penal de autor, en el cual se sanciona a las personas por sus características personales y no por sus actos[189].

De hecho, este temor del que hablamos se materializó en Estados Unidos, mediante el uso del algoritmo “Compas” (*Correctional Offender Management Profiling for Alternative*

[189] SÁNCHEZ VÁSQUEZ, Carolina; TORO-VALENCIA, José. El derecho al control humano: Una respuesta jurídica a la inteligencia artificial. [en línea] Revista chilena de derecho y tecnología. Dic-2021, Vol. 10, n° 2 <https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842021000200211> [consulta: 16 de agosto de 2023].

Sanctions), el cual es utilizado en diversos Estados del país para colocar un puntaje de probabilidad de reincidencia que tiene un sujeto y que se nutre mediante un formulario que deben llenar las personas cuando son detenidas, sin asesoramiento jurídico, el cual contiene preguntas como "una persona que tiene hambre, ¿tiene derecho a robar?"[190].

Este riesgo de discriminación racial también puede afectar a los consumidores. Ello ocurre cuando el proveedor, fundándose en los resultados arrojados por los sistemas de IA que emplea –típicamente, la videovigilancia o las alarmas automáticas–, acusa erróneamente al consumidor de haber cometido un delito en su tienda o le niega el acceso con motivo de su apariencia[191]. De ser así, estaríamos ante un tipo discriminación arbitraria expresamente prohibido por el artículo 15 de la LPDC[192].

Cabe destacar que, para configurar la responsabilidad del proveedor por la infracción a dicho precepto, no es necesario que se haya celebrado un contrato entre él y el consumidor[193]. Además, el hecho de que los sistemas de seguridad empleados sean manejados por una empresa externa no constituye un eximente de responsabilidad, toda vez que, en tal caso, el proveedor sería garante de su elección de contratación (*culpa in eligendo*) y respondería como intermediario (artículo 43 LPDC)[194].

***

Para abordar la discriminación de precios, de género y racial y los sesgos algorítmicos es necesario mejorar la transparencia[195] y la responsabilidad en el diseño y uso de los algoritmos. Además, es importante que los reguladores y las empresas trabajen juntos para garantizar que los algoritmos no se utilicen para discriminar a los consumidores. En resumen, los sesgos algorítmicos pueden contribuir a la discriminación de precios, lo que puede tener un impacto significativo en los consumidores, y es necesario abordar estos problemas para garantizar que los algoritmos sean justos y precisos.

---

[190] DANESI, Cecilia. El imperio de los algoritmos: IA inclusiva, ética y al servicio de la humanidad. Buenos Aires, Galerna, 2022. p.152

[191] ISLER, Erika. *Derecho del consumo. Nociones fundamentales*. Valencia, Tirant lo Blanch, 2021. 217p.

[192] Ley Nº 19.496. CHILE. *Establece Normas sobre Protección de los Derechos de los Consumidores.* Ministerio Secretaría General de la Presidencia, Santiago, Chile, 07 de febrero de 1997. Artículo 15.

[193] ISLER, Erika. *Derecho del consumo. Nociones fundamentales*. Valencia, Tirant lo Blanch, 2021. 217p.

[194] *Ibíd*., p. 217.

[195] *Ibíd*.

Un concepto clave en esta materia es lo que se conoce como "auditoría algorítmica", esto es, aquel proceso de evaluación sistemática de un algoritmo para identificar y corregir sesgos, errores y problemas éticos, cuyo objetivo es garantizar que el algoritmo sea justo y equitativo[196].

La auditoría constituye un mecanismo para comprobar que los algoritmos son diseñados, desarrollados y utilizados de acuerdo con la norma jurídica vigente para garantizar que los principios éticos y jurídicos se reflejan en los sistemas de IA que toman decisiones sobre todos nosotros y, gracias a ellas, se hace la IA más transparente, explicable y eficaz. Del mismo modo, se fomenta la responsabilidad social de las empresas en el desarrollo y uso de algoritmos[197].

Según ha señalado el Consejo para la Transparencia,

> *"El papel que juega la transparencia algorítmica es fundamental, pues abre la posibilidad de auditar y supervisar los datos que entran, cómo se procesan, y cómo se leen en un sistema de toma de decisiones algorítmicas mediante Inteligencia Artificial. De esta manera, es posible minimizar el riesgo de implementar procesos algorítmicos discriminatorios, condicionar arbitrariamente las decisiones de las personas y establecer responsabilidades cuando estos procesos entregan resultados no concluyentes, utilizan datos incorrectos o arrojan resultados injustos"*[198].

Una auditoría algorítmica implica una serie de pasos, cuyo objetivo es identificar, anticipar y corregir los riesgos que puedan surgir durante el ciclo de vida del algoritmo, lo cual, a su vez, favorece los mecanismos de responsabilidad, rendición de cuentas y de protección

---

[196] KASSIR, Sara. *Algorithmic Auditing: The Key to Making Machine Learning in the Public Interest*. [en línea] IBM Center for The Business of Government. Viewpoints. Winter 2019/2020. <https://www.businessofgovernment.org/sites/default/files/Algorithmic%20Auditing.pdf> [consulta: 10 septiembre 2023]

[197] MOTA, Eva y HERRERA, Esther. 2023. *Auditoría algorítmica en la inteligencia artificial en el sector público.* [en línea] Revista Digital Instituto de Investigaciones y Estudios Contables - FCE UNLP (17) <https://revistas.unlp.edu.ar/proyecciones/article/view/14782> [consulta: 09 septiembre 2023].

[198] CONSEJO PARA LA TRANSPARENCIA. Transparencia algorítmica. Buenas prácticas y estándares de transparencia en el proceso de toma de decisiones automatizadas [en línea] Santiago, Chile, <https://www.consejotransparencia.cl/wp-content/uploads/estudios/2020/10/Transparencia-Algoritmica.pdf> [consulta: 17 de agosto de 2023]. p.5.

de los derechos y libertades de las personas físicas involucradas y, especialmente, los derechos fundamentales a la privacidad y a la protección de los datos personales[199].

Es indispensable que el legislador prescriba la obligatoriedad de que los proveedores que emplean mecanismos de IA en la venta de sus productos o prestación de sus servicios se sometan a auditorías algorítmicas periódicas, ya que tales pueden ayudar a identificar y abordar los sesgos algorítmicos que pueden llevar a la discriminación y a otros problemas, así como también, a garantizar que los algoritmos sean precisos y justos y que se utilicen de manera ética, entre otras cosas[200].

Ahora bien, tal deber de auditabilidad podría entenderse, al menos en parte, como una conducta exigible en nuestro ordenamiento jurídico a la luz de la vigencia del principio de transparencia en el consumo. Se volverá sobre esto en la primera sección del tercer Capítulo, al momento de examinar las herramientas previstas en la Ley de Protección a los Consumidores para disminuir o eliminar los riesgos que implica el uso de IA para los consumidores.

Responsabilidad difusa

Responsabilidad Civil

En general, en el ámbito internacional existe consenso en orden a que no es necesario que la IA posea personalidad jurídica para poder perseguir la indemnización de los daños causados por esta tecnología, pues –en principio– es posible hacer responsable a alguna de las personas que crea, mantiene o controla el riesgo asociado al sistema de IA, aun cuando la tecnología haya actuado en forma autónoma[201].

[199] TORROBA, Alejandra. *El impacto social de los algoritmos.* Tesis (Grado en Sistemas de Información). Madrid, España. Universidad Politécnica de Madrid, 2023. p.27

[200] BELLOSO, Nuria. *La problemática de los sesgos algorítmicos (con especial referencia a los de género). ¿Hacia un derecho a la protección contra los sesgos?*. En: LLANO, F(Coord.), GARRIDO, J y VALDIVIA, R (Eds.). Inteligencia Artificial y Filosofía del Derecho. Murcia, 2022, Ediciones Laborum, pp. 45-69, p. 53.

[201] PARLAMENTO EUROPEO. 2020. Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012 (INL). [en línea] <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html> [consulta: 10 septiembre 2023], p. 4.

Así, si nos encontramos en una hipótesis en la que la IA fue desarrollada directamente por el proveedor, y éste suscribe un contrato con el consumidor en el que se disciplina –entre otras cosas– el uso de la tecnología, no debiese existir mayor óbice para perseguir la responsabilidad del proveedor en la medida en que se verifique un incumplimiento contractual y un daño[202].

Sin embargo, lo habitual es que el proveedor emplee sistemas de IA que fueron creados por un tercero experto, y que exista todo un eslabón de personas vinculadas al desarrollo, diseño e introducción de la tecnología[203]. Considerando que el consumidor no suscribe un contrato con cada una de ellas, será bastante más recurrente la aplicación del régimen genérico de responsabilidad extracontractual por culpa. En nuestro medio, esto produce tres grandes dificultades.

En primer lugar, es complejo que, dentro de todo el eslabón de personas vinculadas al sistema de IA utilizado, los consumidores identifiquen a aquella potencialmente responsable de los daños causados, ya que para ello deberían averiguar si el perjuicio halla su explicación en la fabricación, diseño, comercialización o control de la tecnología[204].

Por lo demás, si el perjuicio encuentra su explicación en un proceso en el que intervino un proveedor intermediario, nuestro ordenamiento no da luces respecto de la posibilidad de perseguir su responsabilidad civil cuando no existió un contrato directo de por medio, ya que el artículo 43 de la LPDC refiere únicamente a incumplimientos contractuales[205]. Tampoco resulta claro si es que el proveedor intermediario responde por los hechos dañosos que se hayan cometido en su plataforma de IA y sean atribuibles a terceros[206].

---

[202] Con mayor motivo si es que el contrato celebrado, como resulta habitual, es un contrato de adhesión, ya que en tal caso los artículos 16 letra e) y letra g) LPDC prohíben las exoneraciones de responsabilidad.

[203] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022, considerando 17.

[204] *Ibíd*., considerando 17.

[205] BRANTT, M.G.; y, MEJÍAS, C. *El proveedor intermediario de servicios y su responsabilidad. Un estudio del artículo 43 de la Ley 19.496.* [en línea] Revista de Derecho, Vol. 34, n° 2, pp.29-50, Diciembre 2021, <https://www.scielo.cl/scielo.php?pid=S0718-09502021000200029&script=sci_arttext&tlng=pt> [consulta: 14 agosto 2023]. p. 39

[206] ISLER, Erika. P*lataformas digitales y relación de consumo en Chile: un desafío actual*. En su: *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. 1ºed. Chile, Rubicón Editores, 2023. 196p.

En segundo lugar, aun si el consumidor lograse identificar a la persona presunta y legalmente responsable, es altamente probable que, atendido el carácter transfronterizo de las nuevas tecnologías, la persona en cuestión haya ejecutado sus labores –y, por tanto, haya cometido el hecho dañoso– en el extranjero. Ello supone que el consumidor deberá prever ante qué tribunal litigar y bajo qué derecho se resolverá el asunto, de modo que quizás no pueda aprovecharse de las disposiciones previstas en la LPDC.

En efecto, en nuestro país, a falta de norma legal que regule la situación, resulta aplicable el Código de Bustamante, cuyo artículo 168 consagra el principio *lex loci delicti*, indicando que, sin importar el tribunal ante el que se demande[207], deberá aplicarse la ley del lugar en donde se cometió el hecho dañoso –y no la del lugar en donde ocasione sus efectos–[208]. Por consiguiente, si un consumidor chileno pretende perseguir la responsabilidad por un daño causado por la IA, es posible que deba indagar y probar derecho extranjero, lo que lo dejaría en un estado de incertidumbre y lo desincentivaría a accionar[209].

En tercer lugar, resulta complejo para el consumidor tener que probar la culpa y el factor de causalidad en los daños que le han ocasionado, por cuanto para ello debería explicar la forma precisa en que la IA produjo una información o cometió un acto que le resultó dañoso[210]. Ahora bien, en nuestro ordenamiento, según ha afirmado cierta doctrina, la aplicación de los estándares de culpa infraccional y causalidad normativa a las relaciones de consumo se traduce en que, una vez que el consumidor demuestre la existencia de la infracción, se presuma legalmente la culpa del proveedor y la causalidad en los daños[211]. De ello se seguiría que el consumidor no se enfrenta con la dificultad de probar la culpa y la causalidad en estos casos –dejando a salvo, por cierto, la posibilidad de que el agente derrote las respectivas presunciones–.

---

[207] Actualmente se ha desarrollado el concepto de "foros de protección", en cuya virtud el consumidor podría demandar ante el tribunal que más le convenga. Pero la determinación del derecho que rige el asunto, al menos en principio, seguiría siendo un asunto regido por el artículo 168 del Código de Bustamante.

[208] Decreto 374. CHILE. Código de Derecho Internacional Privado. Ministerio de Relaciones Exteriores, Santiago, Chile, 25 de abril de 1934. Artículo 168.

[209] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022. p.2.

[210] *Ibíd*., considerado 25.

[211] FUENZALIDA, Eduardo. *El acto de consumo como hecho y la responsabilidad civil.* [en línea] Revista de derecho (Coquimbo), Jun. 2018, Vol. 25, n° 1, p. 121-152 <https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-97532018000100121> [consulta: 30 junio 2023].

Sin embargo, amén de que no exista ley que lo afirme, nuestra doctrina solo se encuentra conteste en cuanto al alcance de la culpa infraccional, pues se ha sostenido que la causalidad siempre debe probarse (por aplicación del artículo 1698 del Código Civil), tanto en su faceta natural como jurídica[212]. Vale decir, únicamente resulta pacífico el hecho de que la infracción a una ley o a otro deber de cuidado establecido por una autoridad con potestad normativa, permite presumir legalmente la culpa del agente –que es lo que se conoce como culpa infraccional–[213].

A falta de otra norma especial, podría pensarse también en la aplicación del artículo 2329 del Código Civil, que, de acuerdo al entendimiento dogmático mayoritario, contiene una presunción general de culpa por el hecho propio, aplicable tanto a las actividades peligrosas como a los hechos que por su naturaleza suelen provenir de culpa o dolo[214].

Considerando lo analizado hasta el momento, debiese resultar pacífica la idea de que el uso de IA constituye una actividad peligrosa, debido a la entidad de los daños a los que puede dar lugar. Pero lo cierto es que, incluso si se estimase aplicable el artículo 2329 del Código Civil, el efecto sería el mismo que el de la culpa infraccional: presumir legalmente la culpa del agente. Por tanto, todavía seguiría pendiente la prueba del vínculo causal[215].

Las dificultades que supone la aplicación del régimen general de responsabilidad a los daños derivados por el empleo de IA, han llevado a la Unión Europea a proponer una Directiva sobre Responsabilidad en materia de IA[216], que, según se explicará en el Capítulo IV, hace frente a todos los problemas identificados. Sin embargo, en nuestro país no existen reglas especiales para determinar la responsabilidad civil por los daños ocasionados por la IA, de modo que todas estas situaciones siguen resultando problemáticas para el consumidor chileno.

---

[212] CORRAL, Hernán. *La relación de causalidad en la responsabilidad por productos defectuosos.* Revista Chilena de Derecho Privado, (2):71-94, 2019. p.71. Esta es, por lo demás, la interpretación mayoritaria.

[213] BARROS, Enrique. *Tratado de responsabilidad extracontractual*. Santiago, Editorial Jurídica, 2010. 97-98 pp.

[214] Véase, por todos: *Ibíd*., 147-163 pp.

[215] Cabe destacar que esta dificultad seguiría presente aun en el evento de que el legislador nacional establezca un sistema de responsabilidad objetiva, por cuanto dicho régimen únicamente eliminaría la exigencia de que concurra la culpa o dolo.

[216] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022.

Responsabilidad Infraccional

En cuanto a la responsabilidad infraccional –esto es, aquella que no busca la indemnización de perjuicios, sino que se sancione al proveedor por haber cometido una infracción–, el problema estriba en que, si bien es claro que, en principio, el proveedor es responsable infraccionalmente por los daños que puedan surgir para los consumidores con motivo de las tecnologías incorporadas en los productos y servicios que comercializa, la literalidad del artículo 23 LPDC inciso 1°[217] da a entender que ello será así solo en la medida en que: (i) el respectivo bien o servicio presente fallas o deficiencias técnicas; y (ii) el proveedor actúe con negligencia.

Naturalmente, la aplicación de este precepto no será problemática cuando la incorporación de IA derive en que el bien o servicio no sea apto para el consumo[218]. Sin embargo, puede ocurrir que, pese a que el bien o servicio cumpla su fin y no cuente con fallas, el sistema de IA que se le ha incorporado, en razón de su carácter autónomo e imprevisible, funcione en forma distinta a la esperada y ocasione daños al consumidor[219]. Esa situación pareciera no quedar cubierta por el artículo 23 LPDC.

A mayor abundamiento, aun si se estimare que sí se encuentra cubierta -aduciendo, por ejemplo, que existió una programación deficiente-, sería extremadamente complejo para el consumidor probar las supuestas fallas técnicas y la negligencia del proveedor, atendida la especificidad de la cuestión[220].

No obstante, en nuestro país, a la luz de la jurisprudencia generada en torno al artículo 23 LPDC, lo cierto es que, incluso con la regulación actual, para el consumidor podría resultar factible perseguir la responsabilidad infraccional del proveedor en estas hipótesis. Al respecto, son dos las constataciones relevantes.

---

[217] El precepto indica que: "*Comete infracción a las disposiciones de la presente ley el proveedor que, en la venta de un bien o en la prestación de un servicio, actuando con negligencia, causa menoscabo al consumidor debido a fallas o deficiencias en la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida del respectivo bien o servicio*".

[218] ARAYA Paz, Carlos. *Desafíos legales de la inteligencia artificial en Chile*. Revista chilena de derecho y tecnología. 9 (2): 257-290, 2020. pp. 278-279.

[219] *Ibíd*., p. 279.

[220] *Ibíd.*, p. 279.

En primer lugar, los Tribunales Superiores de nuestro país han interpretado ampliamente el artículo 23 LPDC. En efecto, entienden que la responsabilidad del proveedor por infracción a la seguridad se verifica no solo cuando hay fallas técnicas en los productos o servicios que comercializa, sino también cuando se ha faltado al "deber de profesionalidad"[221].

Si bien el alcance del deber de profesionalidad se analizará en la siguiente Capítulo, es relevante anticipar que ello implica que el proveedor podría desentenderse de los actos autónomos e impredecibles de la IA solo en la medida en que haya evaluado, en forma previa, los riesgos de los sistemas implementados, así como sus estándares de precisión, fiabilidad y efectividad[222]; pues de lo contrario actuaría de mala fe y generaría desconfianza en el consumo.

En segundo lugar, nuestros Tribunales han sostenido que en el artículo 23 LPDC aplica el estándar de culpa infraccional, de suerte que, verificado un daño, es el proveedor quien debe acreditar que tomó las medidas tendientes a evitarlos, y no al revés[223].

El examen conjunto de estas interpretaciones lleva a concluir que, aun cuando en principio la situación parezca compleja, si el proveedor no tiene cuidado con las tecnologías que utiliza, no existe óbice para responsabilizarlo infraccionalmente por acciones autónomas e impredecibles ejecutadas por los sistemas de IA, incluso si los respectivos productos o servicios no tienen fallas técnicas. Y, si el proveedor estima que evalúo diligentemente los riesgos de la tecnología implementada, entonces podría eximirse de responsabilidad, mas él tendría que probarlo.

---

[221] A modo de ejemplo, véase: Corte de Apelaciones de Santiago, Rol 792-2013, 15-04-2014, c. 13; Corte de Apelaciones de Antofagasta, Rol 18-2017, 04-04-2017, c. 5; Corte de Apelaciones de Santiago, Rol Nº 1253-2015, 20-01-2016, c. 6. Asimismo, esta es la tesis sostenida por el SERNAC, según se aprecia en: SERVICIO Nacional del Consumidor. *Guía de Alcances Jurídicos, Ley 19.496* [en línea], p. 1, <https://www.sernac.cl/portal/618/articles-9193_archivo_01.pdf> [consulta: 08 julio 2023].

[222] SERVICIO NACIONAL DEL CONSUMIDOR (Chile). Resolución Exenta Nº 33, que Aprueba Circular Interpretativa sobre Protección de los Consumidores frente al uso de sistemas de Inteligencia Artificial en las relaciones de consumo. Santiago, Chile, 2022, p. 9.

[223] A modo de ejemplo, véase: CS, Rol 92134-2020, 03-07-2023, c. 3; Corte de Apelaciones de Santiago, Rol 707-2021, 07-06-2021, c. 4; Corte de Apelaciones de Talca, Rol 55-2020, 29-10-2020, c. 5. Esta última Sentencia señala, en términos muy claros, que "*en consideración a lo anterior, y a los principios que imperan en el estatuto de protección a los consumidores es que el proveedor tiene un estándar más alto en el deber de garantizar el derecho a la seguridad en el consumo del servicio prestado y dar un adecuado cumplimiento a los términos y condiciones pactados incluyendo el garantizar la calidad, cantidad, identidad, sustancia, procedencia, seguridad, peso o medida del respectivo bien o servicio, de forma que, cuando alguno de sus deberes se ve infringido en perjuicio de los derechos de los consumidores, es el proveedor quien debe probar su diligencia en la prestación del servicio*" (Énfasis agregado).

Con todo, aún persisten los problemas de la responsabilidad civil analizados anteriormente, que son más amplios y no pueden ser resueltos recurriendo a interpretaciones jurisprudenciales. Al efecto, una buena solución podría ser aquella propuesta por la Unión Europea en la Directiva de Responsabilidad en materia de IA, que consagra un régimen especial de responsabilidad que facilita el acceso a la prueba al consumidor y especifica los límites dentro de los cuales responde el proveedor[224]. Se volverá sobre esto en el cuarto Capítulo.

[224] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022.

CAPÍTULO III. ANÁLISIS DE LA NORMATIVA ACERCA DE LA PROTECCIÓN DE LOS CONSUMIDORES Y LA INTELIGENCIA ARTIFICIAL

En el Capítulo anterior, se examinó la incorporación de IA en las relaciones de consumo y su repercusión en la autonomía, privacidad e integridad de los consumidores, dando ideas generales sobre cómo podrían resolverse los desafíos. Ahora se analizará específicamente en qué medida la normativa chilena –actual y propuesta– permite responder a esos desafíos[225]. Para ello, se dividirá el Capítulo en cuatro secciones.

La primera tiene por objeto analizar las leyes vigentes en nuestro ordenamiento que, si bien no refieren a la IA en forma directa, resultan relevantes para configurar la protección de los consumidores ante el uso de dicha tecnología. En concreto, se aludirá a la LPDC y a la Ley Nº 19.628 sobre Protección a la Vida Privada (En adelante "**LPVP**").

Luego, en la segunda sección, se examinarán tres Circulares Interpretativas del SERNAC contingentes para la materia, que iluminan el sentido y alcance de ciertos derechos, obligaciones, principios y/o herramientas consagradas en las leyes anteriores, y, por consiguiente, contribuyen a delimitar ciertos deberes en el uso de la IA por parte de los proveedores.

En la tercera sección, se analizarán críticamente tres proyectos de ley que actualmente se encuentran en tramitación en nuestro país. Dentro de ellos destacan el "Proyecto de ley sobre IA y Robótica" (Boletín 15869-19) y el "Proyecto de Ley que regula el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales", por ser iniciativas que buscan regular la IA y el tratamiento de datos personales, respectivamente. Sin embargo, también se examinará sucintamente el Proyecto de ley "SERNAC te protege" (Boletín 16271-03), pues, si bien su principal propósito es fortalecer las facultades del SERNAC, contiene ciertas disposiciones que buscan hacer frente a los desafíos que supone la modernización de las relaciones de consumo.

[225] Se previene al lector que el Reglamento de Comercio Electrónico será analizado en el Cuarto Capítulo, al momento de proponer una regulación en nuestro ordenamiento. No se estima necesario examinarlo en este Capítulo, no solo por razones de extensión, sino también porque, como se dijo en la Introducción, este cuerpo normativo contribuye principalmente precisando ciertos deberes de información que no difieren sustancialmente de lo que se puede interpretar de la propia LPDC. En ese sentido, resulta más idóneo realizar un examen crítico del Reglamento, que se entiende mejor si, en forma previa, se han estudiado pormenorizadamente estándares extranjeros sobre la materia.

Por último, en la cuarta sección, se hará un balance general respecto del grado de protección que, en su conjunto, brindan al consumidor la normativa chilena vigente y la normativa chilena que aún se encuentra en tramitación. El objetivo de ello es, por una parte, determinar los riesgos que son mitigados adecuadamente, y, por otra, identificar los desafíos pendientes.

I. Herramientas consagradas en la Ley para resolver los desafíos planteados por el uso de la IA en las relaciones de consumo

1. Ley Nº 19.496, que establece normas sobre Protección de los Derechos de los Consumidores

Como primera aproximación, es menester tener presente que la LPDC no ha sido reformada para abordar concretamente el fenómeno de la IA. Su texto no menciona en ningún momento el concepto, ni existen artículos específicos que hayan sido agregados a propósito de los desafíos planteados por el uso de IA.

En seguida, cabe advertir que, en esta ocasión, el meollo del asunto no pasa por identificar qué derechos básicos y subjetivos de los consumidores consagrados en la LPDC cobran especial relevancia ante la incorporación de la IA en el consumo –cuestión examinada previamente–, sino en hallar mecanismos, principios o herramientas previstas en la LPDC que permitan superar o disminuir los riesgos respecto de tales derechos.

A pesar de que el texto legal no haya sido reformado, lo cierto es que estas herramientas sí existen. Y, aplicadas conjuntamente, pueden reducir significativamente los peligros para los consumidores. Se identifican concretamente cuatro de ellas: (i) el deber de informar de manera veraz y oportuna; (ii) el principio de transparencia; (iii) el deber de profesionalidad; y (iv) el control de cláusulas abusivas.

1) Deber de informar de manera veraz y oportuna

El artículo 3º letra b) de la LPDC consagra el derecho del consumidor a recibir una información veraz y oportuna sobre los bienes o servicios ofrecidos y sus características relevantes (lo que

supone, de otro lado, que el proveedor tiene el deber de proporcionársela)[226]. Lo importante de este precepto es que indica no solo que debe entregarse información, sino también cómo (en forma "veraz" y "oportuna") y sobre qué hacerlo (bienes o servicios ofrecidos y sus características relevantes).

Que la información sea entregada de manera "veraz", implica, desde luego, que no debe ser falsa. Sin embargo, la doctrina otorga al concepto un alcance mayor. No se trata solo de que la información sea cierta en un sentido literal, sino que, además, debe ser comprensible[227], completa, útil, accesible y eficiente[228], sin inducir a error ni engaño[229]. Por su parte, que la información sea entregada en forma "oportuna", significa que debe ponerse a disposición antes de la celebración del acto de consumo[230].

Asimismo, el precepto indica que el deber del proveedor de informar veraz y oportunamente aplica tanto respecto del bien o servicio mismo como respecto de sus características relevantes. Se entiende por "características "relevantes" aquellas que el consumidor valoraría razonablemente saber –ya sea por su connotación económica o por poner en peligro sus derechos– para formar un consentimiento adecuado[231].

Aplicando estos deberes a lo que ahora concierne, el presente trabajo plantea que, a la luz de lo analizado en el Capítulo anterior, el hecho de que un servicio o producto incorpore IA constituye una característica relevante. En efecto, la IA supone peligros para ciertos derechos consagrados en la LPDC, de modo que resulta valorable para los consumidores estar al tanto de la utilización de esta tecnología en forma previa a prestar su consentimiento. Esta idea no solo posee asidero teórico, sino también práctico. A modo de ejemplo, un reciente

[226] DFL 3. CHILE. Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021. Artículo 3 letra b).
[227] DE LA MAZA, Íñigo. *El suministro de información como técnica de protección de los consumidores: los deberes precontractuales de información*. Revista de derecho (Coquimbo). 17(2): 2010, p. 44.
[228] MARTORELL, Matías. Análisis crítico del deber del proveedor de informar en forma veraz y oportuna impuesto por el Artículo 3 Letra B) de la Ley de Protección al Consumidor. Tesis (Licenciatura en Ciencias Jurídicas y Sociales). Santiago, Chile. Universidad de Chile, Facultad de Derecho, 2015. 165p.
[229] HERNÁNDEZ Paulsen, Gabriel. *La obligación precontractual de la entidad de crédito de informar al cliente en los servicios bancarios y de inversión*. Madrid, Marcial Pons, 2014. 299p.
[230] MARTORELL, Matías. Análisis crítico del deber del proveedor de informar en forma veraz y oportuna impuesto por el Artículo 3 Letra B) de la Ley de Protección al Consumidor. Tesis (Licenciatura en Ciencias Jurídicas y Sociales). Santiago, Chile. Universidad de Chile, Facultad de Derecho, 2015. 165p.
[231] DE LA MAZA, Íñigo. *El suministro de información como técnica de protección de los consumidores: los deberes precontractuales de información*. Revista de derecho (Coquimbo). 17(2): 2010, p. 45.

estudio indicó que un 89% de los consumidores cree que es relevante saber si está interactuando con una IA o con un humano[232].

Pues bien, una vez que se ha catalogado a la incorporación de IA como una característica relevante, resulta aplicable el deber de información amplio previsto en el artículo 3º letra b) LPDC. Por consiguiente, todo proveedor que emplee IA debe informar al consumidor, previo a la celebración del acto de consumo, sobre dicha circunstancia, comunicando todo lo que sepa respecto del funcionamiento de la tecnología elegida y sus implicancias (por ejemplo: la finalidad del sistema y/o los datos personales que tratará[233]), en términos lo suficientemente claros, simples, comprensibles y útiles como para que el consumidor comprenda los beneficios y peligros del sistema incorporado.

Adicionalmente, en conformidad con lo previsto en el artículo 1 Nº3 de la LPDC, que refiere a la Información Básica Comercial, el proveedor está obligado a facilitar en forma clara, expedita y oportuna los instructivos de uso de los productos y servicios cuyo uso normal suponga un riesgo para la seguridad o integridad de las personas[234]. Considerando todo lo analizado en el Capítulo II, este deber rige plenamente respecto de los productos y servicios que están compuestos por IA, puesto que dicha tecnología posee el potencial de afectar la seguridad e integridad de los consumidores.

Así, a la luz de estos deberes, podría aminorarse el riesgo de que se genere una paradoja de la privacidad, exista un consentimiento viciado y/o se ocasionen daños a los consumidores. Con todo, esta herramienta posee una limitación importante. Según se colige de los artículos 1º Nº 3 y 3º letra b) de la LPDC, los deberes de información aplican únicamente cuando la IA sea un componente del bien o servicio, y no cuando se utilice esta tecnología para comercializarlos. Además, el hecho de proporcionar información, si bien ayuda a que disminuyan las asimetrías y a que el consumidor pueda evitar anticipadamente los riesgos, no garantiza, por sí solo, que el proveedor emplee la tecnología en forma adecuada.

---

[232] SALESFORCE. *Business Adopting AI Risk a 'Trust Gap' with Customers – Salesforce Repor*t. [en línea] <https://www.salesforce.com/news/stories/customer-engagement-research-2023/> [consulta: 30 agosto 2023].

[233] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 33, que Aprueba Circular Interpretativa sobre Protección de los Consumidores frente al uso de sistemas de Inteligencia Artificial en las relaciones de consumo. Santiago, Chile, 2022, p. 7.

[234] DFL 3. CHILE. Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021. Artículo 1 Nº3.

2) Principio de transparencia

Según señala el profesor Jorge Baraona, el principio de transparencia es un principio rector del derecho del consumo, en cuya virtud los proveedores deben generar condiciones propicias para que exista un consumo libre y confiado[235]. Se funda en los deberes de información, pero va más allá de eso[236]. No se trata solo de que los consumidores tengan a su disposición información completa, veraz, clara y comprensible, sino de que el proveedor observe un comportamiento leal en sus prácticas comerciales[237].

La vigencia de este principio se afirma en diversas disposiciones de la LPDC, tales como los artículos 1º Nº 2, 3º letra b), 12, 14, 17, 18 y 32, que consagran deberes de información y/o de adecuado comportamiento[238].

En lo que atañe a la incorporación de la IA en las relaciones de consumo, el principio de transparencia tiene dos usos relevantes. En primer lugar, actuar como un mecanismo de tutela de la privacidad y de los datos personales de los consumidores[239]; y, en segundo lugar, actuar como norma fundante de lo que se denomina "transparencia algorítmica".

La tutela a la privacidad y a los datos personales consiste en que, a la luz del principio de transparencia, para que se entienda otorgada la autorización expresa del titular en el tratamiento de sus datos personales a la que alude el artículo 4º de la Ley Nº 19.628, no basta con que simplemente se haya informado al consumidor el propósito de almacenamiento de sus datos, sino que dicha información debe comunicarse de un modo especial, esto es, "*con un acceso fácil, y redactada de manera clara e inteligible para un usuario medio*"[240].

---

[235] BARAONA, Jorge. *La regulación contenida en la Ley 19.496 sobre protección de los derechos de los consumidores y las reglas del Código Civil y Comercial sobre contratos: Un marco comparativo*. Revista chilena de derecho. 41(2): 2014, p. 386.

[236] BARRIENTOS Camus, Francisca. *Lecciones de derecho del consumidor.* Santiago, Thomson Reuters, 2019. 62p.

[237] BARAONA, Jorge. *La regulación contenida en la Ley 19.496 sobre protección de los derechos de los consumidores y las reglas del Código Civil y Comercial sobre contratos: Un marco comparativo*. Revista chilena de derecho. 41(2): 2014, p. 385.

[238] *Ibíd*., pp. 386-387.

[239] DE LA MAZA, Íñigo y MOMBERG, Rodrigo. *La transparencia como mecanismo de tutela de la privacidad de los consumidores y usuarios en contratos electrónicos*. Revista chilena de derecho y tecnología 7(2): pp. 81-111, 2018.

[240] *Ibíd.*, p. 98. Véase también: Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999. Artículo 4.

En consecuencia, todo proveedor que emplee sistemas de IA, ya sea en la fase de comercialización o en el producto o servicio mismo, debe comunicar al consumidor, en términos sencillos y precisos, la forma en que la IA trabajará con sus datos y cuál es la finalidad de dicho tratamiento. De lo contrario, el consumidor no podría dimensionar las reales implicancias de que la IA utilice sus datos y, por tanto, el consentimiento al que alude el artículo 4º de la Ley Nº 19.628 estaría viciado[241].

A mayor abundamiento, no existiría un consumo libre, confiado y seguro si no se tiene certeza respecto de lo que ocurre con los datos recolectados por la IA, ya que el consumidor no podría, por ejemplo, ejercer sus derechos frente a un eventual almacenamiento ilegal de datos ni, en general, hacer valer ninguna de las acciones que le reconoce la Ley Nº 19.628 frente a tratamientos equívocos[242].

Por su parte, la transparencia algorítmica alude a la apertura o visibilidad del proceso de toma de decisión de los algoritmos. Vale decir, en términos sencillos, que se muestre "*qué datos se utilizan, cómo se utilizan, quiénes los utilizan, para qué los utilizan y cómo se llega a partir de los datos a tomar las decisiones que afectan a la esfera vital de quien reclama esta transparencia* [en este caso, los consumidores]"[243].

Si bien en Chile no existe un "derecho a la transparencia algorítmica" como tal[244], dentro del ámbito de consumo puede fundarse su vigencia en el principio de transparencia. En efecto, más allá del alcance de nombre, un análisis simple permite constatar que, para que el principio de transparencia se cumpla a cabalidad, debe existir transparencia algorítmica. Ello, por cuanto este principio obliga a los proveedores a garantizar un consumo seguro y confiado, lo que solo es posible si los consumidores están conscientes del funcionamiento y de los riesgos de la tecnología con la que interactúan[245].

---

[241] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 174 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores. Santiago, Chile, 28 de febrero de 2022. 14p.

[242] *Ibíd*., p. 15

[243] SANGÜESA, Ramón. *Inteligencia artificial y transparencia algorítmica: It's complicated.* BiD: textos universitaris de biblioteconomia i documentació. 41: 2018, p.2. Corchetes agregados.

[244] AZUAJE, Michelle y FINOL, Daniel. *Transparencia algorítmica y la propiedad intelectual e industrial: tensiones y soluciones*. La Propiedad Inmaterial (30): p. 137, 2020.

[245] RADER, Emilee, COTTER, Kelley, CHO, Janghee. *Explanations as mechanisms for supporting algorithmic transparency*. Proceedings of the 2018 CHI conference on human factors in computing systems (103): p. 3, abr. 2018.

Una vez que la transparencia algorítmica constituye un comportamiento exigible, disminuye significativamente la probabilidad de que se efectúen discriminaciones arbitrarias y/o se ejerzan influencias indebidas sobre la autonomía del consumidor[246]. Ahora bien, aun cuando discutir la efectividad de la transparencia algorítmica como mecanismo de tutela a los consumidores excede el alcance de este trabajo, no puede obviarse que la opacidad de la IA dificulta que el proveedor pueda transparentar completamente el funcionamiento de los algoritmos, incluso si así lo deseare[247].

Adicionalmente, una vez que el proveedor sabe que tendrá que informar sobre el funcionamiento de los algoritmos, posee grandes incentivos en orden a, en primer lugar, optar por tecnologías de IAs más simples y menos funcionales –con tal de poder explicarlas fácilmente–[248], y, en segundo lugar, seleccionar cuidadosamente los aspectos que desea transparentar y transmitir información incompleta[249]. Estos últimos dos problemas pueden ser solucionados, en cierta medida, mediante el "deber de profesionalidad".

3) Deber de profesionalidad

El deber de profesionalidad corresponde "*[a]l nivel de competencia y cuidado especial que se puede exigir razonablemente, de acuerdo con la buena fe, a un proveedor en sus relaciones con los consumidores en el ámbito de su actividad o negocio, en razón de la experticia y habitualidad con las que desempeña su giro*"[250]. Se trata, en definitiva, de que el proveedor observe un comportamiento competente, serio, ético y ajustado a su *lex artis*[251].

---

[246] SANDVIG, Christian, et al. *Data and discrimination: Converting critical concerns into productive inquiry.* En Data and Discrimination: Converting Critical Concerns into Productive Inquiry at the Annual Meeting of the International Communication Association. 2014.

[247] ARAYA Paz, Carlos. 2021. *Transparencia algorítmica ¿un problema normativo o tecnológico?* [en línea] CUHSO (Temuco). 31(2): 306-334. <https://www.scielo.cl/scielo.php?pid=S2452-610X2021005000002&script=sci_abstract&tlng=en> [consulta: 19 de octubre de 2023]. p. 19.

[248] *Ibíd.,* p. 26.

[249] CHROMIK et al, op. cit., p. 1.

[250] GATICA, María Paz y MORALES, María Elisa. *El deber de profesionalidad como elemento determinante del estándar de diligencia en el derecho del consumo: un comentario a la sentencia de la Corte de Apelaciones de San Miguel de 15 de marzo de 2019 (Rol Nº 484-2018)*. Revista de derecho (Coquimbo) 29: p. 11, 2022.

[251] ZÚÑIGA Denegri, Martín. *Principio de préstamo responsable. Naturaleza y fuentes legales en el ordenamiento jurídico chileno.* Revista de Derecho Económico. 79(2): 2022, p. 122.

El comentado deber se construye a partir de varios preceptos de la LPDC, tales como los artículos 1º Nº2 (referido a la habitualidad en el desempeño del giro), 23 (referido a la diligencia) y 24 (referido a la profesionalidad propiamente tal)[252]. Si bien no existe material normativo, doctrinario ni jurisprudencial que analice en detalle el rol del deber de profesionalidad en relación con el uso de IA, los autores de esta Memoria sostienen que el hecho de que los proveedores que emplean sistemas de IA deban cumplir con el deber de profesionalidad, permite arribar a dos conclusiones relevantes.

En primer lugar, queda proscrito el ejercicio de influencias indebidas sobre la autonomía del consumidor, el tratamiento inadecuado de datos personales[253] y las discriminaciones arbitrarias intencionales, ya que no sería un comportamiento competente y profesional aprovecharse de las tecnologías en forma poco ética. Así, en virtud de la profesionalidad, se construye un deber de buen comportamiento general que resulta especialmente atingente en el empleo de sistemas de IA. En otras palabras, queda vedado el "mal uso" intencional de la IA.

En tal sentido, el deber de profesionalidad lograría, al menos, disminuir altamente la probabilidad de ocurrencia de aquellos riesgos que tienen su explicación exclusivamente en el mal comportamiento o descuido del proveedor. El SERNAC ha avalado esta interpretación a propósito del tratamiento de datos personales, señalando que el deber de profesionalidad:

> *"*[C]*onlleva la necesidad de aplicar medidas de seguridad integrales, esto es, técnicas, organizativas y de formación de capital humano que permitan resguardar la confidencialidad, integridad y disponibilidad de los datos personales de consumidores contenidos en sus registros o bases de datos, con la finalidad de evitar la alteración, pérdida, transmisión y acceso no autorizado de los mismos"*[254].

[252] GATICA y MORALES, op. cit., pp. 3-5.

[253] Sobre este punto, véase: SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 174 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores. Santiago, Chile, 28 de febrero de 2022. 21-22 pp.

[254] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 174 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores. Santiago, Chile, 28 de febrero de 2022. 21p.

Sin embargo, dicha lógica también puede ser extendida al cuidado de la autonomía y la integridad de los consumidores, pues lo propio del deber de profesionalidad es que exista un nivel de comportamiento y diligencia acorde al desarrollo de la actividad. Esta idea es la que se esboza, por ejemplo, en la regulación de la Unión Europea, cuando se alude a que el profesional debe esforzarse en observar los principios éticos del uso de la IA en todo momento (ej: respeto de la autonomía humana, prevención del daño, equidad, etc.)[255].

En segundo lugar, existe una buena razón para indicar que, de materializarse los dos incentivos problemáticos que se identificaron al momento de examinar el principio de transparencia, se estaría ante un actuar ilegal. No obstante que dichos incentivos existan, es evidente que ambos comportamientos son abiertamente contrarios a la buena fe y al estándar esperable de un profesional, ya que dan cuenta de un actuar egoísta, elusorio y poco comprometido con la modernización del comercio. Por consiguiente, supondrían una infracción al deber de profesionalidad.

Considerando que la buena fe es uno de los principales fundamentos del deber de profesionalidad[256], no resulta admisible que el proveedor, a sabiendas de que ciertos sistemas de IA son poco funcionales, los utilice para facilitar el cumplimiento normativo y perjudicar a los consumidores. Tampoco puede comunicar menos información que aquella que le es exigible.

Ahora bien, es menester prevenir que el problema de utilizar sistemas poco funcionales solo puede ser resuelto “en cierta medida” por el deber de profesionalidad, puesto que es posible que el proveedor simplemente no esté en condiciones de explicar sistemas de IA más complejos. Y, de ser así, no bastaría con recurrir a un deber general de buen comportamiento para obligarlo a emplear tecnologías que, si bien ayudan a los consumidores, no será capaz de explicar y, por tanto, acarrearán incumplimientos y sanciones administrativas no deseadas para el proveedor.

Además, a falta de norma que lo regule, es complejo dilucidar cuál es el nivel de transparencia propio de un proveedor profesional. Aun cuando pueda fundarse la vigencia de

[255] EUROPEAN COMMISSION, 2019. *Ethics guidelines for trustworthy AI* [en línea], p. 14, <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai,> [consulta: 10 septiembre 2023].
[256] GATICA y MORALES, op. cit., p.11.

la transparencia algorítmica en el derecho de consumo chileno, su balance sigue resultando incierto. Por un lado, la falta de transparencia perjudica a los consumidores; pero, por otro, la transparencia absoluta podría resultar contraproducente, tanto para los proveedores –por el gasto de tiempo y el riesgo de divulgar información comercialmente sensible– como para los consumidores –que quizás no necesitan toda esa información o tenerla en exceso los confunda aún más–[257].

Por último, en cuanto a las manifestaciones del deber de profesionalidad que van más allá de la transparencia, el problema es que, si bien resulta sencillo identificar las abstenciones o conductas negativas que debe observar el proveedor (por ejemplo, no influir maliciosamente en la autonomía, no descuidar datos personales, no discriminar intencional y arbitrariamente, etc.), no pasa lo mismo cuando pensamos en conductas positivas. La única directriz pareciera ser que deben ir motivadas por una buena intención y por el debido resguardo de los derechos de los consumidores. Pero ¿hasta dónde llegamos? Existe la posibilidad de que pasemos el límite y las conductas ya no sean profesionales, sino desproporcionadas o incluso imposibles de cumplir.

4) Control de cláusulas abusivas

En el contexto del comercio electrónico y la utilización o venta de sistemas tecnológicos –como la IA–, es frecuente que los documentos que disciplinan el uso de datos personales y/o la responsabilidad del proveedor por daños asuman la forma de un contrato de adhesión[258]. Según prevé el artículo 1º Nº 6 de la LPDC, un contrato de adhesión es "*aquel cuyas cláusulas han sido propuestas unilateralmente por el proveedor sin que el consumidor, para celebrarlo, pueda alterar su contenido*"[259]. Vale decir, se trata de un contrato que el consumidor puede aceptar o rechazar, mas no negociar.

[257] COMISIÓN EUROPEA. Comunicación "Directrices sobre la transparencia de la clasificación con arreglo al Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo". p. 5. Considerando 25.
[258] DE LA MAZA, Íñigo. y MOMBERG, Rodrigo., 2017. *Términos y condiciones: Acerca del supuesto carácter contractual de las autorizaciones para el tratamiento de datos personales en sitios web*. Revista chilena de derecho y tecnología 6(2): p. 40, 2017.
[259] DFL 3. CHILE. *Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores.* Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021. Artículo 1 Nº6.

El hecho de que estos contratos sean redactados únicamente por la parte que se presenta como más fuerte dentro de la relación, genera un alto riesgo de que existan cláusulas abusivas[260]. En general, se entiende por cláusula abusiva aquella que es notablemente desfavorable para el adherente[261], por ocasionar un desequilibrio significativo en las prestaciones[262] y/o ser contraria al principio de buena fe[263].

A fin de evitar que los contratos de adhesión incorporen cláusulas abusivas, nuestro ordenamiento jurídico permite que pueda controlarse el contenido de estos contratos, tanto desde una perspectiva material (artículo 16 LPDC) como desde una perspectiva formal (artículo 17 LPDC). Este control puede, a su vez, ser preventivo -antes de que se forme el contrato- o represivo -una vez que el contrato ya ha comenzado a regir una relación de consumo-[264].

De este modo, se restringe el campo de aplicación de los principios civiles clásicos de libertad contractual y *pacta sunt servanda*, abriendo cauce a la posibilidad de que exista una intervención judicial respecto del contenido del contrato y se declare la nulidad de aquellas cláusulas que resultan abusivas[265].

En concreto, en lo que atañe a los contratos de adhesión que los proveedores emplean para regular los términos y condiciones de uso de los sistemas de IA -por ejemplo, en plataformas de comercio electrónico o en la venta de productos que incorporan IA-, el control material podría tener, al menos, tres usos relevantes.

Dichos usos son: (i) evitar la inclusión o aplicación de cláusulas que pretendan exonerar de responsabilidad al proveedor por actos cometidos por la IA; (ii) evitar la inclusión o aplicación de cláusulas abusivas en relación al uso y tratamiento de datos personales que

---

[260] DE LA MAZA, Íñigo. C*ontratos por adhesión y cláusulas abusivas: ¿Por qué el Estado y no solamente el mercado?* Revista chilena de derecho privado. (1): 2003, p. 119.
[261] *Ibíd.*, p. 119.
[262] MOMBERG, Rodrigo. *El control de las cláusulas abusivas como instrumento de intervención judicial en el contrato*. Revista de derecho (Valdivia). 26(1): 2013, p. 18.
[263] ECHEVERRI, Verónica. *El control a las cláusulas abusivas en los contratos de adhesión con consumidores*. Opinión jurídica, 10(20): 2011, pp. 130-132.
[264] PIZARRO, Carlos. *La eficacia del control de las cláusulas abusivas en el derecho chileno*. Estudios Socio-Jurídicos. 6(2): 2004, p. 133.
[265] MOMBERG, Rodrigo. *El control de las cláusulas abusivas como instrumento de intervención judicial en el contrato*. Revista de derecho (Valdivia). 26(1): 2013, p. 12.

efectuará la IA[266]; y (iii) evitar, en general, la inclusión o aplicación de cualquier otra cláusula que, en el contexto del uso de IA, pueda considerarse como contraria a las exigencias de la buena fe objetiva u ocasione un desequilibrio contractual significativo en perjuicio del consumidor[267].

En primer lugar, respecto de las cláusulas de exoneración de responsabilidad, cabe constatar que, en principio, los proveedores que utilizan IA podrían verse tentados a incluirlas, toda vez que así se desentienden de cualquier daño que pueda ocasionar la tecnología empleada[268]. Empero, en nuestro ordenamiento, la incorporación de estas cláusulas en contratos de adhesión carece de validez. En efecto, el artículo 16 letra e) de la LPDC indica que no tendrán eficacia alguna las cláusulas que "[c]*ontengan limitaciones absolutas de responsabilidad frente al consumidor que puedan privar a éste de su derecho a resarcimiento frente a deficiencias que afecten la utilidad o finalidad esencial del producto o servicio*"[269]. Por tanto, a través del control material se eliminaría cualquier cláusula de este estilo.

El precepto alude a la invalidez de "limitaciones absolutas de responsabilidad". Sin embargo, siguiendo el criterio desarrollado por el SERNAC, y teniendo en cuenta la existencia del principio pro consumidor previsto en el artículo 2 ter LPDC, también podrían estimarse invalidas aquellas cláusulas que, no obstante establecer limitaciones parciales de responsabilidad, en los hechos, dificulten el ejercicio de acciones de indemnización de perjuicios por parte del consumidor que interactúa con la IA[270].

---

[266] MOMBERG URIBE, Rodrigo; MORALES ORTIZ, Maria Elisa. 2019. *Las cláusulas relativas al uso y tratamiento de datos personales y el artículo 16 letra g) de la Ley 19.496 sobre Protección de los Derechos de los Consumidores.* Revista chilena de derecho y tecnología 8(2): 157-180. Véase también: SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 174 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores. Santiago, Chile, 28 de febrero de 2022.

[267] Si bien este tema no ha sido desarrollado a propósito de la IA, puede llegarse a dicha conclusión interpretando el artículo 16 letra g) de la LPDC.

[268] PARLAMENTO EUROPEO. 2020. *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012 (INL)*. [en línea] <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html> [consulta: 10 septiembre 2023].

[269]DFL 3. CHILE. *Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores.* Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021. Artículo 16 letra e).

[270] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 000174, que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores. Santiago, Chile, 2022; y SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 931 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión de consumo. Santiago, Chile, 03 de diciembre de 2021. Según sostienen dichos documentos, podría arribarse a tales conclusiones a partir de una interpretación amplia del artículo 16 letra e) LPDC, teniendo en cuenta que, en el contexto de los contratos de adhesión, cobra especial importancia

En segundo lugar, en cuanto a las cláusulas abusivas sobre uso y tratamiento de datos personales, es relevante tener a la vista el artículo 16 letra g) de la LPDC. Este precepto establece que no producirán efecto alguno en los contratos de adhesión las cláusulas que: "*En contra de las exigencias de la buena fe, atendiendo para estos efectos a parámetros objetivos, causen en perjuicio del consumidor, un desequilibrio importante en los derechos y obligaciones que para las partes se deriven del contrato. Para ello se atenderá a la finalidad del contrato y a las disposiciones especiales o generales que lo rigen*"[271].

Pues bien, en base a dicha norma, la jurisprudencia y la doctrina nacional han entendido como un ejemplo de cláusulas abusivas son aquellas que buscan obtener el consentimiento del titular de los datos personales mediante una condición general de contratación que se incluye en un contrato cuyo objeto principal no es el tratamiento de datos[272]. En otras palabras, carecen de efecto las cláusulas cuya intención sea adquirir un consentimiento atado, oculto o poco transparente respecto del uso de datos personales.

Fundándose en el mismo precepto, también devienen en abusivas aquellas cláusulas que contravienen disposiciones de la Ley N° 19.628, o que, sin ser ilegales, presumiblemente el consumidor no las habría aceptado en un contrato negociado de manera libre, ni tampoco hubiese esperado -razonablemente- que se incluyeran teniendo en cuenta el objeto principal del contrato que suscribió[273].

Cabe advertir que, en último término, el si se admite o no que todas las situaciones mencionadas den lugar a cláusulas abusivas depende de qué tan amplia sea la interpretación que se da al artículo 16 letra g). Como señalan Momberg y Morales, ciertos operadores jurídicos entienden que, para que una cláusula infrinja este precepto, debe ser contraria a la buena fe objetiva[274] y, además, causar un desequilibrio contractual significativo en perjuicio del

---

la aplicación del principio pro consumidor. Con todo, aun si se estimare que dicha interpretación no es factible, las cláusulas igualmente podrían considerarse abusivas si es que atentan contra la buena fe y generan desequilibrios importantes, en base a lo dispuesto en el artículo 16 letra g).

[271] MINISTERIO DE ECONOMÍA, FOMENTO Y TURISMO (Chile), op. cit. Artículo 16 letra g).

[272] CS, Rol 1533-2015, 07-07-2016, c. 11.

[273] MOMBERG URIBE, Rodrigo; MORALES ORTIZ, Maria Elisa. 2019. Las cláusulas relativas al uso y tratamiento de datos personales y el artículo 16 letra g) de la Ley 19.496 sobre Protección de los Derechos de los Consumidores. Revista chilena de derecho y tecnología 8(2): 157-180. pp. 174-177.

[274] Como se explicará, la para que una conducta sea contraria a buena fe objetiva, no es necesario que exista mala fe o dolo en el actuar, sino que basta con que se trate de una conducta desviada en relación a aquello que le era

consumidor; mientras que otros sostienen que basta con que se satisfaga únicamente uno de esos dos requisitos, en la medida en que pueda arribarse a tal conclusión teniendo a la vista la finalidad del contrato y las disposiciones que le rigen[275].

La presente Memoria adscribe a la segunda tesis, por cuanto, si una de las partes redactó la totalidad del contrato a sabiendas de que su contraparte no tendrá opción de modificarlo, la sola inclusión de una cláusula que ocasione desequilibrios significativos puede concebirse como un acto contrario a la buena fe objetiva[276]. Y, viceversa, la incorporación de cláusulas que atentan en contra de la buena fe objetiva supone, casi siempre, la generación de un desequilibrio significativo. Por tanto, bastaría con probar la existencia de una de dichas circunstancias.

A mayor abundamiento, esta interpretación es más coherente con los principios que inspiran la normativa de protección al consumidor. Al no exigir que siempre se pruebe una infracción a la buena fe, se evita que el carácter abstracto de este concepto dé lugar a interpretaciones diversas que afecten la certeza jurídica en perjuicio de los consumidores[277].

Así pues, todas las situaciones ejemplificadas podrían dar lugar a cláusulas abusivas susceptibles de anulación en base al artículo 16 letra g), ya que atentan en contra de la buena fe o generan desequilibrios significativos. Ello resulta especialmente relevante en el contexto de la IA, atendido que el control contractual constituye un buen mecanismo para evitar que se incluyan cláusulas que habiliten a la IA a tratar datos en forma ilegal, poco ética o sin haber dado un aviso transparente al consumidor.

Con todo, la abusividad de las cláusulas relativas al uso y tratamiento de datos personales puede ir más allá. En efecto, existen otras hipótesis contenidas en el artículo 16 de la LPDC que resultan pertinentes a propósito de ciertas prácticas que pueden desarrollar los proveedores que trabajan con IA.

---

exigible a un sujeto medio. Véase: DÍEZ-PICAZO, Luis. *Fundamentos del Derecho Civil Patrimonial*. 6ª Ed, Madrid, Editorial Civitas, 2007. 61p.

[275] MOMBERG, Rodrigo. y MORALES, María Elisa. Op. Cit. pp. 165-166, 2019.

[276] *Ibíd.*, pp. 165-166.

[277] MOMBERG, Rodrigo. *El control de las cláusulas abusivas como instrumento de intervención judicial en el contrato*. Revista de derecho (Valdivia). 26(1): 2013, p. 18.

El artículo 16 letra a) de la LPDC prescribe que no producirán efecto alguno las cláusulas que "*Otorguen a una de las partes la facultad de dejar sin efecto o modificar a su solo arbitrio el contrato o de suspender unilateralmente su ejecución (...)*"[278]. En virtud de este precepto, no resulta factible, por ejemplo, la inclusión o aplicación de cláusulas que permitan al proveedor responsable de los datos recogidos por la IA, "*modificar unilateralmente o de manera amplia los términos y condiciones bajo los cuales el consumidor autorizó originalmente la recopilación y procesamiento de su información personal*"[279].

Por su parte, el artículo 16 letra c) de la LPDC refiere a la nulidad de las cláusulas que "*Pongan de cargo del consumidor los efectos de deficiencias, omisiones o errores administrativos, cuando ellos no le sean imputables*"[280]. En tal sentido, no resulta factible, por ejemplo, la inclusión o aplicación de una cláusula que indique que el proveedor no garantizará la seguridad de los datos que utilice la IA, ni será responsable de su robo, destrucción o divulgación[281].

Por último, en cuanto a las cláusulas que, a pesar de no versar sobre datos personales, puedan considerarse, en el contexto del uso de IA, como contrarias a las exigencias de la buena fe objetiva u ocasionen un desequilibrio contractual significativo en perjuicio del consumidor, resulta pertinente señalar que estas carecerán de efecto alguno en base a lo dispuesto en el artículo 16 letra g) LPDC.

Como advierte De la Maza, el hecho de que las cláusulas deban observar los parámetros de la buena fe objetiva para ser válidas no solo supone el cumplimiento de los deberes de transparencia y de los aspectos formales de legibilidad del contrato de adhesión, sino también la satisfacción de las "*exigencias que imponen las convicciones éticas imperantes al tráfico comercial*"[282].

---

[278] DFL 3. CHILE. Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021. Artículo 16 letra a).

[279] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 174 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores. Santiago, Chile, 28 de febrero de 2022. 17p.

[280] MINISTERIO de Economía, Fomento y Turismo (Chile), op. cit. Artículo 16 letra c).

[281] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 174 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores. Santiago, Chile, 28 de febrero de 2022. 20-21 pp.

[282] DE LA MAZA, Íñigo. *El control de las cláusulas abusivas y la letra g.* Revista chilena de derecho privado. (3): 2004, p.55.

Si se sigue la tesis de que, en virtud de lo dispuesto en el artículo 16 letra g) de la LPDC, toda cláusula contenida en un contrato de adhesión que infringe la buena fe objetiva –teniendo a la vista el propósito del contrato y las disposiciones que le rigen– deviene en abusiva, entonces debe concluirse que los proveedores no pueden incorporar en sus contratos de adhesión cláusulas que atenten en contra de los principios éticos que inspiran la utilización de IA. La razón de ello estriba en que la vulneración de las convicciones éticas que rigen el ejercicio de la actividad implica, a su vez, una inobservancia de los parámetros de buena fe objetiva.

En efecto, la buena fe objetiva, por definición, corresponde a la "*conducta social que la conciencia social exige en cada caso conforme a un imperativo ético dado*"[283]. De esto se sigue que, en la especie, el respeto de los imperativos éticos del uso de IA se erige como un deber de conducta exigible a la luz de los parámetros de la buena fe objetiva.

Lo relevante del razonamiento expuesto es que, a partir de ello, podría plantearse que los diversos principios éticos que se han desarrollado a propósito del uso de IA en otros países –respeto de la autonomía humana, equidad, transparencia, proporcionalidad, justicia, privacidad, etc.– no pueden ser contrariados en los contratos de adhesión que se celebren en nuestro país, so pena de que la cláusula en cuestión se declare nula. De este modo, se da lugar a un deber de comportamiento ético que rige plenamente en el marco de la celebración de contratos de adhesión, aun cuando ninguno de los principios en cuestión se encuentre positivado en nuestro ordenamiento.

2. Ley Nº 19.628, sobre Protección de la Vida Privada ("LPVP")

Si bien, al igual que la LPDC, la LPVP no ha sido reformada para abordar concretamente el fenómeno de la IA, este cuerpo normativo cuenta con herramientas que pueden ayudar a resolver algunos de los desafíos planteados por el uso de la IA en las relaciones de consumo, tales como:

[283] DÍEZ-PICAZO, Luis. *Fundamentos del Derecho Civil Patrimonial*. 6ª Ed, Madrid, Editorial Civitas, 2007. 61p.

1) Principio de consentimiento informado

Conforme a este principio, consagrado en el artículo 4º de la LPVP, el tratamiento de datos personales sólo puede realizarse con el consentimiento informado del titular de los datos, salvo que exista una base legal que estipule expresamente lo contrario. Lo anterior, con el propósito de proteger la finalidad para el cual fueron recogidos los datos personales, haciéndolo extensivo a su tratamiento[284]. Así las cosas, los primeros cuatro incisos de la norma disponen:

> *"El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen* ***o el titular consienta expresamente en ello****.*
>
> *La persona que autoriza debe ser* ***debidamente informada*** *respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público.*
>
> *La autorización debe* ***constar por escrito.***
>
> *La autorización puede ser revocada, aunque sin efecto retroactivo, lo que también deberá hacerse por escrito."*[285] (énfasis agregado).

De esta manera, la disposición explicita la intención del legislador de proteger y regular de forma estricta de lo datos personales, otorgando así un derecho de vital importancia: el **derecho a la autodeterminación informativa**, definida como el *"control que ofrece a las personas sobre el uso por terceros de información sobre ellas mismas"*[286], la cual fue desarrollada *supra* a propósito de la autonomía del consumidor.

Sin perjuicio de lo anterior, la disposición consagra en sus incisos 5 y 6, de manera no taxativa, una serie de excepciones amplísimas en que no se requiere del consentimiento expreso del titular para tratar sus datos personales, entre las que se encuentran:

---

[284] CÁMARA DE DIPUTADOS (CHILE). *Evaluación de la Ley N° 19.628. Protección de la Vida Privada,* agosto 2016, p.31.

[285] Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999. Artículo 4.

[286] MURILLO DE LA CUEVA, Pablo. *La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad.* En su: *La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*. España, Fundación Coloquio Jurídico Europeo, 2009. p.11.

1. Cuando los datos personales provengan o se recolecten de fuentes accesibles al público, cuando:
    a. Sean de carácter económico, financiero, bancario o comercial;
    b. Se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento; y,
    c. Sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios[287].
2. Cuando el tratamiento de datos personales sea realizado por personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos[288].

Al respecto, es importante mencionar que resulta altamente cuestionable que puedan tratarse libremente antecedentes personales económicos, comerciales, patrimoniales y financieros positivos, ya que aquellos son, de hecho, los datos más relevantes para las empresas de marketing directo, ya que la naturaleza o el contenido de la información que administran o su cartera de clientes es su principal activo[289] y, además, que tales excepciones se contradicen con el inciso final del artículo 3° de la LPVP, según el cual "*[E]l titular puede oponerse a la utilización de sus datos personales con fines de* ***publicidad****, investigación de mercado o encuestas de opinión*"[290], por lo cual habría que determinar cuál de las dos normas habría de regir en caso de conflicto.

Pasando ya a los datos personales de carácter sensible, esto es, aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, el artículo 10 dispone que tales datos, por regla general, no pueden ser objeto de tratamiento[291]. Sin embargo, inmediatamente después

[287] Ley N° 19.628, CHILE, op. cit. Artículo 4.
[288] *Ibíd*.
[289] BERTELSEN REPETTO, Raúl. *Datos personales: propiedad privada, libre iniciativa particular y respeto a la vida privada*. En: "Tratamiento de datos personales y protección de la vida privada", BERTELSEN et al., 3ª edición, Cuadernos de extensión Jurídica, Ediciones Universidad de Los Andes, 2001. p.103.
[290] Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999. Artículo 3.
[291] *Ibíd*. Artículo 10.

consagra tres excepciones, nuevamente, de magna amplitud. Así las cosas, pueden tratarse datos sensibles cuando:

1. La ley lo autorice;
2. Exista consentimiento del titular; y,
3. Cuando sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares[292].

En cuanto a la tercera excepción, se trata de un caso especialísimo en el que la ley autoriza incluso el tratamiento de datos sensibles, que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad[293]. Esta excepción ha sido fuertemente criticada, en tanto, según se desprende de la historia de la ley, se incorporó a petición de las compañías de seguros, Isapres y Fonasa, quienes sostuvieron que era esencial el tratamiento de datos sensibles para su funcionamiento.

Adicionalmente, es necesario hacer énfasis en dos cosas. La primera, en torno al tratamiento de datos por consentimiento expreso del titular, es que tal consentimiento debe ser informado. La información que debe proporcionarse al titular de los datos debe cubrir tanto la finalidad dentro de la cual se enmarcará el tratamiento de datos como su posible comunicación al público, lo que dice relación con el grado de divulgación de sus datos personales que el titular está dispuesto a tolerar[294].

La segunda cuestión a tener en consideración es que, sea que los datos personales y sensibles sean tratados por consentimiento del titular o por autorización de la ley, aquel tratamiento siempre debe realizarse de acuerdo a la finalidad para la cual hayan sido recolectados los datos, tal como se verá en el siguiente apartado.

Para finalizar, resulta muy importante que el legislador consagre en forma expresa la posibilidad de que los titulares de datos personales puedan revocar la autorización del

---

[292] *Ibíd.*

[293] VIAL CLARO, Felipe. *La ley Nº 19.628 sobre protección de datos de carácter personal. Una visión general.* En: "Tratamiento de datos personales y protección de la vida privada", BERTELSEN et al., 3ª edición, Cuadernos de extensión Jurídica, Ediciones Universidad de Los Andes, 2001, p.28.

[294] *Ibíd*., p.27.

tratamiento –aunque por escrito y sin efecto retroactivo–[295]. Así, se concede cierto control a los titulares sobre sus datos personales en caso de que no estén satisfechos con la manera en que aquellos estén siendo tratados o, derechamente, ya no desean que sean tratados y/o comunicados a terceros, pese a haber consentido en ello inicialmente.

Ahora bien, el hecho de que tal autorización no tenga el carácter retroactivo dificulta que los datos sean efectivamente eliminados, más aún si es que ya fueron divulgados, ya que, una vez que los datos se han compartido con terceros, la persona que revoca su autorización no puede controlar directamente esos datos fuera del ámbito de la organización original que los recopiló, lo cual termina por dejar en manos de terceros si los datos son o no eliminados de forma definitiva.

2) Principio de finalidad

El legislador de datos personales ha establecido que todo tratamiento de datos personales debe realizarse para finalidades **específicas y legítimas**. Al respecto, se ha señalado que este principio "*es quizá el más relevante dentro de los principios rectores en el tratamiento de datos personales, ya que éstos pueden ser objeto de tratamiento en forma legítima sólo en cuanto respondan a una finalidad concreta y determinada, además de que las operaciones que recaigan sobre ellos no excedan de aquella*"[296].

Este principio se encuentra consagrado expresamente en el inciso 1º del artículo 9 de la LPVP[297], según el cual "[l]*os datos personales deben utilizarse sólo para los fines para los cuales hubieren sido recolectados, salvo que provengan o se hayan recolectado de fuentes accesibles al público*"[298]. En el mismo sentido, el inciso 2º del artículo 1° de la LPVP dispone que *"*[l]*a persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público"*[299].

[295] Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999. Artículo 4.
[296] CERDA, Alberto. Intimidad de los trabajadores y tratamiento de datos personales por los empleadores. Revista Chilena de Derecho Informático, 2003, no 2, pp. 35-59. p. 46.
[297] VERDUGO, Francisco. *Los principios, derechos del titular de datos y deberes del responsable de datos, en la Ley Nº 19.62*8. En "Derecho Informático", JIJENA, Renato. Editorial: El Jurista, 2022, p.467.
[298] Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999. Artículo 9.
[299] *Ibíd*. Artículo 1.

Así las cosas, el responsable del banco de datos tiene el deber de observar estrictamente el cumplimiento de dicho propósito en toda ocasión que haga uso, o, en términos más amplios, "trate" información de carácter personal[300]. Para garantizar que este deber sea debidamente cumplido, la ley ha concedido al titular de datos personales los derechos ARCO, los cuales serán objeto de estudio más adelante.

Ahora bien, cabe hacer énfasis en la amplitud de la excepción a este principio, según la cual no es necesario respetar el principio de finalidad si es que los datos provienen o han sido recolectados de fuentes accesibles al público[301], puesto que, si bien la disposición se refiere a las fuentes accesibles al público como una excepción al principio de finalidad, en la práctica dichas fuentes constituyen la regla general en materia de tratamiento de datos, dado que la ley las define en términos amplios como "registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes"[302].

3) Principio de calidad de los datos

Este principio se desprende del artículo 9 de la LPVP, específicamente del inciso 1º, ya transcrito, y del inciso 2º, según el cual "*la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos*"[303].

Al respecto, se ha señalado que la concreción de este principio requiere de tres condiciones copulativas:

1. Los datos, tanto en su recogida como en su tratamiento, deben ser exactos, actualizados y responder con veracidad a la situación real del titular.
2. Los datos personales sólo pueden utilizarse para los fines para los cuales se recolectaron, salvo que provengan o se hayan recolectado de fuentes accesibles al público.

[300] VERDUGO, op. cit, p.467.
[301] Ley N° 19.628. CHILE, op. cit. Artículo 4.
[302] VERDUGO, Francisco. *Los principios, derechos del titular de datos y deberes del responsable de datos, en la Ley Nº 19.62*8. En "Derecho Informático", JIJENA, Renato. Editorial: El Jurista, 2022, p.468.
[303] Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999. Artículo 4.

3. Los datos personales deben ser eliminados o cancelados en aquellos casos en que su almacenamiento carezca de fundamento legal o bien cuando hayan caducado[304].

Conforme al tercer requisito, denominado "limitación de almacenamiento", los datos personales deben mantenerse sólo durante el tiempo necesario para cumplir con la finalidad del procesamiento. A su respecto, el artículo 6 de la ley prescribe:

> *"Los datos personales deberán ser eliminados o cancelados cuando su almacenamiento carezca de fundamento legal o cuando hayan caducado.*
>
> *Han de ser modificados cuando sean erróneos, inexactos, equívocos o incompletos.*
>
> *Se bloquearán los datos personales cuya exactitud no pueda ser establecida o cuya vigencia sea dudosa y respecto de los cuales no corresponda la cancelación.*
>
> *El responsable del banco de datos personales procederá a la eliminación, modificación o bloqueo de los datos, en su caso, sin necesidad de requerimiento del titular."*[305].

Como queda de manifiesto, el principio de calidad también se relaciona con el derecho del titular de sus datos a cancelar o eliminar su información personal[306], el cual se enmarca dentro de lo que la doctrina denomina "derechos ARCO", los que veremos a continuación.

4) Derechos ARCO

La LPVP contempla dentro de su regulación los denominados "derechos ARCO", que corresponden a los derechos de acceso, rectificación, cancelación y oposición[307]. De manera

[304] ANGUITA, Pedro. *La protección de datos personales y el derecho a la vida privada. Santiago, Editorial Jurídica*, 2007. pp. 298-299.
[305] Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999. Artículo 6.
[306] VERDUGO, Francisco. *Los principios, derechos del titular de datos y deberes del responsable de datos, en la Ley Nº 19.628.* En "Derecho Informático", JIJENA, Renato. Editorial: El Jurista, 2022, p.487.
[307] CÁMARA DE DIPUTADOS (CHILE). *Evaluación de la Ley N° 19.628. Protección de la Vida Privada*, agosto 2016. p.59.

general, conforme a estos derechos el titular tiene derecho a acceder a sus datos personales y conocer la información que se está tratando; a corregir datos inexactos o incompletos sobre sí mismo; y, a solicitar la eliminación de sus datos personales en ciertas circunstancias, lo cual se desprende de los primeros cuatro incisos del artículo 12 de la Ley, que señalan:

> *"Toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente.*
>
> *En caso de que los datos personales sean erróneos, inexactos, equívocos o incompletos, y así se acredite, tendrá derecho a que se modifiquen.*
>
> *Sin perjuicio de las excepciones legales, podrá, además, exigir que se eliminen, en caso de que su almacenamiento carezca de fundamento legal o cuando estuvieren caducos.*
>
> *Igual exigencia de eliminación, o la de bloqueo de los datos, en su caso, podrá hacer cuando haya proporcionado voluntariamente sus datos personales o ellos se usen para comunicaciones comerciales y no desee continuar figurando en el registro respectivo, sea de modo definitivo o temporal (...)*[308].

A continuación, de manera particular, se abordarán brevemente los cuatro derechos antes mencionados. En primer lugar, el derecho de acceso permite a los titulares de los datos personales acceder al registro o base de datos para conocer qué datos se tratan en ésta, cuál es su objetivo y quién los trata; cómo se obtuvieron, quién el responsable o controlador de dicho registro y si estos datos serán o no cedidos a un tercero[309].

En segundo lugar, el derecho a rectificación permite al titular de los datos solicitar al responsable de una base de datos que corrija, actualice o modifique los datos si así correspondiese, por ser inexactos, erróneos, equívocos o incompletos[310].

---

[308] Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999. Artículo 12.

[309] FUNDACIÓN DATOS PROTEGIDOS. *Una propuesta a la ley de datos personales en Chile. Los datos más allá de la privacidad.* Santiago, Chile < https://datosprotegidos.org/wp-content/uploads/2017/11/InformeLeyDatos_FDP-3.pdf> [consulta: 02 septiembre 2023]. p.5.

[310] GARRIDO, Romina. *El Habeas data y la ley de protección de datos en Chile.* Serie Bibliotecología y Gestión de Información, (83):1-24, Jul-2013. p.15.

En tercer lugar, conforme al derecho a cancelación, se permite al titular solicitar la eliminación del dato cuando el almacenamiento carezca de fundamento legal o el dato estuviere caduco[311]. En otras palabras, este derecho obliga a eliminar los datos personales recopilados si se pierde la habilitación legal para tratarlos; si se revoca el consentimiento por parte del titular, si hay un cambio en las circunstancias que dieron pie a su entrega o si hay modificaciones en los mismos[312].

En cuarto y último lugar, el derecho de oposición es aquel que se ejerce en contra del responsable del registro para impedir que se lleve a cabo el tratamiento de datos de carácter personal o, bien, frenar el mismo[313].

Ahora bien, la Ley no sólo regula los conceptos de cada uno de los derechos ARCO, sino también establece una serie de normas en torno a los mismos. Así, por ejemplo:

1. Establece la gratuidad, en virtud de la cual la información, modificación o eliminación de los datos serán absolutamente gratuitas[314];
2. Regula el caso de que los datos cancelados o modificados hubieran sido comunicados previamente a terceros, en cuyo caso el responsable de los datos deberá dar aviso a la brevedad[315];
3. Establece que estos derechos pueden estar limitados por ningún tipo de medio o convención, de forma tal que no es posible renunciar a los mismos ni a su ejercicio[316]; y,
4. Sin perjuicio de lo anterior, establece que no se trata de derechos absolutos, en tanto contempla dos excepciones en que no es posible pedir información, modificación, cancelación o bloqueo de los datos:
    a. Cuando aquello impida o entorpezca el debido cumplimiento de las funciones fiscalizadoras del organismo público requerido, o afecte la reserva o secreto

311 *Ibíd.,* p.17.
312 FUNDACIÓN DATOS PROTEGIDOS, op. cit.
313 *Ibíd.*
314 Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999. Artículo 12.
315 *Ibíd*.
316 *Ibíd*. Artículo 13.

establecidos en disposiciones legales o reglamentarias, la seguridad de la Nación o el interés nacional; y,

b. Cuando los datos hubieren sido almacenados por mandato legal, fuera de los casos contemplados en la ley respectiva[317].

Sin perjuicio de lo anterior, es importante mencionar que la normativa actual no consagra lo que se conoce como "derecho a la portabilidad de los datos personales", que ni siquiera fue considerado dentro de los derechos ARCO, lo cual queda de manifiesto en la historia de la Ley, que no lo menciona ni una sola vez[318], y que ha sido fuertemente criticado.

5) Principio de seguridad

Conforme a este principio, también conocido como "deber general de cuidado" en el tratamiento de datos personales, las empresas deben garantizar la protección de los datos personales que recopilan y utilizan. Al respecto el artículo 11 de la LPVP prescribe que "[e]*l responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia (...)*"[319].

En la práctica, este principio exige que se adopten medidas apropiadas para proteger los bancos de datos contra los riesgos naturales, como la pérdida accidental o la destrucción por siniestro, y contra los riesgos humanos, como el acceso sin autorización, la utilización encubierta de datos o la contaminación por virus informático[320].

Asimismo, obliga a que todos los que trabajan en el tratamiento de datos personales, ya sean organismos públicos o privados, deban guardar secreto o reserva de la información que haya transitado y de la que ellos hayan tenido conocimiento.

---

[317] *Ibíd*. Artículo 15.

[318] BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. *Historia de la Ley N° 19.628. Sobre protección de la vida privada.* [en línea] <https://obtienearchivo.bcn.cl/obtienearchivo?id=recursoslegales/10221.3/71204/1/documento_3969_1693927810119.pdf> [consulta: 25 de octubre 2023].

[319] Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999. Artículo 11.

[320] JERVIS, Paula. La regulación del mercado de datos personales en Chile. Tesis (Magíster en Derecho). Santiago, Chile. Universidad de Chile, Facultad de Derecho, 2006. 65 h.

6) Régimen de responsabilidad

Conforme a este principio, quienes traten datos personales, ya sean personas naturales o jurídicas, deben hacerse responsables de los daños producidos a los titulares de tales datos con ocasión de la recolección, tratamiento, utilización y comunicación a terceros de los mismos.

Según dispone el artículo 11 de la LPVP, "[e]*l responsable de los registros o bases donde se almacenen datos personales con posterioridad a su recolección deberá cuidar de ellos con la debida diligencia, haciéndose responsable de los daños"*[321]. Mediante esta norma el legislador consagró un régimen de responsabilidad subjetiva, por tanto, quien reclama que se le produjo un daño en el tratamiento de sus datos, debe probar los perjuicios que alega, los cuales pueden ser de carácter moral o patrimonial.

II. Circulares Interpretativas del SERNAC

En la sección anterior, se analizó en qué medida las leyes chilenas vigentes permiten responder a ciertos desafíos planteados por el uso de IA en las relaciones de consumo. En la sección actual, se examinarán tres Circulares Interpretativas del SERNAC contingentes para la materia, las cuales dicen relación con el sentido y alcance de derechos, obligaciones, principios y/o herramientas consagradas en la Ley Nº 19.496 y en la Ley Nº 19.628 que permiten, sea directa o indirectamente, hacer frente a los desafíos identificados. Estas son:

1) Circular Interpretativa sobre protección de consumidores frente al uso de sistemas de Inteligencia Artificial, aprobada mediante la Resolución Exenta Nº 33/2022;
2) Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión de consumo, aprobada mediante la Resolución Exenta Nº 931/2021; y,
3) Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores, aprobada mediante la Resolución Exenta Nº174/2023.

[321] Ley N° 19.628. CHILE, op. cit.. Artículo 11.

Se realizará un examen más detallado y esquematizado respecto de la primera Circular, por ser la única que trata en forma específica el fenómeno de la IA. Las otras Circulares serán analizadas únicamente en aquellos aspectos que, indirectamente, puedan resultar pertinentes en relación a la regulación o mitigación de los riesgos derivados del uso de esta tecnología en las relaciones de consumo.

1. Circular Interpretativa sobre protección de consumidores frente al uso de sistemas de Inteligencia Artificial

Esta Circular Interpretativa del SERNAC, aprobada mediante la Resolución Exenta N° 33, contiene criterios o lineamientos que aplica -a la fecha- la institución, "*tendientes a una adecuada aplicación de distintas normas que dicen relación con el consumidor, en aquellos casos en que un proveedor emplee sistemas de IA cuyas evaluaciones, recomendaciones o decisiones influyan de manera sustantiva en alguna de las fases del vínculo contractual, así como también cuando un sistema de IA constituya un componente de los productos que el proveedor vende o de los servicios que presta*"[322].

El documento comienza dando una introducción al rol de la IA en las relaciones de consumo[323]. Luego, menciona sucintamente los principales riesgos para los derechos de los consumidores derivados del uso de IA[324]. Dentro de ellos, destaca la manipulación a través de *dark patterns*, el perfilamiento o puntuación de clientes, la discriminación de precios, la imprevisibilidad de la toma de decisiones, el peligro hacia la seguridad del consumidor y la facilitación de acuerdos colusorios[325].

Una vez identificados los riesgos, la Circular entrega reglas interpretativas que resultan relevantes en este contexto, y que refieren a principios, derechos y obligaciones contenidos en la normativa sobre protección de los consumidores [326]. Estos son:

---

[322] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 33 que Aprueba Circular Interpretativa sobre Protección de los Consumidores frente al uso de sistemas de Inteligencia Artificial en las relaciones de consumo. Santiago, Chile, 18 de enero de 2022.. 6p.
[323] *Ibíd.*, p. 3.
[324] *Ibíd.*, pp. 4-6.
[325] *Ibíd.*, pp. 4-6.
[326] *Ibíd.*, pp. 6-13.

i. Entrega de información veraz, oportuna y transparente;
ii. Resguardo de la libertad de elección;
iii. Seguridad en el consumo;
iv. Prohibición de toda discriminación arbitraria; y,
v. Protección de los datos personales de los consumidores.

A continuación, se abordará lo dicho por la Circular respecto de cada uno de estos acápites. Al momento de examinar cada regla interpretativa, se hará un resumen del análisis efectuado por la Circular y se formulará un comentario al respecto. Una vez que se terminen de analizar todas las reglas, se realizará un análisis crítico de los aspectos positivos y negativos de la Circular.

i. Entrega de información veraz, oportuna y transparente

La circular comienza citando el artículo 3 letra b) de la LPDC, aludiendo a que los proveedores deben entregar a los consumidores información veraz y oportuna sobre diversos aspectos relevantes de la relación de consumidores, asegurándose de que esta sea suministrada en forma completa, pertinente, accesible, transparente y comprensible[327].

Ello implica que los proveedores han de comunicar a los consumidores información relativa al funcionamiento de sistemas de IA cuando estos efectúen recomendaciones, tomen decisiones o constituyan un rasgo o característica relevante que incida en alguna de las fases de la relación de consumo[328]. En concreto:

> "*[L]os proveedores deben presentar a los consumidores información significativa, entendida como información clara, comprensible y transparente con respecto a: (a) el objetivo o finalidad de los sistemas de IA empleados; (b) su injerencia en el proceso de contratación o de ejecución del contrato, en caso que corresponda; (c) la naturaleza de la interrelación del sistema de IA con el consumidor, en caso que corresponda (en particular, los proveedores deben informar en forma transparente y oportuna si el consumidor está interactuando con un sistema de IA y no con un ser humano, junto con las implicancias*

[327] *Ibíd.*, p. 7.
[328] *Ibíd,* p. 7.

asociadas); y, (d) los datos personales que son tratados por el sistema, incluyendo los tipos de tratamiento que tienen lugar para llegar a una decisión de parte del sistema de IA y su finalidad. De igual manera, cuando un sistema de IA constituya un componente relevante de los productos que el proveedor vende o de los servicios que presta (artículo de IA de consumo), deben informarse los instructivos de uso o condiciones mínimas bajo las cuales funciona dicho sistema"[329].

Por último, se destaca la importancia de los deberes de información para calificar el mérito de ciertas decisiones tomadas por la IA que requieren de justificación objetiva (por ejemplo, el rechazo de una solicitud crediticia), así como para establecer y/o ponderar eventuales responsabilidades de los proveedores[330].

Se trata de un análisis valioso, por cuanto, a partir de los deberes genéricos de información previstos en la normativa, se llega a una conclusión sobre la información concreta que los proveedores que utilizan sistemas de IA deben entregar a los consumidores. Empero, hay dos aspectos que admiten cuestionamientos.

En primer lugar, la interpretación amplia que se da a los deberes de información pareciera no quedar suficientemente bien justificada. Si bien, como se analizó *supra*, el artículo 3 letra b) de la LPDC posee un alcance que va más allá de su sentido literal y existen otros preceptos que destacan la importancia de la forma en que se entrega la información, no queda claro el fundamento normativo en base al cual el proveedor estaría obligado a informar respecto de sistemas de IA que, no obstante incidir en la relación de consumo, no forman parte del bien o servicio mismo.

Lo anterior, atendido que el artículo 3 letra b) alude únicamente a las características relevantes del bien o servicio. Así, en principio, el deber de información veraz, oportuna y transparente no aplicaría, por ejemplo, respecto de algoritmos de una plataforma web que efectúen recomendaciones en una fase precontractual, pero no integren el bien o servicio a

[329] *Ibíd.*, p. 7.
[330] *Ibíd.*, p. 8.

comercializar. Ahora bien, ello no obsta a que pueda arribarse a una conclusión contraria recurriendo a elementos normativos adicionales[331]. Pero la Circular no ahonda al respecto.

En segundo lugar, y más importante aún, la Circular nada dice respecto de cómo garantizar el cumplimiento de estos deberes en la práctica. Aun cuando resulte claro que el proveedor está obligado a entregar información, no se explica cómo juega ello, por ejemplo, con la opacidad de la IA o con la legítima ignorancia que el proveedor puede poseer respecto de sistemas complejos.

ii. Resguardo de la libertad de elección

La Circular comienza citando el artículo 3º letra a) de la LPDC, que consagra el derecho de los consumidores a elegir libremente los bienes y servicios. En seguida, indica que los sistemas de IA pueden afectar dicha autonomía en diversas fases del vínculo de consumo, a través de recomendaciones personalizadas hostigantes o mediante manipulaciones directas a su voluntad[332].

Asimismo, la explotación de sesgos cognitivos, la utilización de algoritmos predictivos y el empleo de *dark patterns* pueden reducir o incluso eliminar la capacidad de decisión del consumidor, ya que este es dirigido a un entorno de elección restringido en donde, en forma inconsciente, puede tomar decisiones perjudiciales que de otro modo no habría tomado, de suerte que su consentimiento terminaría siendo viciado[333].

En el presente acápite, el SERNAC deja en evidencia la importancia de la autonomía del consumidor y cómo esta puede verse afectada por los sistemas de IA. Sin embargo, más allá de resaltar la atingencia del derecho consagrado en el artículo 3º letra a) de la LPDC, no se explica qué puede hacer el proveedor –o, en su caso, el propio consumidor– para evitar que en la práctica los sistemas de IA lesionen el derecho a la libre elección.

---

[331] En efecto, una interpretación sistemática de las diversas herramientas que se analizaron en la primera parte del presente capítulo (deber de profesionalidad, principio de transparencia y control de cláusulas abusivas), podría llevar a concluir que, teniendo como principal fundamento la buena fe, el deber de información puede cubrir aspectos que vayan más allá de los componentes relevantes del bien o servicio mismo.

[332] *Ibíd*., p. 8.

[333] *Ibíd.,* pp. 8-9.

iii. Seguridad en el consumo

La Circular parte citando el artículo 3º letra d) de la LPDC, relativo al derecho a la seguridad en el consumo del que gozan los consumidores. Ello supone, como contrapartida, el deber del proveedor de mitigar los riesgos que puedan derivarse de los bienes y/o servicios que comercializan[334].

Por tanto, los proveedores están obligados a cuidar que los sistemas de IA que empleen presenten "*estándares adecuados de precisión, fiabilidad y efectividad técnica, con el fin de obtener resultados fundados, basados en procedimientos fiables, evitando que estos causen un daño a los consumidores, ya sea este material o inmaterial*"[335]. Vale decir, los proveedores deben realizar una evaluación de riesgos, actuando en forma responsable y diligente[336].

Sin perjuicio de la poca extensión que el SERNAC destina a este acápite, la interpretación que se da al deber de seguridad es clara. Asimismo, el análisis no admite la misma crítica de las secciones anteriores, ya que, a diferencia de lo que ocurre con otros deberes o derechos, sí se explica cómo el proveedor puede evitar daños a la seguridad. En efecto, se propone un deber de cuidado y diligencia del proveedor en orden a evaluar el riesgo de los sistemas empleados, lo que pareciera ser bastante efectivo y factible de implementar.

iv. Prohibición de toda discriminación arbitraria

La Circular emprende el análisis citando el artículo 3 letra c) de la LPDC, que consagra el derecho de los consumidores a no ser discriminados arbitrariamente por parte de los proveedores. Luego, explica que la discriminación arbitraria consiste en efectuar tratos, distinciones, exclusiones o restricciones que carecen de justificación razonable o atentan en contra la dignidad de los consumidores. Ello puede plasmarse, por ejemplo, en la negativa de venta, en el abuso en los sistemas de seguridad y en la publicidad ilícita[337].

---

[334] *Ibíd.*, p. 9.
[335] *Ibíd.*
[336] *Ibíd*.
[337] *Ibíd.,* p. 10.

Respecto de los sistemas de IA, se advierte que estos pueden ser propensos a efectuar discriminaciones arbitrarias, debido al procesamientos de datos incorrectos, a sesgos algorítmicos o a deficiencias en el proceso de elaboración de perfiles[338]. Adicionalmente, es posible que la IA efectúe discriminaciones de precios que atenten en contra de los derechos de los consumidores, y/o que los sistemas de vigilancia que emplean esta tecnología vulneren injustificadamente las garantías fundamentales de las personas. En este último sentido, resulta relevante el artículo 15 LPDC, que indica que los proveedores deben respetar en todo momento la dignidad y los derechos de las personas[339].

Así, los proveedores deben resguardar el derecho de los consumidores a no ser discriminados, impidiendo la amplificación de prejuicios o sesgos que restrinjan la igualdad de acceso o trato –especialmente si los consumidores pertenecen a grupos vulnerables o históricamente excluidos–[340], e implementando medidas que aseguren que no se creen ni perpetúen discriminaciones arbitrarias (por ejemplo, procurar justificar cada una de las decisiones automatizadas)[341].

En este acápite se aborda correctamente el derecho a la no discriminación arbitraria y las formas en que la utilización de IA puede generarla o acentuarla. Asimismo, se proponen medidas que el proveedor puede implementar a fin de evitar que esta se materialice. No obstante, se extraña la mención a la transparencia y a la auditoría algorítmica, que resultan relevantes al momento de entender los motivos que subyacen a las decisiones de la IA. No pareciera ser suficiente establecer la obligatoriedad de que el proveedor trabaje en evitar las discriminaciones arbitrarias si es que no se fijan mecanismos para controlar las decisiones automatizadas –más allá de exigir una justificación–-.

v. Protección de los datos personales de los consumidores

La Circular menciona, primeramente, que el procesamiento de datos es ínsito al funcionamiento de la IA. Considerando que las decisiones automatizadas a menudo buscan

[338] *Ibíd.*
[339] *Ibíd.*
[340] *Ibíd.*, p. 11.
[341] *Ibíd.*

predecir comportamientos de los consumidores u orientarlos en sus necesidades de compra, se llevan a cabo diversas actividades de tratamiento de datos personales[342].

En este contexto, es menester tener presente que la protección de datos personales está consagrada constitucionalmente (artículo 19 Nº4 de la Constitución Política de la República) y la forma y condiciones en que se tratan los datos deben apegarse estrictamente a las disposiciones de la Ley Nº 19.628.

Una vez identificado el marco normativo, la Circular cita los artículos 2 letra f), letra n) y letra o) de la Ley Nº 19.628, para efectos de definir qué se entiende por datos personales y por su tratamiento. Se concluye que las operaciones de análisis automatizado que buscar realizar predicciones, recomendaciones o decisiones en el marco de una relación de consumo, quedan comprendidas dentro de la noción legal amplia de las actividades de tratamiento de datos personales, y que el proveedor asume la calidad de responsable su tratamiento[343].

Luego, se explica que el proceso de tratamiento de datos personales de la IA comprende diversas fases, que van desde la recopilación y medición de datos relevantes para el uso del sistema, hasta la prueba del modelo algorítmico y el uso o despliegue del sistema[344]. Es importante que durante todas estas fases se observen las reglas contenidas en la normativa de protección de datos personales, así como los principios de licitud, proporcionalidad, finalidad, confidencialidad, seguridad y responsabilidad en el tratamiento[345].

Adicionalmente, en virtud de lo previsto en el artículo 4 de la Ley Nº 19.628, si la base legal que autoriza el tratamiento de los datos personales es el consentimiento de su titular, el proveedor debe resguardar que dicho consentimiento haya sido obtenido válidamente y que se preste en forma específica, informada y expresa (por escrito), de modo que el consumidor tenga claridad respecto del propósito por el cual se recopilan sus datos[346].

De igual manera, a la luz de los artículos 6 y 9 de Ley Nº 19.628, es relevante que los datos utilizados por la IA sean actualizados y exactos, y que su tratamiento se apegue

[342] *Ibíd.*
[343] *Ibíd*., p. 12.
[344] *Ibíd*.
[345] *Ibíd.*
[346] *Ibíd.*, pp. 12-13.

estrictamente a los fines para los cuales hubieren sido recolectados -en línea con lo que se comunicó al consumidor al momento de obtener su consentimiento-[347].

También se ahonda en el deber de seguridad que recae en la entidad responsable del tratamiento de datos personales, en virtud del artículo 11 de la Ley Nº 19.628. Dicho deber se "*traduce en la necesidad de aplicar medidas de seguridad técnicas y organizativas adecuadas, que garanticen la confidencialidad, integridad y disponibilidad de los datos personales en cuestión, teniendo especialmente presentes los riesgos que conllevan las actividades de tratamiento y la naturaleza de los datos almacenados (atendiendo, entre otros elementos, a su nivel de sensibilidad)*"[348]. De este modo, el deber de protección que recae en los datos de carácter sensible -frecuentemente utilizados para elaborar perfiles de los consumidores- es aún más intenso[349].

Por último, se menciona que los proveedores que utilizan sistemas de IA que tratan datos personales, deben garantizar en todo momento el ejercicio de los derecho ARCO (acceso, rectificación, cancelación o eliminación, oposición y bloqueo) al titular de dichos datos, sin entorpecer su ejercicio[350].

Este acápite es, probablemente, aquel en el que el SERNAC realiza un mayor desarrollo, ya que analiza varios preceptos legales e indica en forma precisa las implicancias que cada uno de ellos posee en el contexto de las relaciones de consumo, así como las conductas que ha de emplear el proveedor para evitar la transgresión de los derechos consagrados.

Ahora bien, llama la atención que la postura de la institución pareciera ser que el tratamiento de datos personales no resulta problemático en la medida en que se observen las disposiciones de la Ley Nº 19.628, pues no analiza elementos ni resguardos adicionales que deban considerarse además de aquellos que emanan directamente de dicha Ley. Ello resulta extraño si se tiene en cuenta que, en las Circulares Interpretativas que se examinarán

[347] *Ibíd*., p. 13.
[348] *Ibíd*.
[349] *Ibíd*., p. 13.
[350] *Ibíd.*

posteriormente, el SERNAC hizo alusión a la importancia del deber de profesionalidad[351] y de la transparencia[352] en el tratamiento de datos personales –vale decir, recurrió a la LPDC para complementar los deberes–.

Análisis General

Luego de examinar la Circular Interpretativa del SERNAC sobre protección de consumidores frente al uso de sistemas de Inteligencia Artificial, puede concluirse que es destacable que no solo se hayan identificado derechos y deberes de las relaciones de consumo que resultan atingentes para estos efectos, sino que también se haya fijado adecuadamente su sentido y alcance.

En efecto, a pesar de que el texto de la LPDC no ha sido actualizado, la Circular logra plasmar claramente la forma en que los derechos de los consumidores y los deberes de los proveedores cobran relevancia en el contexto de la utilización de IA, indicando incluso, en algunos casos, la diligencia concreta que ha de observar al proveedor.

Con todo, la Circular admite importantes críticas en dos aspectos. La primera de ellas es la que se ha tratado de transmitir al momento de analizar la mayoría de las reglas interpretativas: si bien se explica la importancia y el alcance de ciertos derechos y deberes, no se suele ahondar en herramientas que sirvan para garantizar su cumplimiento. Dicho nivel de análisis solo se encuentra presente, en parte, en lo relativo al deber de seguridad y al tratamiento de datos personales. Pero se ausenta en el resto de las reglas.

Así como se interpretaron dichos derechos o deberes concretos, podrían haberse interpretado otros preceptos de la LPDC que, al consagrar mecanismos de protección generales, vuelven menos probable la vulneración a aquellos derechos que se mencionaron. Ese es el caso del deber de profesionalidad, del control de cláusulas abusivas y del principio

[351] Véase: SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 174 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores. Santiago, Chile, 28 de febrero de 2022. 21p.

[352] Véase: SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 931 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión de consumo. Santiago, Chile, 03 de diciembre de 2021. 14p; y SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 174 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores. Santiago, Chile, 28 de febrero de 2022. 14p.

de transparencia, que, no obstante su pertinencia, se encuentran totalmente ausentes en el documento. En tal sentido, hubiese sido deseable que se realizara un ejercicio similar al desarrollado en la primera parte del presente Capítulo, cuando se analizaron las herramientas previstas en la LPDC para evitar la disminuir los riesgos hacia los consumidores.

La segunda crítica apunta al instrumento jurídico utilizado para consagrar los criterios y lineamientos. Lo que caracteriza a las Circulares Interpretativas es que, por su naturaleza, resultan vinculantes únicamente para los funcionarios del organismo que las dicta[353]. Así lo reconoce, por lo demás, esta propia Circular al momento de indicar su ámbito de aplicación[354].

A falta de otra norma, las Circulares Interpretativas sirven de inspiración y guía para los operadores jurídicos. Sin embargo, ello no les dota de fuerza obligatoria, de suerte que los proveedores podrían desentenderse de los criterios planteados sin temor a recibir consecuencia jurídica alguna. Considerando la importancia de la materia y la ausencia de regulación específica, hubiese sido deseable que, en lugar de dictar la Circular, la institución hubiera hecho uso de su facultad prevista en el artículo 58 letra c) LPDC[355] para, por ejemplo, abogar por la dictación de un reglamento o por la realización de una reforma legal, cuyas disposiciones resultarían extensibles a todos los agentes de las relaciones de consumo.

2. Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión de consumo

Esta Circular Interpretativa del SERNAC, aprobada mediante la Resolución Exenta N° 931 el 03 de diciembre de 2021, tiene por objeto interpretar las normas relativas a cláusulas abusivas, así como también sistematizar el trabajo que ha realizado la institución respecto de la aplicación los diversos literales del artículo 16 de la LPDC, el cual contempla una serie de

[353] DFL 3. CHILE. Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021. Artículo 58 letra b).

[354] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 33 que Aprueba Circular Interpretativa sobre Protección de los Consumidores frente al uso de sistemas de Inteligencia Artificial en las relaciones de consumo. Santiago, Chile, 18 de enero de 2022.. 13p.

[355] DFL 3. CHILE. op. cit. Artículo 58 letra c), que indica que el SERNAC posee la facultad de: "*Proponer fundadamente al Presidente de la República, a través del Ministerio de Economía, Fomento y Turismo, la dictación, modificación o derogación de preceptos legales o reglamentarios en la medida que ello sea necesario para la adecuada protección de los derechos de los consumidores*".

cláusulas que se consideran abusivas en las relaciones de consumo y que, en consecuencia, no producen efecto alguno por orden del legislador[356]. La norma dispone:

> *"No producirán efecto alguno en los contratos de adhesión las cláusulas o estipulaciones que:*
>
> *a) Otorguen a una de las partes la facultad de dejar sin efecto o modificar a su solo arbitrio el contrato o de suspender unilateralmente su ejecución, salvo cuando ella se conceda al comprador en las modalidades de venta por correo, a domicilio, por muestrario, usando medios audiovisuales, u otras análogas, y sin perjuicio de las excepciones que las leyes contemplen;*
>
> *b) Establezcan incrementos de precio por servicios, accesorios, financiamiento o recargos, salvo que dichos incrementos correspondan a prestaciones adicionales que sean susceptibles de ser aceptadas o rechazadas en cada caso y estén consignadas por separado en forma específica;*
>
> *c) Pongan de cargo del consumidor los efectos de deficiencias, omisiones o errores administrativos, cuando ellos no le sean imputables;*
>
> *d) Inviertan la carga de la prueba en perjuicio del consumidor;*
>
> *e) Contengan limitaciones absolutas de responsabilidad frente al consumidor que puedan privar a éste de su derecho a resarcimiento frente a deficiencias que afecten la utilidad o finalidad esencial del producto o servicio;*
>
> *f) Incluyan espacios en blanco, que no hayan sido llenados o inutilizados antes de que se suscriba el contrato;*
>
> *g) En contra de las exigencias de la buena fe, atendiendo para estos efectos a parámetros objetivos, causen en perjuicio del consumidor, un desequilibrio importante en los derechos y obligaciones que para las partes se deriven del contrato. Para ello se atenderá a la finalidad del contrato y a las disposiciones especiales o generales que lo rigen. Se presumirá que dichas cláusulas se encuentran ajustadas a exigencias de la buena fe, si los contratos a que pertenecen han sido revisados y autorizados por un órgano administrativo en ejecución de sus facultades legales, y*

[356] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 931 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión de consumo. Santiago, Chile, 03 de diciembre de 2021. 1p.

h) Limiten los medios a través de los cuales los consumidores puedan ejercer sus derechos, en conformidad con las leyes".

El instrumento analiza el ámbito de aplicación y los aspectos más relevantes de cada uno de los literales que contempla causales de abusividad. Se precisa su sentido y alcance, y se plantean ejemplos prácticos de desequilibrio abusivo de los derechos y obligaciones mediante la transcripción de cláusulas reales incluidas en contratos ofrecidos a consumidores en diversos mercados[357]. Se trata, sin duda, de un asunto que excede el objeto de estudio de la presente Memoria. Sin embargo, esta Circular formula ciertas interpretaciones sobre los tipos de cláusulas abusivas que pueden resultar de utilidad en relación a los contratos que regulan el uso de IA.

Como se explicó al abordar el control de cláusulas abusivas en el comienzo de este Capítulo, es usual que, cuando los proveedores emplean IA en sus plataformas o en sus productos o servicios, los documentos que contienen los términos y condiciones de uso y/o que disciplinan la responsabilidad del proveedor asuman la forma de un contrato de adhesión[358]. Al ser un contrato de adhesión, nuestro ordenamiento jurídico posibilita un control formal y material respecto de sus cláusulas, a fin de dejar sin efecto aquellas que sean abusivas.

La Circular que se analizará en forma posterior a esta, refiere a la misma materia, pero la circunscribe únicamente al tratamiento de datos personales. Por su parte, esta Circular, que fue dictada algunos meses antes, realiza un análisis respecto de las cláusulas abusivas en contratos de adhesión referidas a todo tipo de contenidos. Si bien también ahonda levemente en el tratamiento de datos personales –examinando, por ejemplo, la función del artículo 16 letra g) de la LPDC–[359], el presente apartado centrará su atención en la interpretación y control de cláusulas que puedan tener alguna incidencia en relación al uso de IA y no refieran a datos personales, a fin de evitar repetir los lineamientos que se expondrán al momento de estudiar la otra Circular.

---

[357] *Ibíd*., p. 3.

[358] DE LA MAZA, Íñigo. y MOMBERG, Rodrigo., 2017. *Términos y condiciones: Acerca del supuesto carácter contractual de las autorizaciones para el tratamiento de datos personales en sitios web*. Revista chilena de derecho y tecnología 6(2): p. 40, 2017.

[359] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 931 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión de consumo. Santiago, Chile, 03 de diciembre de 2021. 40p.

Esta Circular comienza hablando sobre los contratos de adhesión, las cláusulas abusivas y los mecanismos de control[360]. Una vez fijado el marco teórico, el documento interpreta cada uno de los literales del artículo 16 de la LPDC[361]. Al efecto, resulta útil tener a la vista lo dicho respecto de los artículos 16 letra c), letra e) y letra g).

En cuanto al artículo 16 letra c), el SERNAC indica que esta disposición busca evitar que se genere un traspaso no negociado de riesgos que vaya en perjuicio del consumidor[362]. Si no concurre (i) fuerza mayor, (ii) un hecho de un tercero sin vinculación jurídica con el proveedor o (iii) negligencia del consumidor, no resulta válido que el proveedor traspase al consumidor la responsabilidad por errores, omisiones o deficiencias[363]. En lo que atañe a la IA, dicha interpretación podría resultar relevante, porque si quien desarrolla los sistemas de IA es un tercero, este poseería un vínculo jurídico contractual con el proveedor, por lo que el proveedor no podría ampararse en aquella circunstancia para poner de cargo del consumidor las falencias de la tecnología.

En cuanto al artículo 16 letra e), la Circular explica que este precepto proscribe la validez de aquellas cláusulas que excluyen completamente la responsabilidad del proveedor frente a los consumidores. Luego, precisa que, si bien el artículo no lo indica, la jurisprudencia nacional se ha inclinado por entender que las cláusulas que limitan parcialmente la responsabilidad del proveedor también podrían ser abusivas en base a este literal[364]. La relevancia de dicha constatación reside en que el proveedor que emplea sistemas de IA y utiliza contratos de adhesión, no podría desentenderse, sea total o parcialmente, de los daños que dichos sistemas ocasionen a los consumidores.

En cuanto al artículo 16 letra g), el SERNAC precisa que, aun cuando no se adhiera a la postura de la jurisprudencia en orden a que las cláusulas que limitan parcialmente la responsabilidad son abusivas, de todas formas estas podrían ser susceptibles de anulación en base al literal g).[365] Adicionalmente, se señala que el precepto refiere a la buena fe objetiva,

[360] *Ibíd.*, pp. 4-16.
[361] *Ibíd.*, pp. 17-26.
[362] *Ibíd.*, p. 21.
[363] *Ibíd*., pp. 20-21.
[364] *Ibíd.*, pp. 22-23.
[365] *Ibíd*., p. 23.

la que debe ser observada por el proveedor en las diversas fases de íter contractual[366]. Por su parte, el desequilibrio importante en los derechos alude a un desequilibrio jurídico, que se produce, por ejemplo, cuando se contravienen las disposiciones generales o especiales que disciplinan el contrato[367].

En este sentido, en base al artículo 16 letra g) LPDC, y sin importar el momento en que sean suscritas, carecen de efectos las cláusulas que lleven al consumidor a renunciar anticipadamente a sus derechos[368], que afecten su derecho de acceso a la información[369] o que comprendan una avaluación anticipada de perjuicios[370], entre otros casos. Ello podría resultar útil para evitar la inclusión de cláusulas en las que el proveedor, bajo el pretexto de estar utilizando una tecnología, pretenda faltar a sus deberes legales y/o disminuir el estándar de protección al que tiene derecho el consumidor.

Como puede apreciarse, esta Circular no trata directamente sobre IA. No obstante, precisa el sentido y alcance que se otorga a la abusividad de ciertas cláusulas que, naturalmente, los proveedores que emplean sistemas de IA podrían verse tentados a incluir. Por tanto, contribuye a que exista una mayor claridad respecto del comportamiento que deben observar estos proveedores al disciplinar la relación con los consumidores.

3. Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores

Primeramente, es necesario señalar que esta Circular dictada por el SERNAC el día 28 de febrero de 2022, mediante la Resolución Exenta N°174, se encuentra directamente relacionada con la Circular Interpretativa N° 931, tratada en el numeral anterior, referida a las cláusulas abusivas contenidas en contratos de adhesión con consumidores, la cual aborda en su numeral 3.6, de manera preliminar e ilustrativa, algunas cláusulas incluidas en contratos de adhesión que autorizan a los proveedores para recolectar y tratar datos personales de

366 *Ibíd.*, p. 25.
367 *Ibíd.*, p. 26.
368 *Ibíd*., pp. 34-36.
369 *Ibíd.*, p. 38
370 *Ibíd.*, p. 43.

consumidores, examinándolas a la luz de la normativa sobre protección de los consumidores[371].

La propia Circular, dictada el 03 de diciembre de 2023, en el numeral antes referido -3.6- señala expresamente que el SERNAC "*abordará de manera específica, en una futura circular interpretativa, la equidad de las estipulaciones referidas a la recolección y tratamiento de datos personales de consumidores*."[372], lo cual se concretiza en la Circular que se analiza a continuación.

Esta Circular Interpretativa contiene los criterios o lineamientos que aplica el SERNAC al interpretar la normativa de protección al consumidor en relación con los términos contractuales bajo los cuales los consumidores autorizan a los proveedores la recolección y posterior tratamiento de sus datos de carácter personal, especialmente, el artículo 16 de la Ley N° 19.496[373], que regula los contratos de adhesión en las relaciones de consumo. En concreto, la Circular enlista una serie de cláusulas que, en caso de estar contenidas en este tipo de contratos, no producen efecto alguno por considerarse abusivas.

Con el propósito de exponer los referidos criterios interpretativos, la Circular los aborda en cinco secciones:

1. Control de forma: transparencia de las políticas de privacidad y de toda estipulación o condición vinculada al tratamiento de datos personales;
2. Cláusulas que contemplan la modificación, suspensión o terminación unilateral de la relación contractual;
3. Cláusulas que ponen de cargo del consumidor los efectos de eventuales deficiencias, omisiones o errores;
4. Cláusulas que contienen limitaciones absolutas de responsabilidad frente al consumidor: y,
5. Cláusulas que contravienen la buena fe contractual.

[371] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 174 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores. Santiago, Chile, 28 de febrero de 2022. 9p.
[372] *Ibíd.*
[373] *Ibíd.*

A continuación, se abordará lo dicho por la Circular en cada una de las secciones señaladas:

i. Control de forma: transparencia de las políticas de privacidad y de toda estipulación o condición vinculada al tratamiento de datos personales

En esta sección, la Circular comienza señalando la importancia del control de forma, en tanto, a su criterio, "*constituye la base para el cumplimiento de una serie de deberes y requisitos contenidos en la LPDC por parte de los proveedores, al garantizar a los consumidores el correcto acceso a la información necesaria e idónea para suscribir el contrato que contiene la relación de consumo*"[374].

Al respecto, dispone que la información que el proveedor debe proporcionar al consumidor para obtener de su parte una autorización válida que habilite el tratamiento de datos en el contexto de un contrato de consumo, debe ser específica tanto en lo que respecta a los datos personales tratados y a las actividades de tratamiento, como en lo concerniente al propósito del tratamiento[375].

Asimismo, menciona que la interacción armónica entre la normativa de protección al consumidor y los estándares sobre protección de datos personales implica que la transparencia de las políticas de privacidad que utilizan los proveedores para efectuar el tratamiento de datos personales de consumidores, puede extenderse a elementos de transparencia formal y transparencia sustantiva[376].

En ese sentido, en lo referente a la transparencia formal, indica que los proveedores deben, al utilizar en sus "Políticas de Privacidad" y en toda otra estipulación, condición o cláusula contractual vinculada a operaciones de tratamiento de datos personales de consumidores, un lenguaje claro y sencillo**,** permitiendo que dichos términos, aun versando sobre elementos de relativa complejidad técnica o jurídica, puedan ser comprensibles para un consumidor promedio[377]. Así las cosas, resulta entonces esperable que se evite el empleo de

[374] *Ibíd.,* p.11.
[375] *Ibíd.*, p.13.
[376] *Ibíd.*, p.14.
[377] *Ibíd.*

políticas de privacidad excesiva e innecesariamente extensas, desorganizadas, confusas o de difícil comprensión[378].

Por su parte, en lo que respecta a la transparencia sustantiva, la Circular señala que las políticas de privacidad y otras estipulaciones contractuales deben permitir a los consumidores conocer qué información concerniente a los mismos será recolectada y cómo esta información será usada[379].

ii. Cláusulas que contemplan la modificación, suspensión o terminación unilateral de la relación contractual

Respecto de este tipo de cláusulas abusivas, la Circular comienza señalando que su prohibición radica en que, atendida la asimetría ya existente entre proveedores y consumidores, su validez no haría más que intensificar aquella desigualdad a niveles irrisorios, dejando incluso el cumplimiento del contrato en manos únicamente de la voluntad del proveedor.

Referente a aquellos casos en que la fuente de licitud que habilita el tratamiento de datos es la autorización del titular de los mismos, la Circular señala que el proveedor debe poder garantizar la obtención de un consentimiento válido, esto es, de una autorización previa a la recolección, expresa (otorgada por escrito), voluntaria, informada y específica, y poder también proporcionar la verificabilidad del consentimiento obtenido. Además, el proveedor debe informar al consumidor titular de los datos que le asiste el derecho irrenunciable para revocar la autorización originalmente otorgada para tratar sus datos, aunque sin efecto retroactivo[380].

Asimismo, con respecto a la modificación de los términos y condiciones originalmente aceptados por el consumidor para la recolección y procesamiento de sus datos personales, dispone que es necesario distinguir entre las modificaciones sustanciales a las estipulaciones incluidas en políticas de privacidad y aquellas que no tienen esa calificación[381].

---

[378] *Ibíd.*
[379] *Ibíd.*, p.15.
[380] *Ibíd.*, p.18.
[381] *Ibíd.*

Se entiende por “sustanciales” aquellas que amplían la información que el consumidor autoriza sea recolectada por el proveedor, alteran las finalidades del tratamiento autorizando operaciones de procesamiento adicionales, incluyen nuevas categorías de terceros a quienes eventualmente se pueda transferir la información del consumidor, alteran el periodo durante el cual los proveedores conservarán la información, modifican las medidas adoptadas para resguardar la seguridad de la información personal de los consumidores, u otra de similar naturaleza con análogo impacto en el tratamiento de datos de los consumidores[382].

En ese sentido, dispone que tales modificaciones serán válidas en la medida que cuenten con la autorización explícita del consumidor que satisfaga los mismos estándares que debe cumplir la autorización original[383]. No cumplen con los requisitos de validez señalados aquellas fórmulas que se sirven de las casillas premarcadas autorizando el tratamiento de datos y de casillas “No acepto” sin marcar (modelos *opt-out*), al revestir el carácter de un mero consentimiento tácito, que no satisface el estándar de consentimiento explicito que establece la LPVP[384].

Por su parte, en cuanto a las modificaciones no sustanciales, señala que, si bien no requieren contar con la autorización explícita del consumidor para ser válidas, deben serle informadas bajo los estándares de transparencia correspondientes[385].

iii. Cláusulas que ponen de cargo del consumidor los efectos de eventuales deficiencias, omisiones o errores

Este tipo de cláusulas ponen en entredicho la adecuada observancia del deber de profesionalidad que recae sobre los proveedores, lo cual se relaciona, asimismo, con el principio de seguridad en el tratamiento de datos personales[386].

Conforme dispone la Circular, los proveedores deben tener especialmente presente los riesgos que conllevan las actividades de tratamiento de datos y la naturaleza de los datos

[382] *Ibíd.*, p.19.
[383] *Ibíd.*, p.18.
[384] *Ibíd.*, p.19.
[385] *Ibíd.*
[386] *Ibíd.*, p.21.

almacenados. En concreto, es necesario que apliquen medidas de seguridad integrales que permitan resguardar la confidencialidad, integridad y disponibilidad de los datos personales de consumidores contenidos en sus registros, con la finalidad de evitar la alteración, pérdida, transmisión y acceso no autorizado a los mismos.

Así las cosas, se entiende que las cláusulas mediante las cuales el proveedor desatienda su deber de profesionalidad en esta materia implican poner de cargo del consumidor los efectos de deficiencias, omisiones o errores administrativos, de modo que no producirán efecto alguno en base a lo previsto en el artículo 16 letra c) de la LPDC[387]. En otras palabras, el solo hecho de que las cláusulas no observen el deber de profesionalidad en el tratamiento de datos personales es considerado abusivo, aun cuando el traslado de responsabilidad no esté plasmado en términos expresos.

Adicionalmente, en relación al derecho a la seguridad en el consumo, señala que los proveedores deben adoptar las medidas necesarias para evitar los riesgos que puedan derivarse del uso o consumo de los productos o servicios que ofrecen, cualquiera sea la naturaleza de estos riesgos[388]. De esta manera, el proveedor, en cumplimiento de su obligación de seguridad, debe evitar vulnerar la garantía fundamental a la protección de datos personales[389].

iv. Cláusulas que contienen limitaciones absolutas de responsabilidad frente al consumidor: y,

El SERNAC sostiene que, en base a la causal contenida en el artículo 16 letra e) de la LDPC, resultan abusivas tanto las cláusulas que suprimen o excluyen de manera absoluta la responsabilidad del proveedor como aquellas que sólo la limitan parcialmente –aun cuando esto último no se consagre expresamente–, pudiendo incidir, entre otros aspectos, en la calificación de las obligaciones del proveedor, en el grado de diligencia que debe emplear o en la reducción de los perjuicios indemnizables[390].

[387] *Ibíd.*, p.22.
[388] *Ibíd.*
[389] *Ibíd.*
[390] *Ibíd.*, p.23.

En esta sección, la Circular hace especial énfasis en que la responsabilidad que recae en el proveedor que efectúa tratamiento de datos personales de consumidores, le obliga a controlar el cumplimiento de los estándares necesarios para la adecuada protección de los consumidores, mediante la adopción de soluciones técnicas diligentes que maximicen dicha protección conforme a sus deberes de profesionalidad y seguridad. Por tanto, las estipulaciones contractuales que de manera explícita o subrepticia eliminan total o parcialmente dicha responsabilidad socavan la antedicha obligación en desmedro de las garantías básicas que deben proteger a los consumidores, y por lo mismo, han de estimarse abusivas[391].

v. Cláusulas que contravienen la buena fe contractual

Finalmente, en la última sección, la Circular se refiere a la cláusula de abusividad, consagrada en el literal g) del artículo 16 de la LPDC, para lo cual comienza por señalar que esta buena fe es aquella denominada "objetiva", esto es, referente al deber de los contratantes de comportarse de manera correcta y leal[392].

Según señala la Circular, en virtud de este parámetro, al momento de redactar las estipulaciones de un contrato de adhesión, el proveedor debe considerar los intereses del consumidor, absteniéndose de defraudar sus razonables expectativas y prescindiendo de aquellas cláusulas que un contratante promedio (debidamente informado y en condiciones de paridad negocial) no hubiera pactado. Además, el contrato debería ser redactado de forma tal que dicho consumidor sea capaz de comprenderlo[393].

Asimismo, menciona, de modo clarificante, que revisten el carácter de abusivas, por contravenir las exigencias de la buena fe, aquellas estipulaciones que pretenden autorizar ciertas operaciones de recolección y tratamiento de datos que resultan excesivas o que se desvían del objetivo típico que un consumidor promedio busca satisfacer mediante la relación de consumo, teniendo en consideración sus razonables expectativas.

---

[391] *Ibíd.*, p.24.
[392] MOMBERG URIBE, Rodrigo; DE LA MAZA GAZMURI, Iñigo; PIZARRO WILSON, Carlos. La protección de los derechos de los consumidores: Comentarios a la ley de protección a los derechos de los consumidores. Santiago, Thomson Reuters, 2013. p. 339.
[393] *Ibíd.*, p.25.

Al respecto, prescribe que los proveedores deben implementar cambios en sus prácticas comerciales a efectos de permitir a los consumidores en los contratos de adhesión:

a. Autorizar de manera positiva y específica las distintas operaciones el tratamiento de datos personales de los consumidores que se proponen;
b. Otorgar autorizaciones de tratamiento supletorias que el usuario pueda denegar si así lo desea según sus preferencias;
c. Evitar la entrega de autorizaciones de tratamiento que se encuentren siempre atadas a una operación comercial con un objeto diferenciado[394].

En la misma línea, señala que los proveedores deberían adecuar la forma en que recaban la autorización de los usuarios para tratar sus datos personales en el marco de un contrato de adhesión, diferenciando la información personal que recaben en virtud o con ocasión de dichos contratos entre aquella que resulta estrictamente necesaria para cumplir con la finalidad específica del contrato y aquella que no[395]. Lo anterior, poniendo a disposición de los consumidores mecanismos que le permitan aceptar por separado las propuestas de tratamiento formuladas por el proveedor.

III. Proyectos de Ley

En esta tercera sección se analizarán tres proyectos de ley relevantes para el tema de la presente Memoria, que actualmente se encuentran en tramitación en el Congreso. Estos tienen como objetivo general la regulación de la IA, la protección de los consumidores y la regulación del tratamiento de datos personales, respectivamente.

En primer lugar, se estudiará el Proyecto de ley sobre IA y Robótica (Boletín 15869-19), que busca establecer un marco regulatorio general para el uso de IA, atendiendo a los riesgos surgidos a propósito del desarrollo, distribución, comercialización y utilización de esta tecnología[396].

---

394 *Ibíd.*, p.27.
395 *Ibíd.*, pp.28-29.
396 CÁMARA DE DIPUTADOS (Chile). Proyecto de Ley que Regula los Sistemas de Inteligencia Artificial, la Robótica y las Tecnologías Conexas en sus Distintos Ámbitos de Aplicación. Boletín Nº 15.869-19, refundido con Boletín Nº 16.821-19. Valparaíso, Chile, 24 de abril de 2023.

En segundo lugar, se examinará el Proyecto de ley "SERNAC te protege" (Boletín 16271-03), que tiene por principal objetivo fortalecer las facultades del Servicio Nacional del Consumidor y prevenir las infracciones a la normativa. La razón que motiva su estudio es que algunas de sus disposiciones resultan interesantes desde el punto de vista de las nuevas tecnologías y dinámicas de las relaciones de consumo[397].

Finalmente, en tercer lugar, se analizará el Proyecto de Ley que regula el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Esta propuesta, si bien no persigue regular la IA directamente, alude al tratamiento automatizado de datos y aumenta el nivel de protección que reciben sus titulares, de modo que contribuiría a proteger a los consumidores en esta materia [398].

1. Proyecto de ley sobre IA y Robótica (Boletín 15869-19)

El Boletín Nº 15.869-19, que "*regula los sistemas de Inteligencia Artificial, la robótica y las tecnologías conexas en sus distintos ámbitos de aplicación*"[399], es un Proyecto de Ley –actualmente en discusión– que tiene por objeto "*establecer un marco jurídico en lo que respecta al desarrollo, comercialización, distribución y utilización de los sistemas de Inteligencia Artificial, en adelante sistemas de IA, asegurando la protección de los derechos fundamentales garantizados por el Estado de Chile*"[400].

Aunque en nuestro país existen otros Proyectos de Ley que refieren a la IA, lo hacen a propósito de materias específicas que son ajenas al consumo. El Boletín 15869-19 es el único, hasta la fecha, que persigue regular la tecnología de un modo general, por lo que sus disposiciones resultarían aplicables a las relaciones de consumo. A mayor abundamiento,

---

[397] MINISTERIO de Economía, Fomento y Turismo (Chile). Proyecto de ley que mejora la protección de los derechos de las personas consumidoras en el ámbito de sus intereses individuales fortaleciendo al Servicio Nacional del Consumidor, y establece otras modificaciones que indica. Boletín N° 16.271-03. Santiago, Chile, septiembre del 2023.

[398] MINISTERIO Secretaría General de la Presidencia (Chile). Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N° 11.144-07. Santiago, Chile, marzo del 2017.

[399] CÁMARA DE DIPUTADOS (Chile). Proyecto de Ley que Regula los Sistemas de Inteligencia Artificial, la Robótica y las Tecnologías Conexas en sus Distintos Ámbitos de Aplicación. Boletín Nº 15.869-19, refundido con Boletín Nº 16.821-19. Valparaíso, Chile, 24 de abril de 2023.

[400] *Ibíd*., p.2.

dentro de los Considerandos del Boletín se indica que uno de sus objetivos es "*proteger a los consumidores en general y, en particular, el tratamiento de datos personales"*[401].

En términos generales, este Proyecto resulta fuertemente inspirado por la regulación de la Unión Europea sobre la materia[402], "*especialmente en la propuesta de Reglamento de Inteligencia Artificial del Parlamento Europeo (AI ACT), pero de forma extremadamente acotada*"[403], cuyo enfoque –según se examinará en el cuarto Capítulo– está basado en el riesgo.

En efecto, al igual que la AI ACT, el Boletín distingue entre sistemas de IA de riesgo inaceptable (artículo 3º) y sistemas de IA de alto riesgo (artículo 4º). Asimismo, es posible hallar, aunque en forma implícita, el reconocimiento de sistemas de IA de "bajo riesgo", que serían todos aquellos que, a pesar de no encajar con ninguno de los criterios señalados en los artículos 3º y 4º, pueden ser subsumidos dentro de la definición general de sistema de IA.

Según señala el Proyecto, se entiende por sistema de IA:

> "*[E]l software que se desarrolla empleando una o varias de las siguientes técnicas: Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo.*
>
> *b. Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico).*
>
> *c. Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización*"[404].

---

401 *Ibíd*., p.3.
402 *Ibíd*., p.1.
403 ROMERO, Sebastián. *El Desafío Regulatorio de las Nuevas Tecnologías: Análisis del Uso de Datos Personales e Inteligencia Artificial en el Contexto de Campañas Electorales. Una Mirada Nacional y Comparada*. Tesis (Licenciatura en Ciencias Jurídicas y Sociales). Santiago, Chile. Universidad de Chile, Facultad de Derecho, 2023. 69p.
404 CÁMARA DE DIPUTADOS (Chile), op. cit. Artículo 2º.

Luego, teniendo como base dicha definición –que a su vez es idéntica a la de la AI ACT europea–, se efectúa la categorización por riesgo a la que se hizo referencia. Su importancia estriba en que los sistemas de riesgo inaceptable solo pueden ser utilizados por autoridades policiales[405]; mientras que el empleo de los sistemas con riesgos "aceptables", al menos en principio, está disponible para toda la población. A su vez, la diferencia entre los sistemas de IA de alto riesgo y los de bajo riesgo radica en que el uso de los primeros está supeditado al cumplimiento de varios deberes legales de cuidado y transparencia por parte de los operadores, en tanto que los segundos se rigen principalmente por la autorregulación.

La conveniencia o inconveniencia concreta de adoptar un sistema de regulación de IA basado en el riesgo será analizada en detalle en el Capítulo IV, al examinar la AI Act europea. Con todo, en términos generales, resulta positivo que el proyecto identifique que no todos los sistemas de IA poseen el mismo potencial de daño hacia las personas y que tenga en cuenta dicho factor para efectos de determinar los deberes y cuidados legales exigibles. De lo contrario, la regulación podría llevar a ciertos proveedores a asumir costos que, por la funcionalidad concreta de su tecnología, parecen ser excesivos e injustificados.

En cuanto al control obligatorio al que deben quedar sujetos los sistemas de IA de alto riesgo, el Proyecto propone la creación de una Comisión Nacional de Inteligencia Artificial, que, entre otras funciones, se encargará de autorizar previamente el desarrollo, la comercialización, la distribución y la utilización de esta tecnología en el territorio nacional[406]. Para tal efecto, la autoridad administrativa podrá basarse no solo en el riesgo abstracto de la tecnología empleada, sino también en el riesgo real o concreto, puesto que cuenta con la facultad de exigir a los agentes que sometan sus sistemas de IA a pruebas y entreguen bajo confidencialidad los respectivos resultados[407].

Asimismo, el artículo 9º del Proyecto dispone que, si la Comisión determina que un sistema de IA es de alto riesgo, otorgará la autorización de uso únicamente si el agente cuenta con (i) un plan de gestión de riesgos y monitoreo de datos de entrada; (ii) sistemas que permitan controlar la finalidad de la tecnología y su precisión, ciberseguridad y solidez; (iii) la

[405] *Ibíd*. Artículo 3º.
[406] *Ibíd*. Artículos 5 y 6
[407] *Ibíd*. Artículo 7.

posibilidad de generar un registro automático de los procesos; (iv) instrucciones de uso accesibles; y (v) medidas que permitan la vigilancia humana sobre la IA[408].

Por último, el Proyecto aclara que el hecho de emplear una tecnología de menor riesgo, si bien abre cauce a la autorregulación, no supone libertad total. En efecto, el artículo 10 indica que:

> "*Independiente del riesgo, los desarrolladores, proveedores y usuarios de sistemas de IA destinados a interactuar con personas garantizarán que estén diseñados y desarrollados de forma que las personas estén informadas de que están interactuando con un sistema de IA.*
>
> *Igualmente, e independiente del riesgo, los desarrolladores, proveedores y usuarios de sistemas de IA que generen o manipulen contenido de imagen, sonido o video que se asemeje notablemente a personas, objetos, lugares u otras entidades o sucesos existentes, y que pueda inducir erróneamente a una persona a pensar que son auténticos o verídicos, deberán asegurarse que quienes accedan a dicho contenido sepan que ha sido generado de forma artificial o manipulado por un sistema de IA*"[409].

Es difícil negar que todas estas normas podrían contribuir, aunque sea indirectamente, a aumentar el grado de protección del consumidor. Más allá de que el solo hecho de regular la tecnología disminuye la probabilidad de que los proveedores incurran en malas prácticas, el enfoque basado en el riesgo parece ser adecuado y, en términos generales, los criterios que se han adoptado para medir la peligrosidad de un sistema de IA no difieren sustancialmente de los propuestos por la Unión Europea. Asimismo, el control administrativo especializado que se propone ayudaría a aumentar la seguridad y fiabilidad de los sistemas.

Sin perjuicio de lo anterior, los autores de la presente Memoria estiman que el Boletín presenta deficiencias importantes[410]. En primer lugar, la propia definición de sistema IA dificulta que la ley se adecúe a los avances tecnológicos. Al igual que la AI ACT –cuya definición es

[408] *Ibíd*. Artículo 9.
[409] *Ibíd*. Artículo 10.
[410] Las críticas al proyecto se formulan pensando, principalmente, en mejoras que resultan deseables desde el punto de vista de la protección a los consumidores.

idéntica–, se incurre en el error de tratar de detallar los componentes y características de la IA actual, identificándola con ciertos *softwares*.

En lugar de ello, hubiese sido preferible seguir un criterio similar al ofrecido por la *US Algorithmic Accountability Act of* 2022, en donde se omite la "cuestión ontológica" de definir que es un sistema de IA según los conocimientos actuales y simplemente se indica que el objeto de la regulación son los procesos automatizados[411]. Así las cosas, "*resulta extremadamente necesario que el desarrollo legislativo del boletín N° 15869-19 permita que el proyecto en comento se convierta en un cuerpo legal dinámico*"[412].

En segundo lugar, el artículo 5º del Proyecto establece que los miembros de la Comisión Nacional de Inteligencia Artificial "*no recibirán remuneración ni beneficio alguno por su participación*"[413]. Considerando la dificultad de las labores que se les encomienda, podría resultar contraproducente que se desempeñen gratuitamente. Al efecto, no debe olvidarse que la IA es una tecnología en constante desarrollo, de modo que su estudio requiere una dedicación constante, especialmente si se ven amenazados derechos fundamentales de las personas.

En tercer lugar, la normativa propone una regulación que está enfocada casi exclusivamente en el control de la seguridad de la IA. Como se examinó en el Capítulo II de la presente Memoria, los consumidores –y las personas en general– que interactúan con la IA no solo ven amenazada su integridad, sino también su autonomía y su privacidad. En ese sentido, tal como se ha propuesto en la Unión Europea y en Estados Unidos, hubiese sido deseable que se establecieran deberes de transparencia o auditoría algorítmica.

La única referencia a la transparencia se encuentra en el artículo 10, en cuanto se indica que los sistemas de IA deben diseñarse de manera tal que las personas puedan tener

411 MÖKANDER, J., JUNEJA, P., WATSON, D.S. y FLORIDI, L., 2022. *The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other?* [en línea] Minds and Machines, Agosto-2022, Vol. 32, n°. 4 <https://link.springer.com/article/10.1007/s11023-022-09612-y> [consulta: 18 octubre 2023]. p. 753. Se volverá sobre este tema en el Capítulo IV, al momento de examinar los estándares para Chile.
412 ROMERO, Sebastián. *El Desafío Regulatorio de las Nuevas Tecnologías: Análisis del Uso de Datos Personales e Inteligencia Artificial en el Contexto de Campañas Electorales. Una Mirada Nacional y Comparada*. Tesis (Licenciatura en Ciencias Jurídicas y Sociales). Santiago, Chile. Universidad de Chile, Facultad de Derecho, 2023. 72p.
413 CÁMARA DE DIPUTADOS (Chile), op. cit. Artículo 5.

conocimiento respecto de la circunstancia de estar interactuando con un sistema de IA[414]. Pero nada se dice, por ejemplo, respecto del deber de información sobre los procedimientos o las finalidades empleadas.

Por lo demás, aun cuando la protección de la integridad de las personas pareciera ser el principal enfoque, lo cierto es que dicho derecho tampoco queda totalmente garantizado, ya que el Proyecto no contiene norma alguna sobre la responsabilidad civil del agente que emplea sistemas de IA.

Siendo justos, es entendible que así haya ocurrido, considerando que la principal inspiración fue la AI ACT de la Unión Europea, y dicha normativa tampoco aborda la problemática. Empero, la diferencia es que en el caso europeo existen otras Directivas que buscan adecuar las reglas de la responsabilidad civil a la IA, como, por ejemplo, la Propuesta de Directiva 2022/0302 sobre responsabilidad por productos defectuosos[415] o la Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial[416]. En cambio, según se analizó en el Capítulo II –y también anteriormente en este Capítulo–, en Chile no existe adecuación legal alguna al régimen de responsabilidad, por lo que la omisión, aun cuando sea entendible, no se justifica.

En cuarto lugar, la propuesta pareciera ignorar el carácter transfronterizo de la IA, por cuanto sus reglas poseen únicamente aplicación local. Según se explicó en el Capítulo II, el problema de ello es que un consumidor nacional podría verse obligado a probar derecho extranjero, cuando se vea afectado por una IA cuyo proceso de fabricación, distribución y/o comercialización involucra a agentes radicados fuera del país.

La aplicación de la ley en el espacio no puede hacer caso omiso a estas problemáticas, máxime si lo que está en juego es la indemnidad de los consumidores. De ahí que las reglas del Derecho Internacional Privado cobren especial relevancia para conseguir una adecuada regulación de las nuevas tecnologías.

---

[414] *Ibíd*. Artículo 10.

[415] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos. Bruselas, Bélgica, 2022.

[416] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022.

En quinto lugar y último lugar, llama la atención el artículo final del Boletín, que dispone que: "*El desarrollo, distribución, comercialización o uso de sistemas de IA de riesgo inaceptable serán sancionados con presidio mayor en su grado mínimo*"[417]. Naturalmente, surge la pregunta de qué tan disuasivo o efectivo es el establecimiento de una sanción penal en circunstancias que el empleo de estas tecnologías suele llevarse a cabo por personas jurídicas. Si bien la LPDC no excluye la posibilidad de que los proveedores sean personas naturales, lo habitual es que quien desarrolla, distribuye o comercializa productos lo haga bajo una forma societaria.

2. Proyecto de ley "SERNAC te protege" (Boletín 16271-03)

El Boletín 16271-03, que "*Mejora la protección de los derechos de las personas consumidoras en el ámbito de sus intereses individuales fortaleciendo al Servicio Nacional del Consumidor, y establece otras modificaciones que indica*" (más conocido como "SERNAC Te Protege"), es un Proyecto de Ley recientemente impulsado que persigue ampliar las potestades sancionatorias del SERNAC; modernizar el procedimiento administrativo de reclamo por infracciones a la LPDC; asegurar que las empresas cuenten con canales de atención de reclamos; consagrar un sistema de incentivos que ayude a prevenir infracciones y sanciones; fortalecer a las asociaciones de consumidores; establecer la responsabilidad de las plataformas intermediarias; y, en general, ampliar el grado de protección efectivo de los consumidores[418].

Si bien el grueso de la reforma se concentra en fortalecer al SERNAC, y ni el mensaje ni el articulado del Proyecto hacen referencia alguna a la IA, existen algunas modificaciones y/o nuevas disposiciones que, de ser introducidas a nuestro ordenamiento, podrían resultar relevantes para resguardar los derechos de los consumidores ante el uso de IA por parte de los proveedores. Considerando que la calidad del Proyecto hace esperable que en un futuro sea aprobado –aunque sea con modificaciones–, se ha estimado conveniente destinar un apartado al análisis de dichas normas.

---

[417] CÁMARA DE DIPUTADOS (Chile), op. cit. Artículo 15.

[418] MINISTERIO de Economía, Fomento y Turismo (Chile). Proyecto de ley que mejora la protección de los derechos de las personas consumidoras en el ámbito de sus intereses individuales fortaleciendo al Servicio Nacional del Consumidor, y establece otras modificaciones que indica. Boletín N° 16.271-03. Santiago, Chile, septiembre del 2023. pp. 9-10. Véase también: https://www.sernac.cl/portal/604/w3-propertyname-788.html.

Una primera propuesta de modificación relevante es la realizada al artículo 1 Nº1, que es el precepto que precisa qué se entiende por consumidor[419]. La reforma plantea eliminar la expresión "en virtud de cualquier acto jurídico oneroso" de la definición, de manera de ampliar la protección a aquellos clientes potenciales que interactúan con el proveedor[420]. La importancia de ello en relación con el objeto de estudio estriba en que, actualmente, hay personas que interactúan con plataformas de IA proporcionadas por el proveedor y, a pesar de no comprar nada, pueden resultar vulneradas en sus derechos, en cuyo caso, siguiendo el texto legal actual, no resulta claro que queden amparados por la LPDC.

No obstante, en verdad la reforma no hace más que reconocer algo que ya está bastante asentado en la dogmática nacional. En efecto, la doctrina mayoritaria entiende que dicha expresión ya no constituye un requisito para adquirir la calidad de consumidor[421]. Asimismo, se ha sostenido que, incluso si no se entendiese suprimida dicha expresión, la situación en que el cliente interactúa con plataformas de IA y comparte sus datos personales sin adquirir ningún bien o servicio, ya queda cubierta por la definición actual, por cuanto el hecho de brindar acceso a datos personales posee un valor económico para los proveedores, lo que impide catalogar como gratuito el acto[422].

Ahora bien, sin perjuicio de que los autores de esta Memoria adscriben a dichos planteamientos, no puede negarse que la supresión legal del requisito brinda una mayor certeza jurídica. El hecho de elevar a rango legal esta postura no deja lugar a dudas incluso para quienes se han mostrado reacios a extender el régimen.

Una segunda propuesta de modificación relevante es la introducción de un nuevo inciso cuarto al artículo 12 LPDC, que indica que:

---

419 *Ibíd.*

420 *Ibíd.*, pp. 31 y 34.

421 Véase, por todos: ISLER, Erika. P*lataformas digitales y relación de consumo en Chile: un desafío actual*. En su: *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. 1ºed. Chile, Rubicón Editores, 2023. 193p.

422 MOMBERG URIBE, Rodrigo; MORALES ORTIZ, Maria Elisa. 2019. *Las cláusulas relativas al uso y tratamiento de datos personales y el artículo 16 letra g) de la Ley 19.496 sobre Protección de los Derechos de los Consumidores*. Revista chilena de derecho y tecnología 8(2): 157-180. pp. 176.

"*El proveedor deberá mantener canales expeditos para la recepción, registro, respuesta, y reporte de reclamos, al menos equivalentes a aquellos disponibles para la oferta y comercialización de bienes y servicios, y no podrá condicionar su recepción al pago del monto reclamado. Para estos efectos, se entenderá por reclamo toda presentación escrita formulada por un consumidor ante el proveedor para dar cuenta de una situación concreta relacionada con el ejercicio de sus derechos*"[423].

El solo hecho de imponer al proveedor la obligación de mantener canales que permitan gestionar reclamos rápidamente en todas las fases del vínculo de consumo es algo destacable. Pero la razón por la que se menciona la norma en este apartado es por el rol que podrían cumplir los sistemas de IA para estos efectos. La capacidad de manejo de datos de la IA permite recibir reclamos, categorizarlos, sistematizarlos y tramitarlos en forma rápida y sencilla[424]. Considerando la potencialidad de la tecnología, esta norma podría ser un incentivo para que los proveedores la aprovechen eficientemente.

Un tercer aspecto importante es la introducción de los nuevos incisos primero, segundo y tercero al artículo 15, que pasan a anteceder a los incisos actuales -sin reemplazarlos-. La propuesta indica:

"*Los proveedores deberán garantizar en la prestación de bienes y servicios, una atención y trato digno, respetuoso, y no discriminatorio.*

En el caso de consumidores que sean parte de grupos de especial protección, el proveedor deberá adoptar todas las medidas adecuadas o ajustes necesarios para evitar que dicha situación signifique un menoscabo o vulneración en la atención y trato que se les otorga.

Los proveedores deberán abstenerse de realizar conductas ofensivas, denigrantes o intimidatorias respecto de los consumidores"[425].

---

[423] MINISTERIO de Economía, Fomento y Turismo (Chile). Proyecto de ley que mejora la protección de los derechos de las personas consumidoras en el ámbito de sus intereses individuales fortaleciendo al Servicio Nacional del Consumidor, y establece otras modificaciones que indica. Boletín N° 16.271-03. Santiago, Chile, septiembre del 2023, p. 36.

[424] ZTZ. TECH GROUP. *5 beneficios clave de incorporar la Inteligencia Artificial en la gestión de reclamos.* [en línea] <https://ztz.ai/5-beneficios-clave-de-incorporar-la-inteligencia-artificial-en-la-gestion-de-reclamos/> [consulta: 10 septiembre 2023].

[425] MINISTERIO de Economía, Fomento y Turismo (Chile). Proyecto de ley que mejora la protección de los derechos de las personas consumidoras en el ámbito de sus intereses individuales fortaleciendo al Servicio

La incorporación de estos incisos se traduciría en un mayor resguardo para los consumidores ante la posibilidad de que la IA efectúe discriminaciones arbitrarias, pues se obliga al proveedor a resguardar que los consumidores reciban un trato adecuado. Adicionalmente, el nuevo inciso segundo, al utilizar la expresión "grupos de especial protección", no solo evoca la idea de grupos históricamente discriminados, sino también la de consumidores hipervulnerables[426].

Son consumidores hipervulnerables quienes, por razones endógenas, circunstanciales, situacionales o culturales, poseen una capa de vulnerabilidad adicional a aquella que es estructural o inherente a su calidad de consumidor, y, en consecuencia, enfrentan una mayor exposición al riesgo de vulneración de sus derechos[427].

Dentro de aquellos consumidores que por razones circunstanciales pueden calificarse como hipervulnerables, encontramos al consumidor electrónico. Se estima que este consumidor posee una capa adicional de vulnerabilidad puesto que, al verse en la obligación de interactuar con nuevas tecnologías, no solo enfrenta asimetrías informativas intensas, sino también asimetrías técnicas que dificultad su decisión de consumo[428].

Una vez que se concibe al consumidor electrónico como un consumidor hipervulnerable, resulta aplicable el deber especial de cuidado y trato digno que consagra el nuevo inciso segundo del artículo 15 LPDC, así como los deberes de profesionalidad e información en sus versiones más intensificadas[429]. De este modo, existiría un resguardo alto en orden a evitar que, como consecuencia de la interacción con sistemas de IA, el consumidor electrónico sufra menoscabos o discriminaciones.

Nacional del Consumidor, y establece otras modificaciones que indica. Boletín N° 16.271-03. Santiago, Chile, septiembre del 2023, p. 37.

[426] *Ibíd.*, pp. 29-30.

[427] Definición construida en base a: CHILE. Resolución Exenta N° 001038 del Servicio Nacional del Consumidor, que Aprueba Circular Interpretativa sobre noción de consumidor hipervulnerable, 31 de diciembre de 2021; y, LÓPEZ Díaz, Patricia. *El consumidor hipervulnerable como débil jurídico en el derecho chileno: una taxonomía y alcance de la tutela aplicable*. Latin american legal studies, 10(2): 2022, p. 382.

[428] LÓPEZ Díaz, Patricia. *El consumidor hipervulnerable como débil jurídico en el derecho chileno: una taxonomía y alcance de la tutela aplicable*. Latin american legal studies, 10(2): 2022, p. 402.

[429] SERVICIO Nacional del Consumidor (Chile). Resolución Exenta N° 1038 Aprueba Circular Interpretativa sobre noción de consumidor hipervulnerable, Santiago, Chile, 31 de diciembre de 2021, pp. 24-25.

Un cuarto aspecto interesante del Proyecto, y probablemente aquel que resulta más innovador y atingente para estos efectos, es el nuevo artículo 43 de la LPDC, que viene a sustituir el texto actual[430]. El precepto propuesto dispone que: "*El proveedor que actúe como intermediario en la comercialización de bienes o servicios responderá directamente frente al consumidor por el incumplimiento de las obligaciones contractuales, sin perjuicio de su derecho a repetir contra los que resulten responsables*"[431].

El artículo 43 actual permite al consumidor perseguir la responsabilidad del proveedor que actúe como intermediario en la prestación de servicios. El texto propuesto, en cambio, habilita a perseguir la responsabilidad del proveedor que actúa como intermediario en la comercialización de bienes o servicios.

Al reemplazar la palabra "prestación" por "comercialización" e incluir también a los bienes, se busca extender la responsabilidad a aquellas plataformas online de IA que los proveedores utilizan como ayuda en sus procesos de comercialización, vale decir, las páginas web, softwares o tecnologías automatizadas con las que el consumidor interactúa directamente[432]. Con todo, el artículo propuesto no suprime la expresión "*por el incumplimiento de las obligaciones contractuales*", por lo que solo se podría hacer responsable al proveedor intermediario en la medida en que exista un contrato de por medio y este se encuentre incumplido.

Un último aspecto interesante del Proyecto es la dictación del artículo 50 G-30, que consagra un principio de cooperación administrativa entre el SERNAC y otras autoridades sectoriales[433]. En lo que atañe a la utilización de IA, este precepto podría ser especialmente

---

[430] El texto actual del artículo 43 LPDC indica: "*El proveedor que actúe como intermediario en la prestación de un servicio responderá directamente frente al consumidor por el incumplimiento de las obligaciones contractuales, sin perjuicio de su derecho a repetir contra el prestador de los servicios o terceros que resulten responsables*". DFL 3. CHILE. Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021. Artículo 1 Nº3.

[431] MINISTERIO de Economía, Fomento y Turismo (Chile). Proyecto de ley que mejora la protección de los derechos de las personas consumidoras en el ámbito de sus intereses individuales fortaleciendo al Servicio Nacional del Consumidor, y establece otras modificaciones que indica. Boletín N° 16.271-03. Santiago, Chile, septiembre del 2023, p. 40.

[432] *Ibíd.*, pp. 27-28.

[433] El precepto indica: "*Artículo 50 G-30.- Si el Servicio llegara a tomar conocimiento de hechos que únicamente pudieran constituir una infracción de disposiciones legales o reglamentarias distintas a las contenidas en esta ley, relacionadas con la protección de los derechos de los consumidores, procederá a denunciar los posibles incumplimientos ante los organismos sectoriales o instancias jurisdiccionales respectivas. Por su parte, si un*

relevante si es que se aprueba el Proyecto de Ley sobre Datos Personales que crea la Agencia de Protección de Datos Personales, pues en tal caso el SERNAC estaría legalmente obligado a mantener una comunicación fluida con dicho ente, lo que redundaría en una protección más completa y especializada para los consumidores.

3. Proyecto de ley sobre el tratamiento de datos personales

El Proyecto de Ley que regula el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, que refunde los Boletines 11.092-07[434] y 11.144-07[435] [436], es una iniciativa legislativa que busca perfeccionar las normas relativas a los datos personales, la cual, entre otras cosas, recoge las recomendaciones de la Organización para la Cooperación y el Desarrollo Económico (En adelante "**OCDE**") respecto de los principios y contenidos básicos que deben recoger las normativas internas de los países miembros para asegurar el respeto a la privacidad y la protección de los datos personales.

Según señala el Boletín 11.144-07,

> *"Este proyecto de ley tiene como objetivo general actualizar y modernizar el marco normativo e institucional con el propósito de establecer que el tratamiento de los datos personales de las personas naturales se realice con el consentimiento del titular de datos o en los casos que autorice la ley, reforzando la idea de que los datos personales deben estar bajo la esfera de control de su titular, favoreciendo su protección frente a toda intromisión de terceros y estableciendo las condiciones regulatorias bajo las cuales los terceros pueden efectuar legítimamente el tratamiento de tales datos, asegurando estándares de calidad, información, transparencia y seguridad"*[437].

organismo sectorial llegara a tomar conocimiento de hechos que pudieran constituir una infracción a disposiciones contenidas en la presente ley, deberá denunciar dicha circunstancia al Servicio".

[434] MINISTERIO Secretaría General de la Presidencia (Chile). Proyecto de ley sobre Protección de Datos Personales. Boletín N° 11.092-07. Santiago, Chile, enero del 2017.

[435] MINISTERIO Secretaría General de la Presidencia (Chile). Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N° 11.144-07. Santiago, Chile, marzo del 2017.

[436] CÁMARA DE DIPUTADAS Y DIPUTADOS. *Tratamiento de datos personales tendrá nuevo marco legal*. [en línea] 08 de mayo 2023 <https://www.camara.cl/cms/noticias/2023/05/08/tratamiento-de-datos-personales-tendra-nuevo-marco-legal/> [consulta: 15 de octubre 2023].

[437] MINISTERIO Secretaría General de la Presidencia (Chile). Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N° 11.144-07. Santiago, Chile, marzo del 2017.

Para ello, establece una serie de obligaciones para las empresas y organizaciones que manejan datos personales, tales como obtener el consentimiento explícito de los titulares de los datos, informar sobre el uso que se dará a los datos, garantizar la seguridad de los datos y permitir el acceso y rectificación de los mismos por parte de los titulares. Adicionalmente, crea la Agencia de Protección de Datos Personales, la cual tiene como objetivo supervisar y fiscalizar el cumplimiento de las obligaciones que se consagran y, además, sancionar a las empresas y organizaciones que no cumplan con la ley.

En cuanto al contenido del proyecto, el Boletín 11.144-07 señala que "*el ámbito de aplicación de la ley es todo tratamiento de datos personales que realicen las personas naturales o jurídicas, incluidos los órganos públicos, que no se encuentre regido por una ley especial*"[438]. Además, establece el carácter supletorio de esta normativa para todos aquellos tratamientos de datos regulados en leyes especiales y excluye de manera expresa de este régimen regulatorio "*al tratamiento de datos personales que se realice en el ejercicio de las libertades de emitir opinión y de informar regulado por las leyes especiales (...) y el tratamiento que efectúen las personas naturales en relación con sus actividades personales*"[439].

Además, incorpora un conjunto de principios rectores en materia de protección y tratamiento de los datos personales que han sido reconocidos en las directrices de la OCDE y en la legislación comparada, que son: licitud del tratamiento, finalidad, proporcionalidad, calidad, seguridad, responsabilidad e información. Asimismo, en el tratamiento de datos personales por parte de los organismos públicos se incorporan además los principios de coordinación, eficiencia, transparencia y publicidad[440].

Adicionalmente, busca reforzar y ampliar los derechos de los titulares de datos, para lo cual reconoce expresamente los derechos de acceso, rectificación, cancelación, oposición y portabilidad de los datos personales, denominados "derechos ARCO" y, con el objeto de asegurar un ejercicio eficaz de tales derechos, establece un procedimiento, según señala, "directo y eficaz" para que cualquier titular de datos pueda recurrir directamente ante el responsable de datos.

---

438 *Ibíd*., p.5.
439 *Ibíd*.
440 *Ibíd*., p.6.

En relación al derecho de oposición, el Proyecto otorga al titular de datos personales, mediante el artículo 8, el derecho a oponerse y a no ser objeto de decisiones basadas en el tratamiento automatizado de sus datos personales que produzca efectos jurídicos en él o le afecte significativamente, salvo en cuando la decisión sea necesaria para la celebración o ejecución de un contrato entre el titular y el responsable, exista consentimiento previo y expreso del titular o lo señale la ley.

Lo anterior, sin perjuicio del deber del responsable de adoptar las medidas necesarias para asegurar los derechos, libertades del titular, su derecho a la información y transparencia, el derecho a obtener una explicación, la intervención humana, a expresar su punto de vista y a solicitar la revisión de la decisión[441].

Adicionalmente, el Proyecto innova por completo al introducir a nuestro ordenamiento jurídico el derecho a la portabilidad de los datos personales, en tanto aquel no se encuentra contemplado en la Ley actual. En virtud de aquel derecho, el titular de datos puede solicitar y obtener del responsable en un formato electrónico estructurado, genérico y de uso habitual, una copia de sus datos personales y comunicarlos o transferirlos a otro responsable de datos[442] y, además, en ejercicio de este derecho, tendría la facultad de requerir que sus datos personales se transmitan directamente de responsable a responsable de datos cuando sea técnicamente posible[443].

Por lo demás, el Proyecto establece el consentimiento como la fuente principal de legitimidad del tratamiento de los datos personales, el que debe ser -según indica- libre, informado, inequívoco, otorgado en forma previa al tratamiento y específico en cuanto a su finalidad o finalidades. Lo anterior, por supuesto, sin hacer mención a las excepciones, las cuales parecen ser, en abstracto, bastante amplias, en tanto se señala al respecto:

---

[441] CÁMARA DE DIPUTADOS (CHILE). *Oficio Nº 18.347 mediante el cual la Cámara de Diputados dio su aprobación al Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*, de 08 de mayo de 2023. p.12.

[442] MINISTERIO Secretaría General de la Presidencia (Chile). Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N° 11.144-07. Santiago, Chile, marzo del 2017, p.7.

[443] EY. Proyecto de ley de datos personales: ¡Qué se viene para este año 2023? [en línea] 18 de enero 2023 <https://www.ey.com/es_cl/tax/ey-tax-alert-chile/proyecto-de-ley-de-datos-personales-que-se-viene-para-este-anio-2023> [consulta: 18 de octubre 2023].

"Se consideran excepciones a las regla del consentimiento, tales como cuando la información ha sido recolectada de una fuente de acceso público; cuando sean datos relativos a obligaciones de carácter económico, financiero, bancario o comercial; o cuando el tratamiento sea necesario para la ejecución o el cumplimiento de una obligación legal o de un contrato en que es parte el titular"[444].

Además, configura un nuevo y renovado régimen de responsabilidades de los responsables de datos, estableciendo una serie de obligaciones y deberes, tales como acreditar la licitud del tratamiento que realizan, deberes de información y deberes de reserva y confidencialidad, de información y transparencia, entre otros.

Por otra parte, regula la cesión o transferencia de las bases de datos personales que disponga o administre el responsable de datos, así como el régimen del tratamiento que efectúa un tercero o mandatario en representación o por encargo del responsable y, también, regula el tratamiento automatizado de grandes volúmenes de datos.

Por lo demás, mediante este Proyecto de ley se busca elevar el estándar para el tratamiento de los datos sensibles, estableciendo que sólo puede realizarse cuando el titular consienta libre e informadamente, en forma expresa, salvo ciertas excepciones, las cuales son contempladas de forma expresa.

También, incorpora una regulación específica para la transferencia internacional de datos personales, ajustándola a los estándares y recomendaciones de la OCDE, para lo cual modifica los actuales artículos 27, 28 y 29 de la LPVP.

Adicionalmente, el Proyecto contempla, por fin, una de las innovaciones más esperadas: la creación de una autoridad de control, denominada "Agencia de Protección de Datos Personales", que tiene por objeto –principalmente– "*velar por la protección de los derechos y libertades de las personas titulares de datos y por el adecuado cumplimiento de*

[444] MINISTERIO Secretaría General de la Presidencia (Chile). Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N° 11.144-07. Santiago, Chile, marzo del 2017, p.7.

las normas relativas al tratamiento de los datos"[445], para lo cual introduce tres títulos nuevos a la actual LPVP.

Al respecto, cabe destacar que en el Proyecto el legislador establece, en el artículo 15 ter, una nueva obligación para los responsables de tratamiento de datos, conforme a la cual deberán realizar, previo al inicio de las operaciones del tratamiento, una evaluación del impacto en protección de datos personales, cuando sea probable que un tipo de tratamiento, por su naturaleza, alcance, contexto, tecnología utilizada o fines, se pueda producir un alto riesgo para los derechos de las personas titulares de los datos personales[446]. En este ámbito, la Agencia de Protección de Datos cobra especial importancia en tanto órgano de orientación y también consultivo, en tanto:

> *"*[E]*stablecerá y publicará una lista orientativa de los tipos de operaciones de tratamiento que requieran o no una evaluación de impacto relativa a la protección de datos personales. La Agencia también establecerá las orientaciones mínimas para realizar esta evaluación, considerando a lo menos en dichos criterios, la descripción de las operaciones de tratamiento, su finalidad, la evaluación de la necesidad y la proporcionalidad con respecto a su finalidad, la evaluación de los riesgos y medidas de mitigación.*
>
> *Los responsables podrán consultar a la Agencia de Protección de Datos, cuando en virtud del resultado de la evaluación, el tratamiento demuestre ser de alto riesgo a efectos de obtener recomendaciones de parte de dicha entidad.".*

Finalmente, el Proyecto contempla un catálogo específico de infracciones a los principios y obligaciones establecidos en la ley y establece sanciones correlativas a la gravedad de la infracción que van desde la amonestación escrita a multas que oscilan entre 1 y 5.000 UTM.

Así las cosas, como es posible observar, el Proyecto de Ley viene a elevar el estándar actual en la materia de tratamiento de datos personales, teniendo especialmente a la vista

---

[445] *Ibíd.*, p.10.

[446] CÁMARA DE DIPUTADOS (CHILE). *Oficio Nº 18.347 mediante el cual la Cámara de Diputados dio su aprobación al Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*, de 08 de mayo de 2023. p.20.

legislación extranjera y los compromisos internacionales que ha adquirido el país durante los más de 20 años que ha estado la actual Ley de Protección de Datos Personales en Vigencia.

Lo anterior afectará sustancialmente las relaciones de consumo, en tanto implica más derechos para los titulares de datos personales, lo cual conlleva, a su vez, más deberes y obligaciones para los responsables del tratamiento de datos personales, en este caso, los proveedores, quienes deberán adaptar sus prácticas a la nueva normativa. Así, por ejemplo, surgirá la obligación legal implementar medidas técnicas y organizativas para garantizar la seguridad, confidencialidad, integridad, disponibilidad y resiliencia de los datos.

IV. Aspectos positivos y desafíos pendientes

Una aproximación inicial a la normativa de consumo vigente en nuestro país podría llevar a pensar que los consumidores no se encuentran protegidos respecto del uso de IA, por cuanto la LPDC no ha sido reformada en ese sentido y lo único que existe son Circulares de carácter no vinculante.

Empero, luego de haber realizado un estudio acabado de toda la legislación pertinente, no cabe sino concluir que hay varios riesgos que, no obstante la ausencia de reformas, pueden ser abordados en forma relativamente satisfactoria. Así, por ejemplo, al interpretar los deberes de transparencia y profesionalidad previstos en la LPDC, se aprecia que los proveedores que emplean IA deben informar los aspectos esenciales sobre el funcionamiento de la tecnología, así como observar una alta diligencia en su utilización y en el tratamiento de datos personales. Más aún, puede afirmarse que la transparencia algorítmica constituye un comportamiento exigible para los proveedores.

Adicionalmente, a partir de la noción de buena fe objetiva desarrollada por la doctrina, es posible sostener que el control de cláusulas abusivas deriva en la anulación de aquellas estipulaciones que no respeten los principios éticos que inspiran el uso de la IA, aun cuando no se encuentren positivados en nuestro ordenamiento.

Por último, el tratamiento de los datos personales de los consumidores está sujeto a los principios de consentimiento, finalidad, calidad, seguridad y respeto de los derechos ARCO,

lo que sugiere que el proveedor no cometerá vulneraciones indebidas a la privacidad de los consumidores. Si se tienen en cuenta los criterios expuestos en la Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores, todo ello iría acompañado de un deber de transparencia. Por lo demás, se espera que esta regulación sea mejorada una vez aprobado el Proyecto de Ley sobre el tratamiento de datos personales.

Ahora bien, aún existen bastantes desafíos que no logran ser cubiertos en forma satisfactoria por la normativa actual y propuesta, o bien, que derechamente resultan ignorados. El ejemplo más ilustrativo de ello dice relación con la responsabilidad civil derivada por los daños cometidos por la IA.

En el Capítulo II se explicó que existen dificultades para identificar a quién demandar y probar la causalidad. Además, al ser la IA una tecnología transfronteriza, es probable que el consumidor deba probar derecho extranjero para defender sus intereses. No obstante dichas circunstancias, en el presente Capítulo nada se dijo respecto del problema. Sería un agrado decir que fue una omisión, pero no es el caso. Es simplemente porque no existe norma ni herramienta que permita hacerse cargo del problema, aunque sea someramente.

Por otro lado, es menester que la normativa vigente en torno al tratamiento de datos personales sea actualizada atendiendo al desarrollo de la tecnología. Para ello, debe tenerse especialmente en cuenta las implicancias del *big data*, el *machine learning*, el comercio electrónico y las plataformas en el tratamiento masivo de datos, en el sentido de regular las posibilidades de actuación de los proveedores respecto de los datos personales de sus consumidores que recopilan, tratan y distribuyen a terceros.

En concreto, debe estrecharse de manera significativa lo que se entiende por “fuente accesible al público”, ya que, al ser –en la práctica– la regla general, se termina convirtiendo el consentimiento de los consumidores en el régimen de excepción en cuanto a fuente de licitud del trato de datos personales. Ello resulta aún más grave si se tiene en cuenta que, mientras no se apruebe el Proyecto de Ley sobre datos personales, no existe autoridad especializada en materia de datos personales.

Por su parte, en cuanto a la transparencia, si bien la transparencia algorítmica es exigible en nuestro ordenamiento, y es claro que esta debe moldearse en conformidad con el deber de profesionalidad del proveedor, puede que el proveedor simplemente no esté en condiciones de explicar sistemas de IA complejos. Además, a falta de norma que lo regule, es difícil dilucidar cuál es el nivel de transparencia propio de un proveedor profesional y no queda claro si los deberes de información aplican cuando la IA no sea un componente propio del bien o servicio comercializado. Lo ideal sería lograr un equilibrio entre el derecho a la transparencia de los consumidores y la protección de información sensible de las empresas.

En cualquier caso, es difícil sostener que dicha transparencia pueda ser extendida a un deber general de someterse a auditorías algorítmicas. En tal sentido, es necesario que dicho mecanismo sea reconocido expresamente, con el fin de disminuir y, en lo posible, erradicar los sesgos algorítmicos. Si bien exigir a todos los proveedores someterse a auditorías puede ser costoso y contraproducente, sería razonable que se reconozca esta herramienta y se permita su aplicación en forma proporcional, por ejemplo, atendiendo al tamaño del proveedor y/o al riesgo asociado a la tecnología empleada.

En fin, aun cuando el deber de profesionalidad sugiera que los proveedores han de observar una alta diligencia y respetar los principios éticos en el empleo de la IA, es difícil saber en qué deberes concretos de conducta positiva se traduce aquello. Por tanto, queda pendiente establecer otros deberes de control en el uso de la IA que sean ilustrativos sobre qué debe hacer exactamente un proveedor profesional en esta materia.

En suma, los desafíos identificados pueden ser agrupados, respectivamente, en las siguientes categorías: (i) responsabilidad civil de la IA; (ii) perfección del tratamiento de datos personales; (iii) precisión de los deberes de transparencia y de sus límites; (iv) posibilidad de auditoría algorítmica; (v) precisión de otra clase de controles que los proveedores profesionales deban observar al emplear la IA.

CAPÍTULO IV. HACIA UNA NUEVA REGULACIÓN

Como se indicó en la Introducción, la presente Memoria partió de la hipótesis de que la incorporación de IA en las relaciones de consumo debe ser admitida y potenciada en la medida en que se regulen adecuadamente sus riesgos. Hasta el momento, el camino adoptado para comprobar dicho planteamiento ha consistido en, en primer lugar, brindar un marco teórico de la IA y la evolución de las relaciones de consumo; en segundo lugar, analizar los beneficios y riesgos de esta tecnología para los derechos de los consumidores, esbozando las soluciones generales que admiten los problemas identificados; y, en tercer lugar, examinar en qué medida la normativa chilena posibilita –o eventualmente posibilitará– hacer frente a tales desafíos.

El Capítulo anterior finalizó indicando que, a pesar de que la normativa chilena permite abordar adecuadamente algunos aspectos de la IA en las relaciones de consumo, aún existen bastantes riesgos que a falta de regulación especial no pueden ser cubiertos. En tal sentido, este último Capítulo pretende estudiar y analizar el alcance de ciertos estándares sobre la materia desarrollados en la Unión Europea y en Estados Unidos –a nivel federal–[447], a fin de determinar cómo estas normativas pueden dar respuesta a los desafíos que en nuestro medio todavía se encuentran pendientes y evaluar si ello resulta suficiente para mitigar o disminuir significativamente los riesgos hacia los derechos de los consumidores. Además, se formularán una serie de propuestas concretas cuya implementación, a juicio de los autores, podría contribuir sustancialmente a mejorar el estado de la materia en cuestión.

I. Estándares Internacionales de la Unión Europea y Estados Unidos

En este apartado se analizarán diversas normativas pertinentes de la Unión Europea y de Estados Unidos, tanto aquellas ya consagradas como aquellas propuestas que pueda resultar de utilidad tener a la vista. Con todo, se advierte desde ya al lector que estas normativas serán examinadas solo en cuanto puedan interesar a la resolución de los desafíos que se identificaron como pendientes al finalizar el Capítulo anterior. No se pretende hacer una reproducción completa de cada uno de los preceptos que contienen los instrumentos.

[447] Se previene que la normativa analizada será la federal, de modo que no se ahondará en la forma concreta en que cada uno de los 50 Estados que componen EEUU ha planteado o consagrado sus propias directrices; sin perjuicio de que, respecto de ciertas materias en particular, pueda exponerse la regulación de cierto Estado a modo meramente ilustrativo.

Asimismo, el análisis se dividirá por estándar y no por instrumento. Vale decir, en lugar de examinar cada normativa en forma aislada, se crearán apartados que permiten agrupar los problemas individualizados al finalizar el Capítulo anterior, y, en ellos, se mencionarán y explicarán conjuntamente todas las disposiciones o directrices (según sea el caso) europeas y norteamericanas que consagran estándares sobre los problemas en cuestión, identificando el instrumento normativo al que pertenecen.

Así, por ejemplo, habrá un apartado en el que se estudiarán los estándares relacionados con la transparencia de la IA, y en él se recogerán conjuntamente preceptos de diversas normativas estadounidense y europea que tratan la materia. Se ha optado por dicha metodología porque permite entender en forma más sistemática la regulación y, al mismo tiempo, efectuar un contraste específico entre la forma en que Europa y Estados Unidos han abordado los problemas.

1. Responsabilidad Civil de la IA

En el Capítulo II, al momento de examinar el fenómeno de la responsabilidad difusa, se identificaron cuatro problemas que, en nuestro ordenamiento, dificultan al consumidor perseguir la responsabilidad civil por los daños que le ocasionen los sistemas de IA: (i) la necesidad de identificar al presunto agente causante del daño; (ii) la incertidumbre sobre el alcance de la responsabilidad de los proveedores intermediarios; (iii) el carácter transfronterizo de esta tecnología, que puede derivar en la aplicación de derecho extranjero; y (iv) la prueba del vínculo de causalidad entre el hecho dañoso y el daño.

A continuación, se examinarán diversas disposiciones propuestas o consagradas en la Unión Europea y en Estados Unidos que permiten hacer frente a cada uno de dichos problemas. La respuesta normativa a cada problema será analizada por separado, a fin de proporcionar una aproximación más específica sobre el enfoque regulatorio adoptado.

a. Identificación del agente

Unión Europea

En cuanto a la identificación del agente responsable, resulta interesante tener a la vista la Resolución del Parlamento Europeo, de 20 de octubre de 2020, que recoge una "Propuesta de Reglamento relativo a la responsabilidad civil por el funcionamiento de sistemas de inteligencia artificial"[448]. En él se establece que puede hacerse responsable por los daños ocasionados por la IA tanto al "operador inicial" como al "operador final".

El operador inicial corresponde a "*toda persona física o jurídica que define, de forma continuada, las características de la tecnología y proporciona datos y un servicio de apoyo final de base esencial y, por tanto, ejerce también grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA*"[449]; mientras que el operador final es "*toda persona física o jurídica que ejerce un grado de control sobre un riesgo asociado a la operación y el funcionamiento del sistema de IA y se beneficia de su funcionamiento"*[450]*.*

En otras palabras, puede ser responsable tanto quien crea el sistema de IA (operador inicial) como quien se beneficia de su funcionamiento y, en los hechos, lo controla (operador final o proveedor)[451]. Asimismo, el artículo 11 de la Propuesta de Reglamento establece que esta responsabilidad es de carácter solidario[452]. En principio puede extrañar que ambos operadores respondan en los mismos términos. No obstante, ello se debe a que, aunque el operador inicial suele tener una mayor incidencia en los riesgos operativos, el operador final "*ejerce un grado de control sobre un riesgo asociado al funcionamiento y la operación de un sistema de IA, comparable al del propietario de un vehículo*"[453].

De este modo, en principio, el consumidor puede perseguir la responsabilidad en contra de quién desarrolla o quien utiliza el sistema de IA, sin necesidad de tener que averiguar si el

[448] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021.
[449] *Ibíd*. Artículo 3 letra f).
[450] *Ibíd*. Artículo 3 letra e).
[451] SANTOS Morón, M. *Derecho de daños e inteligencia artificial: hacia una posible regulación en la UE*. En: CORNEJO, M. e ISLER, E. (Eds.). *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. Santiago, Rubicón Editores, 2023. p. 143.
[452] PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA (Unión Europea), op. cit. Artículo 11.
[453] *Ibíd*. Considerando 10.

perjuicio en concreto halla su explicación en la fabricación, diseño, comercialización o control de la tecnología, lo que facilita la identificación de los eventuales demandados.

Cabe advertir que, de manera posterior a esta propuesta de Reglamento, se propuso una "Directiva relativa a la adaptación de las normas de responsabilidad civil extracontractual a la inteligencia artificial" (Directiva sobre responsabilidad en materia de IA) que, no obstante ser el instrumento jurídico que da continuación a lo contenido en el Reglamento, no se pronuncia específicamente sobre contra qué agentes puede perseguirse el daño.

Sin embargo, si se tienen a la vista los antecedentes contenidos en la misma Directiva, puede estimarse que dicha omisión se debe a que se optó por realizar una evaluación de impacto de la regulación propuesta y establecer temporalmente un articulado que abordara una menor cantidad de aspectos[454]. Y, comoquiera, si la Directiva no fuese reformada para incluir esta responsabilidad solidaria dual, ello no impide tener este criterio a la vista para efectos de proyectar una futura regulación que dé mayor protección a los consumidores chilenos.

Por su parte, la Propuesta de Directiva 2022/0302 sobre responsabilidad por productos defectuosos, también contiene una disposición que facilita al consumidor identificar al agente responsable de los daños. En efecto, su artículo 7 indica que:

> *"1. Los Estados miembros garantizarán que* ***el fabricante de un producto defectuoso pueda ser considerado responsable de los daños causados por ese producto****. Los Estados miembros garantizarán que, cuando un componente defectuoso haya provocado que el producto sea defectuoso,* ***el fabricante de un componente defectuoso también pueda ser considerado responsable de los mismos daños****.*
> *2. Los Estados miembros garantizarán que,* ***cuando el fabricante del producto defectuoso esté establecido fuera de la Unión, el importador del producto defectuoso y el representante autorizado del fabricante puedan ser considerados responsables de los daños causados por ese producto****.*

[454] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos. Bruselas, Bélgica, 2022. p. 11.

3. Los Estados miembros garantizarán que, ***cuando el fabricante del producto defectuoso esté establecido fuera de la Unión y ninguno de los operadores económicos a que se refiere el apartado 2 esté establecido en la Unión, el prestador de servicios de tramitación de pedidos a distancia pueda ser considerado responsable de los daños causados por el producto defectuoso****.*

4. Cualquier persona física o jurídica que modifique un producto que ya haya sido introducido en el mercado o puesto en servicio se considerará fabricante del producto a efectos del apartado 1, cuando la modificación se considere sustancial con arreglo a las normas nacionales o de la Unión aplicables en materia de seguridad de los productos y se lleve a cabo fuera del control del fabricante original.

5. Los Estados miembros garantizarán que, ***cuando no pueda identificarse a un fabricante con arreglo al apartado 1 o, cuando el fabricante esté establecido fuera de la Unión, no pueda identificarse a un operador económico con arreglo a los apartados 2 o 3, cada distribuidor del producto pueda ser considerado responsable cuando: a) el demandante solicita al distribuidor que identifique al operador económico o a la persona que suministró el producto al distribuidor; y b) el distribuidor no identifique al operador económico o a la persona que suministró el producto al distribuidor en el plazo de un mes a partir de la recepción de la solicitud"***[455] (énfasis agregado).

Como puede apreciarse, el precepto establece una cadena de responsabilidad que va aplicando en forma subsidiaria. En principio, responde directamente el fabricante del producto y/o del componente defectuoso; si estos se encuentran fuera del territorio jurisdiccional, responde el importador o su representante autorizado; si ellos tampoco están dentro del territorio, responderá el prestador de servicios a distancia; y, finalmente, si este no posee domicilio en la Unión, responderá el distribuidor del producto –que vendría siendo homologable al proveedor en nuestro medio–.

[455] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos. Bruselas, Bélgica, 2022. Artículos 7.1 a 7.5.

De este modo, se consagra una especial protección para los consumidores, puesto que siempre podrán demandar a alguien, con independencia de que no todos los miembros de la cadena de producción, distribución y uso de la IA sean identificables o posean sus domicilios en el territorio. El objetivo de ello es garantizar que la víctima pueda ejercer acciones a todo evento[456].

Estados Unidos

Actualmente, a diferencia de lo que ocurre en la Unión Europea, en Estados Unidos no existe ninguna normativa federal que regule en forma específica la responsabilidad derivada por el uso de IA[457]. Por tanto, en relación con el régimen de responsabilidad general, no hay ninguna facilidad o adecuación normativa destinada a facilitar que el consumidor pueda identificar al agente responsable del daño.

Sin perjuicio de lo anterior, la sección 3 letra f) de la Orden Ejecutiva N° 13.960 de 03 de diciembre del 2020 enfatiza en la necesidad de que las labores humanas involucradas en los procesos de diseño, desarrollo, adquisición y uso de la IA estén claramente definidas, de manera que resulte menos complejo efectuar una trazabilidad de los procedimientos e identificar a los presuntos responsables por acciones u omisiones del sistema[458].

Adicionalmente, algunos juristas norteamericanos han propuesto adoptar un "enfoque híbrido" de responsabilidad en esta materia, que permita hacer responsable de los daños ocasionados por la IA tanto a la entidad fabricante como al operador del sistema[459]. Ello sería posible a través de una aplicación extensiva de ciertos principios del *common law*, como, por ejemplo, los que rigen la responsabilidad productos defectuosos[460].

---

[456] LIGÜERRE, Carlos Gómez. La Propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos. InDret, 2022 <https://www.raco.cat/index.php/InDret/article/download/406110/500347> [consulta: 07 diciembre 2023]. p. 3.

[457] ZEIN, Dr Sarah. The Civil Liability for Artificial Intelligence. [en línea] BAU Journal-Journal of Legal Studies-مجلة الدراسات القانونية. Vol. 2022(1). <https://digitalcommons.bau.edu.lb/lsjournal/vol2022/iss1/14/> [consulta: 05 de diciembre de 2023]. p. 6. Por lo demás, cabe destacar que los autores de la presente memoria revisaron toda la normativa federal para asegurarse de la veracidad de tal constatación.

[458] PRESIDENTE de los Estados Unidos (Estados Unidos). Executive Order N° 13.960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, 03 de diciembre de 2020. Sección 3 (f).

[459] ZEIN, op. cit., p. 6.

[460] *Ibíd.*, p. 6

No obstante, conviene precisar que esta es una propuesta jurisprudencial que aún no se encuentra asentada. En consecuencia, bajo este régimen, las facilidades que poseen los consumidores en orden a identificar al agente responsable por los daños son solo eventuales, en tanto dependen de un criterio extensivo que no necesariamente será compartido por todos los jueces.

b. Responsabilidad de los Intermediarios

Unión Europea

En la Unión Europea, este asunto comenzó a ser regulado en la Directiva CE 2000/31/CE sobre Comercio Electrónico[461], a propósito de las plataformas online que prestan servicios de alojamiento.

Dicha Directiva distingue, entre sus artículos 12 y 14, según si el servicio prestado por el intermediario consiste en brindar: (i) acceso a red o mera transmisión de datos (artículo 12); (ii) almacenamiento temporal de los datos transmitidos –para aumentar la velocidad de la red–[462] (artículo 13); o (iii) alojamiento permanente de los datos (artículo 14). Cada uno de los preceptos establece causales de exención de responsabilidad, que, de verificarse, permiten al proveedor intermediario desentenderse de la información contenida en sus plataformas. Estas hipótesis se conocen como puertos seguros o *safe harbours*[463].

En términos generales, respecto de los proveedores que realizan una mera transmisión de datos (artículo 12) o los almacenan temporalmente (artículo 13), se consolida un régimen que permite la exención de responsabilidad en la medida en que proveedor juegue un rol pasivo, vale decir, que se limite a permitir la transmisión de la información o volverla más eficiente, sin modificar ni controlar los datos[464]. Esto hace sentido si se tiene en cuenta que la naturaleza de sus labores es esencialmente técnica y automática[465].

---

[461] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022.
[462] AMAYUELAS, E.A., 2020. *La responsabilidad de los intermediarios en Internet ¿puertos seguros a prueba de futuro?*. Cuadernos de Derecho Transnacional, 12(1): p. 808-837. p. 811.
[463] *Ibíd*., p 809.
[464] PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA (UE), op. cit., considerando 42.
[465] *Ibíd.*

Los proveedores que alojan permanente los datos (artículo 14), en tanto, solo podrán ser considerados responsables si es que, teniendo conocimiento efectivo de que sus plataformas alojan información o actividades ilícitas, no actúan con prontitud para retirarlas. Lo anterior ha sido criticado por cierta doctrina, ya que, considerando que el artículo 15 dispone que ninguno de los intermediarios tendrá un deber general de supervisar la información de sus plataformas, se genera la paradoja de que, entre menos controla el contenido el intermediario, menos arriesga ser responsable. En efecto, si nunca supervisa, nunca tomará conocimiento efectivo de los eventuales contenidos ilícitos alojados, por lo que se amparará en un puerto seguro[466].

Con todo, se trata de un régimen que establece en forma precisa las causales de exención de responsabilidad de los intermediarios, distinguiendo según el tipo de actividad que realiza, lo que ya constituye un avance en relación con nuestra regulación. Además, cabe destacar que la principal crítica que admiten estos puertos seguros –que es la relacionada con la paradoja de los intermediarios que alojan datos en forma permanente–, se soluciona, prácticamente en su totalidad, con la propuesta de Reglamento de Servicios Digitales ("DSA"), que reforma la Directiva de Comercio Electrónico y trata en forma más moderna esta y muchas otras materias.

Si bien el DSA reproduce exactamente las mismas causales de exoneración de responsabilidad previstas en la Directiva de Comercio Electrónico (artículos 4 a 6 DMS), complementa en dos aspectos que ayudan a perfeccionar el régimen[467]. En primer lugar, en su artículo 7 consagra que:

> *"No se considerará que los prestadores de servicios intermediarios no reúnen las condiciones para acogerse a las exenciones de responsabilidad a que se refieren los artículos 4, 5 y 6 por la única razón de que realicen, de buena fe y de modo diligente, investigaciones por iniciativa propia de forma voluntaria, o adopten medidas con el fin de detectar, identificar y retirar*

[466] MARTÍN, S. *Cambio de horizontal a vertical: el dilema de la responsabilidad de los intermediarios de intercambio de contenidos protegidos en el derecho europeo*. En: CORNEJO, M. e ISLER, E. (Eds.). *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. Santiago, Rubicón Editores, 2023. pp. 171-173.

[467] Ello, sin perjuicio de las numerosas novedades que introduce en materia de control de contenidos y transparencia. Estas serán analizadas en una sección posterior, por ser aspectos que, a pesar de su trascendencia, no se vinculan directamente con la responsabilidad civil.

contenidos ilícitos, o bloquear el acceso a estos, o adoptar las medidas necesarias para cumplir los requisitos del Derecho de la Unión y del Derecho nacional en cumplimiento del Derecho de la Unión, incluidos los requisitos establecidos en el presente Reglamento"[468].

Así, acaba con la paradoja de no control que acechaba a los intermediarios de almacenamiento permanente de datos, pues aumenta "*la seguridad jurídica de los intermediarios que implementen mecanismos voluntarios para detectar, identificar y retirar contenidos ilícitos, o inhabilitar el acceso a los mismos, de sus servicios, en la medida en que no perderán su inmunidad por estas investigaciones voluntarias (es decir, por la moderación del contenido) si se llevan a cabo de buena fe y con diligencia*"[469]. En otras palabras, los intermediarios sabrán que, si investigan adecuadamente y toman conocimiento efectivo de contenidos ilícitos, no se volverán responsables por ese solo hecho, sino que, por el contrario, estarían disminuyendo las probabilidades de serlo en un futuro.

Más aún, la doctrina ha sostenido que la implementación de las medidas de investigación del artículo 7 "*debería resultar en muchas situaciones un presupuesto para considerar que el intermediario ha actuado con el nivel de diligencia mínimo que le es exigible para beneficiarse de la exención de responsabilidad*"[470].

En ese sentido, considerando que el Capítulo III del DSA justamente se titula "Obligaciones de diligencia debida para crear un entorno en línea transparente y seguro", podría entenderse que, cuando el artículo 7 utiliza la expresión "diligente", está reconduciendo a los deberes diligencia consagrados en dicho Capítulo, y, por tanto, el intermediario solo se eximiría de responsabilidad si es que sus investigaciones se realizaron contando con un sistema interno de gestión de reclamos (artículo 20) y cumpliendo con los deberes mínimos de transparencia informativa (artículos 14 y 15)[471].

---

[468] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/1925 sobre mercados disputables y equitativos en el sector digital. Bruselas, Bélgica, 2022. Artículo 7.
[469] CASTELLÓ, José. *Nuevo régimen de responsabilidad de los servicios digitales que actúan como intermediarios a la luz de la propuesta de Reglamento relativo a un mercado único de servicios digitales*. 2021. p. 18.
[470] DE MIGUEL ASENSIO, Pedro. *Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales*. La Ley Unión Europea. (109), p. 10.
[471] *Ibíd*., p. 17.

El segundo aspecto importante con el que complementa el DSA en esta materia, dice relación con el establecimiento de una excepción a la exención de responsabilidad de los intermediarios que alojen datos en forma permanente, cuando dichos intermediarios son plataformas en línea que interactúan directamente con el consumidor de una forma tal que lo llevan a pensar, razonablemente, que la información o las ofertas allí contenidas son proporcionadas por la propia plataforma y no por terceros. En concreto, el precepto señala:

> "*El apartado 1* [–que contiene la exención de responsabilidad–] *no se aplicará con respecto a la responsabilidad, en virtud del Derecho en materia de protección de los consumidores, de las plataformas en línea que permitan que los consumidores celebren contratos a distancia con comerciantes, cuando dicha plataforma en línea presente el elemento de información concreto, o haga posible de otro modo la transacción concreta de que se trate, de manera que pueda inducir a un consumidor medio a creer que esa información, o el producto o servicio que sea el objeto de la transacción, se proporcione por la propia plataforma en línea o por un destinatario del servicio que actúe bajo su autoridad o control*"[472].

El DSA se encarga de precisar ejemplos de dichas prácticas. Dentro de ellos se menciona a las plataformas en línea que: (i) no muestran claramente la identidad del comerciante; (ii) no revelan la identidad o los datos de contacto del comerciante hasta después de la formalización del contrato celebrado entre el comerciante y el consumidor; (iii) comercializan el producto o servicio en su propio nombre en lugar de señalar el nombre del comerciante que efectivamente suministra el producto o servicio. Se previene, con todo, que dichos casos son meramente ilustrativos y no taxativos[473].

En suma, se delimitan con precisión los casos en los cuales los intermediarios resultan responsables –incluso si no hubieren celebrado un contrato con el consumidor–, atendiendo a la naturaleza de las funciones que realizan y contemplando una regulación especial para aquellos intermediarios que, en los hechos, actúan como proveedores directos.

---

[472] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022. Artículo 6.3.

[473] *Ibíd,* considerando 24.

Estados Unidos

Si bien en Estados Unidos no existe ninguna normativa federal específica que regule la responsabilidad derivada del uso de IA, la responsabilidad de los intermediarios y de las plataformas se encuentra normada hace casi 30 años, en la "*Communications Decency Act of 1996*"[474].

La disposición que trata la materia es la afamada "*section* 230". Al efecto, indica que "*ningún proveedor o usuario de un servicio de ordenadores interactivo deberá ser tratado como el publicador o emisor de cualquier información proporcionada por otro proveedor de contenido informativo*"[475]. Asimismo, dispone que ningún proveedor o usuario será considerado responsable por cualquier medida que adopte voluntariamente y de buena fe para restringir el acceso o la disponibilidad material que considere obsceno, lascivo, sucio, excesivamente violento, acosador o de otro modo objetable, esté o no constitucionalmente protegido (también conocida como protección del "buen samaritano")[476].

De esta manera, se da lugar a una inmunidad amplia, pues los intermediarios, por regla general, no serán considerados responsables respecto de contenidos creados por usuarios que se alojen en sus plataformas, ni tampoco por actos de moderación voluntaria y de buena fe que efectúen sobre estos contenidos. Las excepciones que haya lo anterior son la responsabilidad penal federal, las violaciones a la privacidad electrónica y las transgresiones a la propiedad intelectual, que por disposición expresa de la ley no quedan cubiertas por la inmunidad[477].

Ahora bien, a pesar de que la amplitud del texto de la sección ha llevado a que los tribunales norteamericanos extiendan la inmunidad incluso a plataformas que indirectamente fomentan o hacen más fácil la realización de actividades ilegales[478], la doctrina ha precisado que, si se tiene en cuenta la historia de la ley y el modo en que ha evolucionado el internet, la

[474] CONGRESO de los Estados Unidos (Estados Unidos). Communications Decency Act of 1996. Washington D.C., Estados Unidos, 08 de febrero de 1996.
[475] *Ibíd.*, sección 230. Traducción libre de: "*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*".
[476] *Ibíd.*
[477] *Ibíd*.
[478] CITRON, Danielle Keats; WITTES, Benjamin. T*he internet will not break: Denying bad samaritans sec. 230 immunity.* Fordham L. Rev. 86, pp. 406-408, 2017.

conclusión debiese ser que la inmunidad alcanza únicamente a los intermediarios que, en forma comprometida y de buena fe, han tratado de controlar o tomar medidas razonables para disminuir la probabilidad de que exista material abusivo dañoso en sus plataformas, aun si han fallado en el intento[479].

No cubre, en cambio, a intermediarios que diseñan plataformas propicias para la realización o creación de contenido ilegal, y, a sabiendas de que lo alojan o que probablemente lo alojen, no hacen nada para impedirlo. En este caso estaríamos ante un mal samaritano, que debe responder civilmente cuando los contenidos de terceros ocasionen daños a consumidores o usuarios[480].

A la precisión anterior cabe agregar que, según ha sostenido la doctrina, la inmunidad tampoco alcanza a aquellos intermediarios que emplean algoritmos de recomendación, cuando es el contenido generado por estos algoritmos el que ha dañado a usuarios o consumidores. En efecto, la protección brindada por la sección 230 presupone que el intermediario aloja contenido desarrollado por otro proveedor de contenidos de información (en otras palabras, un tercero)[481]. En este caso, el contenido no sería creado por un tercero, sino por los propios algoritmos que emplea el intermediario, de modo que no queda amparado por el puerto seguro[482].

Así, aparentemente el régimen legal estadounidense permite construir la responsabilidad de los intermediarios que emplean IA en forma más precisa y amplia que la DSA de la Unión Europea, al evitar que queden cubiertos por la inmunidad al usar algoritmos de recomendación.

Podría contra argumentarse que los algoritmos son en cierto sentido un tercero, por cuanto constituyen una tecnología autónoma que es distinta del intermediario en sí. Además, su funcionamiento es opaco, de modo que es posible que la IA realice procesos que no sean comprendidos ni directamente controlados por quienes emplean la tecnología[483]. De ser así,

---

[479] *Ibíd*., p. 417.
[480] *Ibíd*., p. 418.
[481] TREMBLE, Catherine. *Wild Westworld: Section 230 of the CDA and Social Networks' Use of Machine-Learning Algorithms*. Fordham L. Rev. 86: 2017, p. 829.
[482] *Ibíd.*, p. 868.
[483] *Ibíd*., pp. 863-864.

no debería descartarse la aplicación de la sección 230. Sin embargo, tal tesis es difícil de sostener en circunstancias que el proveedor dirige la publicidad en forma intencional y no se limita simplemente a difundir contenidos de algoritmos ajenos[484].

Este último razonamiento se ha utilizado, por ejemplo, para descartar la inmunidad de intermediarios que emplean sistemas de IA generativa como Chat GPT. Los algoritmos no pueden ser considerados como "proveedores de contenidos de información" (que son los terceros que generan contenidos respecto de los que los intermediarios poseen inmunidad), ya que cuando el intermediario los emplea está creando su propio contenido o, al menos, aprovechándose directamente de su beneficio, por lo que pierde la neutralidad que justifica la protección del intermediario clásico[485].

A mayor ahondamiento, la idea de que la IA no queda cubierta por la sección 230 no solo ha tomado fuerza en la doctrina, sino que también ha sido objeto de desarrollo normativo. En efecto, en la "Bipartisan Framework on AI Legislation" del año 2023 se ordena expresamente al Congreso clarificar que esta sección no resulta aplicable a los sistemas de IA[486].

Cabe destacar que el hecho de que los intermediarios que emplean IA no queden cubiertos por la inmunidad de la sección 230, no supone afirmar su responsabilidad en todos y cada uno de los casos. Simplemente se descarta la operación de una exención automática. Pero, para determinar la responsabilidad de un intermediario en una situación específica, habrá que evaluar si se cumplen los requisitos del respectivo régimen, que en este caso, a falta de normativa especial, es el sistema general de *tort of negligence* (responsabilidad extracontractual por culpa).

c. Carácter transfronterizo

Unión Europea

[484] *Ibíd*., p. 868.
[485] PERAULT, M., 2023. Section 230 Won't Protect ChatGPT. *J. Free Speech L.*, vol. 3, p. 365.
[486] Senadores Richard Blumenthal & Josh Hawley (Estados Unidos), *Bipartisan Framework on Artificial Intelligence Legislation*, 08 de septiembre de 2023.

En lo que atañe a las implicancias del carácter transfronterizo de la IA en la responsabilidad civil, podría pensarse que no tiene sentido realizar una comparación entre la normativa de la Unión Europea y la de un Estado independiente, desde que la primera corresponde a una regulación comunitaria que está pensada para ser aplicada en muchos Estados; mientras que a la segunda subyace, por lo general, una lógica meramente interna.

Empero, más allá de que dicha constatación resulta cuestionable por hacer caso omiso a la necesidad de proteger la indemnidad de los consumidores en el contexto de la IA –cuestión que debiera regir con independencia del lugar en donde se ubique del agente que comete el daño–, lo interesante de la regulación de la Unión Europea es que no solo aborda el carácter transfronterizo en situaciones en que hay actores de diversos Estados de la Unión involucrados –que es algo que obviamente preverá–, sino también cuando participan agentes no comunitarios. En ese sentido, se regulan situaciones en las que participan personas o elementos extranjeros en relación con aquel lugar en el que naturalmente regirá la regulación, lo que es perfectamente extrapolable a la perspectiva estatal.

A modo meramente ilustrativo, si pensamos hipotéticamente en que la UE es un Estado único constituido por muchas naciones, el hecho de regular algo que excede las fronteras de dicho Estado sería equivalente a lo que en Chile supondría regular situaciones que involucran elementos o personas externas al territorio. Vale decir, es la misma lógica, solo que a distinta escala. De ahí que los criterios adoptados en la Unión Europea puedan eventualmente ser replicados en nuestro país.

Pues bien, ya aclarado ese punto, corresponde examinar la normativa de la Unión Europea. Se trata, en verdad, de un asunto en el que las disposiciones hablan por sí solas. La forma en que las Diversas Directivas y Reglamentos se encargan de precisar sus respectivos ámbitos de aplicación es tan clara, que no hace falta dar explicaciones complejas para percibir el alto grado de protección con el que cuentan los consumidores.

En términos generales, un estudio de la diversa normativa sobre IA y responsabilidad que se pronuncia sobre la situación permite constatar que lo relevante es que el consumidor, usuario o destinatario se encuentre dentro del territorio regulado y haga uso de los productos o servicios estando en él, con total independencia del lugar en donde el proveedor posea su establecimiento.

Así, por ejemplo, el apartado 1º del artículo 2º del DSA señala que: "*1. El presente Reglamento se aplicará a los servicios intermediarios ofrecidos a destinatarios del servicio que tengan su lugar de establecimiento o estén situados en la Unión, con independencia de donde los prestadores de dichos servicios intermediarios tengan su lugar de establecimiento*"[487].

En el mismo sentido, el apartado 2º del artículo 1º del Reglamento de Mercados Digitales ("DMA") prevé que: "*2. El presente Reglamento se aplicará a los servicios básicos de plataforma prestados u ofrecidos por guardianes de acceso a usuarios profesionales establecidos en la Unión o a usuarios finales establecidos o situados en la Unión, independientemente del lugar de establecimiento o residencia de los guardianes de acceso y del Derecho que, por lo demás, sea aplicable a la prestación del servicio*"[488].

Por su parte, el apartado 1º del artículo 2º de la AI Act replica los criterios citados, pero va un paso más allá y establece, también, una causal de aplicación asociada a que se haga uso de la información dentro del territorio, incluso si tanto el usuario como el proveedor pertenecen a un tercer país. En efecto, dispone que:

> "*1. El presente Reglamento es aplicable a: a) los proveedores que introduzcan en el mercado o pongan en servicio sistemas de IA en la Unión, con independencia de si dichos proveedores están establecidos en la Unión o en un tercer país; b) los usuarios de sistemas de IA que se encuentren en la Unión; c) los proveedores y usuarios de sistemas de IA que se encuentren en un tercer país, cuando la información de salida generada por el sistema se utilice en la Unión*"[489].

En suma, el hecho de que ciertos agentes tengan su establecimiento o desempeñen sus funciones fuera del territorio jurisdiccional, no constituye un óbice para que el consumidor pueda eventualmente perseguir su responsabilidad haciendo uso del derecho al que él mismo

---

[487] *Ibíd.* Artículo 2.1.

[488] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/1925 sobre mercados disputables y equitativos en el sector digital. Bruselas, Bélgica, 2022. Artículo 1.2.

[489] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículo 2.1.

se encuentra sometido. Esto lo alivia de la carga de tener que indagar y probar derecho extranjero para presentar una demanda de indemnización de perjuicios cuando en la cadena asociada a la producción, distribución y uso de la IA participan agentes extranjeros.

Estados Unidos

En Estados Unidos, dado que no existe una normativa especial sobre responsabilidad de la IA, no hay disposiciones que se hagan cargo –en forma directa– del problema relacionado con que el hecho dañoso cometido por la IA ocurra en un Estado y los efectos se manifiesten en otro. Sin embargo, siendo justos, ello no debiese resultar problemático para los ciudadanos norteamericanos, ya que la jurisprudencia nacional que se ha desarrollado sobre responsabilidad extracontractual en casos de derecho internacional privado permite que los consumidores afectados utilicen su propia ley, aun cuando el hecho generador de la responsabilidad se haya verificado en otro lugar[490].

Vale decir, a diferencia de nuestro ordenamiento, para determinar la ley aplicable a los casos de responsabilidad extracontractual transfronterizos, no rige plenamente el principio de *lex loci delicti,* sino que es posible emplear la ley del lugar en donde la víctima resultó dañada. En efecto, para determinar la ley aplicable, los Tribunales estadounidenses emplean criterios y normas que no son axiológicamente neutras. Estas normas permiten que el juez utilice cláusulas de escape o recurra a un factor de conexión alternativo que, a la postre, redunde en la aplicación del derecho que brinde una mayor protección al consumidor (que normalmente será el de su propio Estado)[491].

Así, por mucho que no exista una regulación específica de esta materia a propósito de la IA, el problema puede ser resuelto a partir de las normas genéricas que rigen los casos de responsabilidad extracontractual en el derecho internacional privado de los Estados Unidos, pues al aplicarlas se evita que el consumidor se vea en la necesidad de estudiar y probar derecho extranjero.

[490] GARRO, Alejandro. *El Derecho Internacional Privado en los Estados Unidos: Balance y Perspectivas*. Revista Mexicana de Derecho Internacional Privado, Número especial, pp. 97-114, 2000.
[491] *Ibíd,* pp. 97-114.

d. Prueba de la causalidad

El último problema referido a la responsabilidad civil derivada de los daños ocasionados por la IA, dice relación con la necesidad de probar el vínculo de causalidad entre la acción u omisión del sistema y el daño ocasionado al usuario. Esto puede desincentivar el ejercicio –o condicionar el éxito– de acciones de indemnización de perjuicios, por cuanto:

> "[L]*as 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*"[492].

En otras palabras, la complejidad y la opacidad de la IA llevan a que sea prácticamente imposible explicar la causa concreta del daño, porque para ello habría que entender el funcionamiento completo del sistema de IA, describir cómo interactúan todos sus componentes y saber qué acción u omisión específica del proceso fue la que ocasionó el daño[493]; lo que, si ya resulta desafiante para una empresa promedio, con mayor razón lo será para un consumidor.

Unión Europea

Para dar solución a este problema, la Unión Europea consagra presunciones refutables de causalidad. Así, la Directiva sobre Responsabilidad en materia de IA indica que, en principio, el vínculo causal entre la acción u omisión y los daños se presumirá si es que el demandante prueba: (i) la culpa del demandado –esto es, que infringió un deber de diligencia previsto en la normativa europea–; (ii) que el deber de diligencia infringido tenga por fin evitar la producción de los daños ocasionados; (iii) que, por tanto, pueda considerarse razonablemente probable,

[492] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022. Considerando 3º.

[493] SANTOS Morón, M. *Derecho de daños e inteligencia artificial: hacia una posible regulación en la UE*. En: CORNEJO, M. e ISLER, E. (Eds.). *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. Santiago, Rubicón Editores, 2023. p. 139

basándose en las circunstancias del caso, que la culpa ha influido en los resultados producidos por el sistema de IA o en la no producción de resultados por parte del sistema de IA; y (iv) que esa producción o no producción de resultados le ha ocasionado daños[494].

Sin embargo, luego el artículo matiza que, respecto de los agentes que puedan ser catalogados como proveedores o usuarios de alto riesgo en base a la AI ACT, la culpa –que es un antecedente necesario para presumir la causalidad- se entenderá probada solo si es que el deber infringido es uno de aquellos específicos que consagran los Capítulos pertinentes de tal cuerpo normativo.

En el caso de los proveedores de alto riesgo, dichos deberes van asociados al manejo de datos de calidad, la transparencia informativa, la vigilancia humana, etc.[495]; mientras que en el caso de los usuarios de alto riesgo, los deberes dicen relación con supervisar, utilizar, suspender o interrumpir el funcionamiento del sistema de IA siguiendo los instructivos de uso, así como no exponerlo a datos de entrada bajo su control que no resulten pertinentes de acuerdo a la finalidad del sistema[496].

Respecto de los sistemas de IA que no son de alto riesgo, la presunción de causalidad solo aplicará cuando el órgano jurisdiccional nacional considere excesivamente difícil para el demandante demostrar el nexo causal[497]. Dicha dificultad será medida atendiendo al nivel de opacidad, autonomía, complejidad y otras características del sistema de IA empleado[498].

Por su parte, la Directiva sobre responsabilidad por los daños causados por productos defectuosos también establece una presunción de causalidad, pero no asociada a la culpa, sino al carácter defectuoso del producto. Su artículo 6 dispone que: "*3. Se presumirá el nexo causal entre el carácter defectuoso del producto y el daño cuando se haya comprobado que*

494 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea), op. cit. Artículo 4. Cabe advertir que, para la construcción de todos los requisitos, no solo se tuvo a la vista la norma, sino también la interpretación doctrinaria y las explicaciones que la misma Directiva brinda en las páginas previas. Al efecto, véase: (i) CASALS, M.M., 2023. Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial. *InDret*, pp. 72-73; y (ii) Directiva Responsabilidad IA, p. 15.

495 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022. Artículo 4.

496 *Ibíd.*

497 *Ibíd.*

498 *Ibíd.* Considerando 28.

el producto es defectuoso y el daño causado sea de un tipo compatible normalmente con el defecto en cuestión"[499].

Como puede apreciarse, todas estas presunciones de causalidad, si bien varían levemente según la naturaleza de los actores involucrados o del daño ocasionado, evocan lo que en doctrina se conoce como causalidad normativa por imputación objetiva[500]. En concreto, pareciera utilizarse como criterio el fin de protección de la norma relevante, en el sentido de que, si la norma que se ha infringido –sea que consagre un deber de diligencia o una causal de producto defectuoso– tiene por finalidad evitar la materialización de los daños que, de hecho, fueron ocasionados, el resultado dañoso podrá ser objetivamente imputado al actuar del demandado, atendido el estrecho vínculo normativo que existe entre su culpa y el daño[501].

Este criterio también posee aplicación general en el ámbito de la responsabilidad civil extracontractual de nuestro ordenamiento, para efectos de demostrar la concurrencia de causalidad normativa[502]. Sin embargo, la principal diferencia radica en que en la Unión Europea se indica que dicha imputación objetiva genera una presunción legal de causalidad; en tanto que en Chile esta imputación solo satisface el aspecto normativo de la causalidad, quedando pendiente de probar, todavía, la causalidad natural, esto es, la relación empírica concreta de causa a efecto entre el hecho y el daño[503].

En ese sentido, el régimen de causalidad europeo es más favorable para el consumidor que el régimen chileno. Con todo, el consumidor europeo aún enfrenta una gran dificultad: ¿cómo accede a las pruebas necesarias para poder probar la infracción al deber de diligencia del agente, la existencia del daño y su vinculación con la culpa, o, si fuere el caso, el carácter defectuoso del producto? Recordemos que, de no acreditarse dichas circunstancias, no operarán las presunciones de causalidad.

---

[499] *Ibíd.* Artículo 6.3.

[500] PANTALEÓN Prieto, Ángel. *Causalidad e imputación objetiva: criterios de imputación*. Asociación de Profesores de Derecho Civil (coords.). Centenario del Código Civil (1889-1989). Tomo II. Madrid, Editorial Universitaria Ramón Areces, pp. 1561-1591, 1990.

[501] *Ibíd.*, pp. 1580-1581.

[502] BARROS, Enrique. *Tratado de responsabilidad extracontractual*. Santiago, Editorial Jurídica, 2010. 384-391pp.

[503] *Ibíd.*, p. 374. Ello, por lo demás, sin perjuicio de que la causalidad normativa pueda ser rebatida a partir de la aplicación de otros criterios.

La normativa europea prevé una solución parcial a este problema. No es el objetivo de la presente Memoria ahondar en aspectos procesales del derecho a acceso a la prueba, pero, en lo que ahora interesa, el artículo 3 de la Directiva sobre Responsabilidad en materia de IA[504] y el artículo 8 de la Directiva sobre responsabilidad por los daños causados por productos defectuosos[505] disponen que todo consumidor que haya resultado dañado y cuente con pruebas o hechos que acrediten la viabilidad o verosimilitud de su pretensión[506], podrá requerir al Tribunal que ordene al demandado, respetando los principios de necesariedad y proporcionalidad, la exhibición de las pruebas que obren en su poder y resulten pertinentes[507].

En el caso de la Directiva sobre Responsabilidad en materia de IA, se prevé un requisito adicional, relacionado con que el demandante haya realizado, en forma previa a requerir asistencia del Tribunal, todos los intentos proporcionados para obtener del demandado las pruebas pertinentes[508]. Como contrapartida a la mayor exigencia, se contempla una sanción para el demandado que se niegue a exhibir, que consiste en que se presumirá legalmente su infracción a un deber de diligencia –lo que facilita la aplicación del artículo 4–[509].

En síntesis, para dar solución a las dificultades asociadas a la prueba del nexo de causalidad respecto de los daños ocasionados por la IA, la normativa europea establece: (i) presunciones legales de causalidad que funcionan en base a un criterio de imputación objetiva; (ii) facilidades de acceso a la prueba al consumidor, con el fin de que le resulte más fácil acreditar el cumplimiento de los requisitos necesarios para que operen las presunciones. Ambas reglas suponen adaptaciones al régimen ordinario de responsabilidad civil, que redundan en una protección más alta y especializada a favor de los consumidores.

Quizás el único aspecto problemático de este régimen es que, aun teniendo acceso a las pruebas pertinentes, podría resultar complejo para el consumidor probar la infracción

---

[504] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022. Artículo 3.

[505] *Ibid.* Artículo 8.

[506] Nótese que, en este punto, solo se exige acreditar que la pretensión sea viable o verosímil. Las Directivas no ahondan sobre estos conceptos en sus Considerandos, pero, desde luego, sus sentidos naturales y obvios remiten a un estándar mucho menor que aquel necesario para poder condenar posteriormente en el juicio.

[507] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022. Artículo 3.

[508] *Ibíd.*

[509] *Ibíd.*

concreta del proveedor y su probabilidad de incidencia en los daños. Pero esto podría ser solucionado en nuestro ordenamiento si es que se aplica el estándar de culpa infraccional –ya vigente–, y, además, se explicita que la sola infracción a una norma que tiene por finalidad evitar la producción de ciertos daños, es suficiente para que pueda considerarse razonablemente probable que, en el evento de que dichos daños se materialicen, la culpa influyó en ello[510].

Estados Unidos

Como ya se ha explicado, actualmente en Estados Unidos no existe una normativa federal que regule la responsabilidad derivada del uso de IA. Por consiguiente, no hay disposiciones que supongan una adecuación al régimen ordinario de causalidad, y el consumidor deberá probar el nexo causal de conformidad a las reglas generales de la responsabilidad extracontractual.

Esto ha sido criticado por la propia doctrina estadounidense, que, teniendo a la vista las propuestas de la Unión Europea, ha advertido que las nuevas tecnologías pueden ocasionar problemas de causalidad que no logran ser adecuadamente resueltos por el sistema general de *tort* del *common law*[511]. En efecto, los consumidores deben probar el nexo causal sin contar con ninguna facilidad para ello, lo que resulta especialmente sensible si se tiene en cuenta que la jurisprudencia norteamericana ha señalado que la causalidad "puramente lógica" o la "causa eficiente" no bastan para tener por establecida la responsabilidad[512].

Ahora bien, sin perjuicio de lo anterior, cabe destacar que el sistema norteamericano contiene una norma que, en cierto sentido, complementa la idea de imputación objetiva por causalidad normativa que esboza la regulación europea. La norma en cuestión es la sección 16 letra B de la "*Digital Platform Commission Act*" del año 2023, que indica que si el agente causante del daño indemniza los perjuicios derivados de la infracción a una ley específica,

[510] Podría estimarse que esto viene implícito en la normativa europea, porque forma parte del criterio de imputación objetiva. Pero, a falta de precisión y de doctrina que se pronuncie sobre ese aspecto de la Directiva, probablemente la mejor opción sea que, si se consagra un régimen similar en Chile, se introduzca una disposición expresa que se oriente en tal sentido.
[511] HEISS, Stefan. *Towards Optimal Liability for Artificial Intelligence: Lessons from the European Union's Proposals of 2020.* [en línea] Hastings Sci. & Tech. LJ, 2021, vol. 12, p. 205. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/hascietlj12&div=11&id=&page=> [consulta: 13 octubre 2023]. p. 205.
[512] *Ibíd*., p. 205.

quedará exento de responsabilidad ante el denunciante únicamente en lo que refiera a la infracción de dicha ley[513].

Como puede apreciarse, no es una norma que facilite o dificulte la prueba del vínculo causal. Sin embargo, resulta interesante por dos razones. En primer lugar, pareciera sugerir que existe un estrecho vínculo entre el fin de protección de una norma jurídica y los daños ocasionados, en el sentido que, así como hay daños que quedan cubiertos por aquello que buscaba proteger la norma, también habrá daños que excedan ese ámbito de protección y, por ende, no puedan ser objetivamente imputados a la infracción.

En segundo lugar, deja a salvo la posibilidad de que puedan perseguirse indemnizaciones que vayan más allá de una determinada infracción. Vale decir, no por el hecho de que un consumidor haya conseguido una sentencia indemnizatoria favorable respecto de una infracción, se va a entender que hubo una reparación integral de todos los daños que le ha ocasionado la IA. Es probable que haya daños que correspondan a otra infracción, que se manifiesten en forma ulterior o que solo posean una causalidad fáctica. En ese sentido, la norma deja espacio para que el consumidor intente perseguirlos incluso si ya obtuvo una reparación parcial.

2. Datos Personales

En el Capítulo II, al momento de examinar lo que ocurre entre el derecho a la vida privada y el tratamiento de datos personales, se identificaron tres materias que, en nuestro ordenamiento, han sido abordadas de manera compleja o, más bien, difusa: (i) obligaciones de los proveedores que tratan datos personales; (ii) tratamiento automatizado de datos personales; y (iii) tutela judicial efectiva de los consumidores en materia de protección de datos.

A continuación, se examinarán diversas disposiciones propuestas o consagradas, en primer lugar, en la Unión Europea, con especial énfasis en el Reglamento General de Protección de Datos -que establece los requisitos específicos para empresas y organizaciones

[513] CONGRESO de los Estados Unidos (Estados Unidos). *S.4201 - Digital Platform Commission Act of 2022.* Washington D.C., Estados Unidos, 12 de mayo de 2022. Sección 16.

sobre recogida, almacenamiento y gestión de los datos personales- y, en segundo lugar, en Estados Unidos, que permiten hacer frente a cada uno de dichos problemas[514].

a. Obligaciones de los proveedores que tratan datos personales

Unión Europea

En el ámbito de las obligaciones de los proveedores que tratan datos personales, se abren importantes perspectivas para comprender el delicado equilibrio entre la protección de la privacidad y la necesidad de utilizar datos personales en la era digital. Para ello, a continuación se analizarán una serie obligaciones que impone la normativa europea para aquellos que, en el desenvolvimiento de su negocio, traten datos personales, entre las que se encuentran las obligaciones de información, de seguridad y de evaluación de impacto, en casos de riesgo.

Primeramente, muy ligado a lo que es la transparencia, se impone a los proveedores que traten datos personales una serie de deberes de información, los cuales incluyen informar a los consumidores acerca de cómo se recopilan, utilizan y protegen sus datos personales. Al respecto, el artículo 13 del RGPD detalla exhaustivamente aquella información que debe facilitar el proveedor responsable del tratamiento a sus consumidores al momento de obtener datos personales de los mismos[515]. De esta manera, la norma prescribe en sus primeros dos incisos:

> *"1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:*
>
> *a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;*
>
> *b) los datos de contacto del delegado de protección de datos, en su caso;*
>
> *c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;*

---

514 EUROPA. *Reglamento General de Protección de Datos*. [en línea] 06 de julio 2022 <https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm> [consulta: 22 de octubre 2023].

515 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Bruselas, Bélgica, 2016. Artículo 13.

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;

c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;

e) el derecho a presentar una reclamación ante una autoridad de control;

f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales

casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado"[516].

Asimismo, el propio artículo 13 prescribe que tal información debe facilitarse dentro de un plazo "razonable" y que, en caso de que el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente[517].

En la misma línea, el artículo 14 regula aquella información que deberá facilitar a los consumidores en aquellos casos en que sus datos personales no hayan sido obtenidos directamente de los mismos, con la diferencia de que en su inciso 5 señala una serie de excepciones en que tal obligación no aplica. Según dispone, tal información no debe ser puesta a disposición, en la medida en que:

"a) el interesado ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por

[516] *Ibíd.*
[517] *Ibíd.*

el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza legal"[518].

Adicionalmente, el artículo 24 del RGPD consagra la obligación de los proveedores de aplicar medidas técnicas y organizativas apropiadas en torno a los datos personales que se tratan, con el objeto de velar por la protección de los mismos y la rendición de cuentas en torno a las medidas implementadas por las empresas. Al respecto, dispone:

"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario"[519].

Por su parte, el artículo 25 del RGPD establece la obligación de los proveedores de proteger los datos personales de sus consumidores desde el diseño y por defecto[520], lo cual significa que deben considerar la privacidad y la seguridad de los datos desde el inicio de cualquier proceso de tratamiento de datos y de forma predeterminada.

Ligado a lo anterior, el Reglamento establece una serie de obligaciones en torno a la seguridad en el tratamiento de datos personales de los consumidores. A su respecto, por ejemplo, además de la obligación que establece el artículo 24 de aplicar medidas técnicas y organizativas apropiadas en torno a los datos personales, prescribe que se deben notificar las violaciones de seguridad de los datos personales a la autoridad de control (artículo 33)[521] y, además, que los proveedores deben comunicar estas violaciones a propios consumidores (artículo 34)[522].

Por lo demás, el artículo 30 del RGPD requiere que cada responsable y su representante mantengan un registro, por escrito, de las actividades de tratamiento realizadas

[518] *Ibíd.* Artículo 14.
[519] *Ibíd.* Artículo 24.
[520] *Ibíd.* Artículo 25.
[521] *Ibíd.* Artículo 33.
[522] *Ibíd.* Artículo 134.

bajo su responsabilidad y, también, de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable[523].

Adicionalmente, los artículos 35 y 36 del RGPD consagran dos procedimientos preventivos de suma importancia: la evaluación de impacto y la consulta previa, que son herramientas fundamentales para evaluar y mitigar los riesgos asociados al tratamiento de datos personales. Así las cosas, el artículo 35 dispone:

> *"Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares"*[524].

Por su parte, referente a la consulta previa, el artículo 36 ordena al responsable del tratamiento de datos consultar *"a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo"*[525].

Para finalizar, cabe destacar que el DMA estipula una serie las obligaciones de los guardianes de acceso en el contexto del tratamiento de datos personales, con el propósito de garantizar la transparencia y la responsabilidad en la recopilación y el uso de datos personales por parte de los grandes proveedores[526].

Estados Unidos

[523] *Ibíd.* Artículo 30.
[524] *Ibíd.* Artículo 35.
[525] *Ibíd.* Artículo 36.
[526] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/1925 sobre mercados disputables y equitativos en el sector digital. Bruselas, Bélgica, 2022.

En el ámbito de las obligaciones de los proveedores que tratan datos personales, la *Digital Services Oversight and Safety Act,* de 2022, aplicable a la cualquier plataforma en línea que utilice información personal en combinación con un proceso algorítmico para vender o publicar anuncios, con excepción a las pequeñas empresas, establece en su sección 9 que la Comisión Federal de Comercio (En adelante "**FTC**") emitirá regulaciones que requieran a los proveedores de una gran plataforma que utilice un sistema de recomendación especificar en los términos y condiciones del proveedor, de manera clara, accesible y comprensible, cómo se recopila o infiere cualquier información personal utilizada por el sistema de recomendación sobre un usuario de la plataforma, y las categorías de dicha información[527].

En segundo lugar, exige a los proveedores proporcionar una opción que no dependa de la información personal del usuario (ya sea recopilada o inferida) para determinar el orden de la información presentada al usuario. Al respecto, señala que la Comisión puede determinar excepciones razonables para garantizar la funcionalidad del producto, como la preferencia de idioma del usuario o el lugar reconocido, mas tal opción debe establecerse como predeterminada o presentarse de manera prominente dentro de la interfaz principal que contiene los resultados del sistema de recomendación[528].

En la emisión de regulaciones, la Comisión puede determinar que cierta información personal no se puede utilizar para personalizar un sistema de recomendación sin el consentimiento específico del usuario. En tal caso, un proveedor de una gran plataforma cubierta debe obtener de manera independiente el consentimiento para categorías separadas de información personal (categorizadas y de acuerdo con los estándares establecidos por la Comisión) en lugar de obtener un consentimiento global para toda la información personal o múltiples categorías de información personal simultáneamente[529].

Por su parte, la Orden Ejecutiva sobre el Desarrollo y Uso Seguro y Confiable de la IA, de 30 de octubre de 2023, aborda en diversas secciones materias relevantes en torno a las

[527] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.6796 - Digital Services Oversight and Safety Act of 2022*. Washington D.C., Estados Unidos, 18 de febrero de 2022. Sección 9, letra a) Nº 1.
[528] *Ibíd*. Sección 9, letra a Nº 2.
[529] *Ibíd*. Sección 9, letra b.

obligaciones de los proveedores que traten datos personales de sus consumidores, en tanto gira en torno a regulación del desarrollo y uso de la IA a nivel federal[530].

Sobre esa premisa, la sección 2 de la Orden establece que la IA debe ser segura y proteger la privacidad y las libertades civiles de los estadounidenses a medida que continúa avanzando su desarrollo[531]. En esa línea, en cuanto a la protección de la privacidad y las libertades civiles, la orden establece que la IA está facilitando la extracción, reidentificación, vinculación, inferencia y acción sobre información sensible sobre la identidad, ubicación, hábitos y deseos de las personas[532].

Para combatir este riesgo, señala la norma, el Gobierno debe garantizar que la recopilación, uso y retención de datos sea legal, segura y mitigue los riesgos de privacidad y confidencialidad, y, además, lo que más importante para los efectos de esta Memoria, dispone que las agencias deben utilizar herramientas técnicas y políticas disponibles, incluidas las tecnologías que mejoran la privacidad, para proteger la privacidad y combatir los riesgos legales y sociales más amplios que resultan de la recopilación y uso indebidos de los datos de las personas[533].

Por su parte, la sección 8 de la Orden destaca la importancia de proteger a los consumidores en el contexto del uso de la IA, para lo cual alienta a las agencias reguladoras independientes a considerar el uso de todas sus autoridades para proteger a los consumidores estadounidenses de fraudes, discriminación y amenazas a la privacidad, así como para abordar otros riesgos que puedan surgir del uso de la IA incluidos los riesgos para la estabilidad financiera[534].

Asimismo, la sección 9 de la Orden establece que se tomarán medidas para proteger la privacidad de los estadounidenses a medida que la IA avanza, lo cual incluye la evaluación y revisión de los procesos sobre cómo las agencias manejan la información comercialmente

[530] PRESIDENTE de los Estados Unidos (Estados Unidos). *Executive Order N° 14.110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 de octubre de 2023. p.1.
[531] *Ibíd.* Sección 2.
[532] *Ibíd*.
[533] *Ibíd.* Sección 3.
[534] *Ibíd.* Sección 8.

disponible que contiene datos personales, que pueden ser adquiridos directamente o a través de proveedores externos[535].

En lo que respecta a la legislación propuesta, el Proyecto de Ley "*American Data Privacy and Protection Act*" (En adelante "**ADPPA**") que se ingresó al Congreso estadounidense en el año 2021 tiene como objetivo proporcionar derechos fundamentales de privacidad de datos a los consumidores, establecer mecanismos sólidos de supervisión y crear una aplicación significativa[536].

Este proyecto, que es la primera ley federal en los Estados Unidos en torno a la protección de datos personales en contexto de IA, aplica a todas aquella entidad o persona, -excepto un individuo actuando en un contexto no comercial- que por sí sola o en conjunto con otros determine los propósitos y medios de recopilación, procesamiento o transferencia de datos personales o "cubiertos", y que esté sujeta a la Ley de la Comisión Federal de Comercio, sea un transportista común sujeto a la Ley de Comunicaciones de 1934 y todas las leyes modificatorias y complementarias o sea una organización no constituida para llevar a cabo negocios en beneficio propio o en el de sus miembros, e incluye cualquier entidad o persona que controle, sea controlada por, o esté bajo control común con la entidad cubierta[537]. Esto es lo que se entiende por "entidad cubierta".

Ahora bien, la propia norma señala que no se aplica en tres casos específicos:

1. Entidad gubernamental federal, estatal, tribal, territorial o local, como un organismo, autoridad, junta, oficina, comisión, distrito, agencia o subdivisión política del Gobierno Federal o de un Estado, gobierno tribal, territorial o local;
2. Persona o entidad que esté recopilando, procesando o transfiriendo datos cubiertos en nombre de una entidad gubernamental federal, estatal, tribal, territorial o local, en la medida en que dicha persona o entidad actúe como proveedor de servicios para la entidad gubernamental; o
3. Entidad que sirva como un centro de recursos nacionales sin fines de lucro designado por el Congreso y como centro de información para brindar

[535] *Ibíd*. Sección 9.
[536] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.8152 - American Data Privacy and Protection Act.* Washington D.C., Estados Unidos, 21 de junio de 2021, p.1.
[537] *Ibíd*. Sección 2.

asistencia a víctimas, familias, profesionales que trabajan con niños y el público en general en asuntos relacionados con niños desaparecidos y explotados[538].

Teniendo claridad respecto de los sujetos a quienes se refiere la ley y pasando ya de plano a lo que son las obligaciones de los proveedores que tratan datos personales, el proyecto establece una serie de principios que los proveedores deben respetar al tratar datos personales. Estos principios incluyen la minimización de datos, los deberes de lealtad, la protección por diseño, la lealtad a las personas físicas en materia de fijación de precios, transparencia y seguridad[539]. Además, otorga a los titulares personales los derechos a acceder, corregir, eliminar y transportar o portar sus datos personales, entre otros, en términos similares a cómo lo aborda la normativa de la UE[540].

Así las cosas, la sección 101, sobre minimización de datos personales, señala que una empresa no puede recopilar, procesar o transferir datos personales a menos que la recopilación, procesamiento o transferencia se limite a lo que sea razonablemente necesario y proporcional para:

a. Proporcionar o mantener un producto o servicio específico solicitado por el individuo al que pertenecen los datos; o
b. Efectuar un propósito permitido según el inciso (b), el cual enlista 17 excepciones, entre las cuales se encuentran, por ejemplo, proporcionar o mantener un producto o servicio específico solicitado por el individuo al que pertenecen los datos; detección y prevención de fraude e identidad; pago o recaudación de impuestos; cumplir con una obligación legal impuesta por ley federal, estatal, tribal o local; prevenir, prevenir lesiones inminentes o riesgos graves para la salud; y, proporcionar publicidad dirigida, siempre que se cumplan los requisitos de la ley, incluida la sección 204(c)[541].

En cuanto a los deberes de lealtad, la sección 102 de la ADPPA establece que las entidades cubiertas deben actuar de manera justa y equitativa con los individuos a quienes

[538] *Ibíd*.
[539] *Ibíd*.
[540] *Ibíd*.
[541] *Ibíd*. Sección 101.

pertenecen los datos personales que tratan y deben cumplir con los principios de transparencia, responsabilidad y confidencialidad en el tratamiento de los datos cubiertos[542].

Por otro lado, la sección 104 de la ADPPA establece la obligación de las entidades cubiertas de actuar con lealtad hacia las personas físicas en relación con la fijación de precios, en el sentido de proporcionar precios justos y equitativos a los individuos a quienes pertenecen los datos y evitar la discriminación en la fijación de precios basada en la información personal de los consumidores[543].

En lo que respecta a la protección por diseño, esta obligación se encuentra consagrada en la sección 103 de la ADPPA, según la cual las entidades cubiertas deben implementar medidas de privacidad por diseño en el desarrollo de productos y servicios que involucren el tratamiento de datos personales. En otras palabras, las empresas deben considerar la privacidad desde el inicio del proceso de diseño y desarrollo, en lugar de tratar de agregar medidas de privacidad después de que se haya creado el producto o servicio[544].

En el mismo sentido, la sección mencionada también establece que las entidades cubiertas deben implementar medidas de seguridad adecuadas para proteger los datos personales que manejan, lo que incluye la implementación de medidas técnicas y organizativas apropiadas para garantizar la confidencialidad, integridad y disponibilidad de los datos personales[545].

Relativo al principio de seguridad, la sección 208 del ADPPA establece que una entidad o proveedor de servicios cubierto por la norma debe establecer, implementar y mantener prácticas y procedimientos razonables de seguridad de datos administrativos, técnicos y físicos para proteger y asegurar los datos cubiertos contra el acceso y la adquisición no autorizados[546].

Asimismo, señala que tales prácticas deben ser apropiadas para el tamaño y complejidad de la entidad o proveedor de servicios, la naturaleza y alcance de la recolección,

[542] *Ibíd*. Sección 102.
[543] *Ibíd*. Sección 104.
[544] *Ibíd*. Sección 103.
[545] *Ibíd*.
[546] *Ibíd*. Sección 203.

procesamiento o transferencia de datos cubiertos, el volumen y la naturaleza de los datos cubiertos, la sensibilidad de los datos cubiertos, el estado actual de la tecnología y las limitaciones para proteger los datos cubiertos, y el costo de las herramientas disponibles para mejorar la seguridad y reducir las vulnerabilidades al acceso y adquisición no autorizados de los datos cubiertos[547].

Además, la sección establece requisitos específicos para las prácticas de seguridad de datos, incluyendo la identificación y evaluación de vulnerabilidades, la toma de medidas preventivas y correctivas, la evaluación de las medidas preventivas y correctivas, la eliminación de datos personales de acuerdo con un programa de retención, la capacitación de los empleados y la designación de un oficial para mantener y aplicar estas prácticas[548]. La Comisión puede emitir regulaciones para establecer procesos para cumplir con esta sección y debe consultar con el Instituto Nacional de Estándares y Tecnología para establecer estos procesos[549].

Por su parte, sección 202 de la ADPPA, relativa a la transparencia, dispone que las entidades cubiertas por este proyecto de ley deben proporcionar a los individuos políticas de privacidad que detallen la recopilación, el procesamiento, la transferencia y la seguridad de sus datos[550].

Señala, además, que tales entidades tienen la obligación de implementar políticas, prácticas y procedimientos razonables para la recopilación, el procesamiento y la transferencia de datos cubiertos, los cuales deben corresponder al tamaño, la complejidad, las actividades relacionadas con los datos cubiertos, los tipos y la cantidad de datos cubiertos con los que la entidad se involucra y el costo de implementación en comparación con los riesgos planteados[551].

Ahora bien, el proyecto también establece obligaciones específicas para los proveedores, como obtener el consentimiento expreso afirmativo de los individuos antes de

[547] *Ibíd*.
[548] *Ibíd*. Sección 103.
[549] *Ibíd*.
[550] *Ibíd*. Sección 202.
[551] *Ibíd*. Sección 101.

recopilar, procesar o transferir sus datos personales[552]. Asimismo, los proveedores también deben notificar a los individuos cualquier cambio material en su política de privacidad y proporcionar una oportunidad razonable para que los individuos retiren su consentimiento a cualquier recopilación, procesamiento o transferencia sustancialmente diferente de datos previamente recopilados bajo la política modificada[553].

Además, la ADPPA permite la transferencia de datos cubiertos a un tercero en el contexto de una fusión, adquisición, quiebra o transacción similar, siempre que la entidad cubierta proporcione a cada individuo afectado un aviso que describa la transferencia y brinde una oportunidad razonable para retirar cualquier consentimiento dado previamente y solicitar la eliminación de sus datos cubiertos[554].

Adicionalmente a lo anterior, cabe destacar el proyecto de ley propuesto en 2023 llamado "*Algorithmic Justice and Online Platform Transparency Act*" (En adelante "**AJOPTA**"), el cual tiene como objetivo prohibir el uso discriminatorio de la información personal por parte de las plataformas en línea en cualquier proceso algorítmico, exigir transparencia en el uso de procesos algorítmicos y moderación de contenido, y para otros fines[555].

El proyecto de ley establece que las plataformas en línea deben divulgar información clara y accesible sobre los procesos algorítmicos utilizados y cómo se recopila o infiere cualquier información personal utilizada por el sistema de recomendación sobre un usuario de la plataforma[556]. Además, se establece que las plataformas en línea deben proporcionar una opción que no dependa de la información personal del usuario para determinar el orden de la información presentada al usuario[557].

b. Elaboración de perfiles y publicidad personalizada

Unión Europea

[552] *Ibíd.*
[553] *Ibíd*.
[554] *Ibíd*. Sección 203.
[555] CONGRESO de los Estados Unidos (Estados Unidos). *S.2325 - Algorithmic Justice and Online Platform Transparency Act.* Washington D.C., Estados Unidos, de 13 de julio de 2023. p.1.
[556] *Ibíd*.
[557] *Ibíd*.

En cuanto a la elaboración de perfiles, en la Unión Europea, el artículo 4 del RGPD la define como "*toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*"[558].

Al respecto, a propósito de los deberes de información de los proveedores, el artículo 13 del RGPD, señala que el responsable de los datos debe facilitar al interesado la existencia de decisiones automatizadas, incluida la elaboración de perfiles y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado[559].

Por su parte, en el artículo 21 del Reglamento el legislador europeo otorga a los consumidores el derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernen sean objeto de un tratamiento, lo cual incluye la elaboración de perfiles[560].

En la misma línea, el artículo 22 dispone que "[t]*odo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar*"[561]*, c*on lo cual se busca proteger a los consumidores y, en general, a las personas de decisiones automatizadas que puedan tener un impacto importante en sus derechos, sin intervención humana adecuada o sin considerar adecuadamente su situación individual.

Sin embargo, es importante destacar que, a pesar de ese aparente afán de protección, tal precepto ha sido bastante criticado por dos factores. En primer lugar, por poseer un ámbito de aplicación bastante limitado, ya que el su aplicación está supeditada a que la decisión que

[558] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Bruselas, Bélgica, 2016. Artículo 4.
[559] *Ibid*. Artículo 13.
[560] *Ibid*. Artículo 21.
[561] *Ibid*. Artículo 22.

afecte a un individuo se base “únicamente” en un tratamiento automatizado de sus datos personales y, además, que la decisión en cuestión produzca efectos jurídicos en el individuo o le afecte significativamente de un modo similar.

Así las cosas, el hecho de que el tratamiento de los datos no esté exclusivamente automatizado ya excluye la aplicación del artículo 22 RGPD. Asimismo, en cuanto al segundo requisito, resulta cuestionable que muchas de las decisiones de personalización en el ámbito de los contratos con consumidores produzcan efectos de carácter propiamente jurídicos en el sentido del precepto[562].

En segundo lugar, se ha criticado fuertemente que este derecho esté sujeto a tres excepciones bastante amplísimas, en función de las cuales se permite la adopción de decisiones o la elaboración de perfiles completamente automatizadas si ello:

a) Es necesario para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
b) Está autorizado por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; o
c) Se basa en el consentimiento explícito del interesado.

Ahora bien, cabe destacar, eso sí, que el RGPD establece para los casos b) y c) una obligación del responsable de proporcionar información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado, en pos de mejorar la transparencia.

Pasando a lo que se conoce como “publicidad personalizada”, se trata de un asunto bastante discutido en la actualidad, puesto que los proveedores de servicios, sobre todos aquellos de gran tamaño, combinan los datos recabados a través de cada uno de sus productos para elaborar perfiles de usuarios tremendamente precisos e íntimos, los cuales luego utilizan para personalizar la experiencia de sus usuarios, supuestamente, “a costo cero”.

[562] RUBÍ PUIG, Antoni. *Elaboración de perfiles y personalización de ofertas y precios en la contratación con consumidores.* Revista de educación y derecho= Education and law review,. 24: 2021, p.13.

Al respecto, el artículo 26 del DSA, relativo a la publicidad en las plataformas en línea, prohíbe a los prestadores de plataformas en línea presentar a los destinatarios del servicio anuncios basados en la elaboración de perfiles utilizando las categorías especiales de datos personales a que se refiere el artículo 9, apartado 1, del Reglamento[563], esto es, aquellos que *"revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física"*[564].

Estados Unidos

Respecto de esta materia la normativa federal estadounidense actual no contempla reglas explícitas ni específicas. Sin embargo, en cuanto a los estándares propuestos la ADPPA define la publicidad personalizada o "*targeted adversiting*" como la presentación de anuncios en línea a individuos o dispositivos basados en preferencias, características o intereses conocidos o predichos asociados con identificadores únicos"[565].

Sin embargo, la ley establece que la publicidad personalizada no incluye la publicidad o marketing en respuesta a la solicitud específica de información o retroalimentación de un individuo, la publicidad contextual, esto es cuando un anuncio se muestra en función del contenido en el que aparece y no varía según quién ve el anuncio, o el procesamiento de datos cubiertos únicamente para medir o informar sobre publicidad o contenido, rendimiento, alcance o frecuencia, incluyendo la medición independiente[566].

Asimismo, el proyecto de ley menciona también que una entidad puede recopilar, procesar o transferir datos cubiertos con el propósito de proporcionar publicidad personalizada, siempre y cuando dicha recopilación, procesamiento o transferencia se limite a lo que sea

[563] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022. Artículo 26.
[564] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Bruselas, Bélgica, 2016. Artículo 9.
[565] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.8152 - American Data Privacy and Protection Act.* Washington D.C., Estados Unidos, 21 de junio de 2022. Sección 2.
[566] *Ibíd*.

razonablemente necesario y proporcional para tal fin. Esto significa que la entidad cubierta puede utilizar datos previamente recopilados de acuerdo con la ley para proporcionar publicidad personalizada, siempre y cuando cumpla con los requisitos de la ley, incluida la sección 204(c), que establece las condiciones para proporcionar publicidad dirigida[567].

Ahora bien, la normativa consagra en el literal c) de su sección 204 el derecho a optar por no recibir publicidad personalizada. Este derecho se refiere a la posibilidad de que un individuo se oponga a la transferencia de sus datos cubiertos a terceros con fines publicitarios y a la capacidad de optar por no recibir publicidad personalizada. En particular, establece que una entidad cubierta o un proveedor de servicios que entregue directamente publicidad personalizada debe proporcionar a los individuos un medio claro y conspicuo para optar por no recibir dicha publicidad, respetar cualquier designación de exclusión voluntaria por parte de un individuo y permitir que un individuo realice una designación de exclusión voluntaria con respecto a la publicidad personalizada a través de un mecanismo de exclusión voluntaria[568].

Además, la misma disposición establece que una empresa no puede transferir o dirigir la transferencia de los datos cubiertos de un individuo a un tercero si el individuo se opone a la transferencia y debe permitir que el individuo se oponga a dicha transferencia a través de un mecanismo de exclusión voluntaria[569].

c. Derechos y acciones de tutela de los consumidores

Unión Europea

Por último, en relación con los derechos y acciones de tutela de los consumidores en el contexto del tratamiento de datos personales, el RGPD establece una serie de derechos de vital importancia para los consumidores, tales como el derecho de acceso, de rectificación, de supresión, de limitación, de portabilidad y de oposición, los cuales se detallan de manera exhaustiva entre los artículos 15 y 21 del cuerpo legal y, además, impone a los proveedores, en su artículo 12, la obligación de facilitar a los consumidores el ejercicio de sus derechos.

---

[567] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.8152 - American Data Privacy and Protection Act.* Washington D.C., Estados Unidos, 21 de junio de 2021. Sección 10.
[568] *Ibíd*. Sección 204.
[569] *Ibíd*.

Respecto del derecho a la portabilidad de los datos, se ha discutido el alcance que le otorga al mismo el RGPD, pues "*del tenor literal del art. 20 podríamos entender que consiste en un derecho a "copiar y pegar" la información suministrada por el usuario que (...) abarcaría los datos proporcionados y generados por el us*uario"[570], que no es lo mismo que aquello que se conoce como "portabilidad en tiempo real", que permite que dos productos o servicios puedan interconectarse y trabajar juntos a través de medios técnicos[571].

Sin perjuicio de lo anterior, el DMA, en su artículo 6º, exige a los guardianes de acceso una "portabilidad efectiva" que incluya el "acceso continuo y en tiempo real los datos proporcionados y generados por estos y la transferencia de los mismos "en tiempo real de forma eficaz, como por ejemplo a través de interfaces de programación de aplicaciones de alta calidad[572].

Volviendo al RGPD, sus artículos 77, 78 y 79 establecen tres derechos importantísimos para los consumidores. En primer lugar, el artículo 77 consagra el derecho a presentar una reclamación ante una autoridad de control en caso de que el individuo involucrado considere que el tratamiento de sus datos personales infringe las normas que contempla el Reglamento, mientras que el artículo 78 otorga a los consumidores derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna y el artículo 79 otorga aquel de tutela judicial efectiva derecho contra un responsable o encargado del tratamiento de sus datos personales.

Para finalizar este acápite, cabe mencionar que la AI ACT no establece una regulación específica ni menos detallada en torno a los datos personales de los usuarios de sistemas que empleen IA en su funcionamiento, salvo por el caso en que tales datos, recabados para otros fines en el desarrollo de determinados sistemas de IA, sean utilizados en aras del interés público en el espacio controlado de pruebas para la IA. Sin embargo, la propuesta hace hincapié en que la protección de datos personales es un derecho fundamental de los

[570] TAMAYO VELASCO, Jimena, et al. *Big data, competencia y protección de datos: el rol del Reglamento General de Protección de Datos en los modelos de negocio basados en la publicidad personalizada.* Revista de estudios europeos (78): 2021, p.198.
[571] *Ibíd.*, p.197.
[572] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/1925 sobre mercados disputables y equitativos en el sector digital. Bruselas, Bélgica, 2022. Considerando 54.

ciudadanos de la Unión Europea y, además, se refiere explícitamente en múltiples ocasiones al RGPD, en pos de enfatizar su plena aplicación.

Estados Unidos

Actualmente en la normativa estadounidense no se contempla un régimen específico de tutela de los consumidores en caso de que sus derechos relativos a los datos personales de los que son titulares. Sin perjuicio de lo anterior, es importante mencionar que la normativa federal de los Estados Unidos incluye varias leyes y órdenes ejecutivas que buscan proteger los datos personales de los consumidores en el contexto de la IA, como ya se ha venido diciendo.

De esta manera, por ejemplo, la Orden Ejecutiva sobre el Desarrollo y Uso Seguro y Confiable del 2023 de la Inteligencia Artificial establece que el gobierno federal hará cumplir las leyes y principios de protección al consumidor existentes y promulgará salvaguardas apropiadas contra el fraude, el sesgo no intencional, la discriminación, las infracciones a la privacidad y otros daños de la IA[573].

En la misma línea, la Ley de Supervisión y Seguridad de Servicios Digitales de 2022 establece un marco integral para la transparencia, la responsabilidad y la seguridad en línea, y crea la Oficina de Supervisión y Seguridad de Servicios Digitales dentro de la Comisión Federal de Comercio, mientras que la Ley de Justicia Algorítmica y Transparencia de Plataformas en Línea prohíbe el uso discriminatorio de la información personal por parte de las plataformas en línea en cualquier proceso algorítmico y exige transparencia en el uso de procesos algorítmicos y moderación de contenido.

Además, el Marco Bipartidista sobre la Legislación de IA, la Ley de Iniciativa Nacional de IA de 2020, la Ley de Responsabilidad Algorítmica de 2023 y el Plan para una Declaración de Derechos de IA también contienen disposiciones relevantes para la protección de los datos personales de los consumidores en el contexto de la IA.

[573] PRESIDENTE de los Estados Unidos (Estados Unidos). *Executive Order N° 14.110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 de octubre de 2023.

En lo que respecta a la legislación propuesta, la ADPPA consagra en su sección 403 una serie de disposiciones relativas a la ejecución por personas de la norma en cuestión, para lo cual comienza por señalar que:

> "[C]*ualquier persona o clase de personas por una violación de esta Ley o un reglamento promulgado bajo esta Ley por una entidad cubierta o proveedor de servicios puede entablar una acción civil contra dicha entidad en cualquier tribunal federal de jurisdicción competente*"[574].

En otras palabras, la disposición establece que cualquier persona o clase de personas puede presentar una acción civil contra una entidad cubierta o proveedor de servicios por una violación de la Ley o un reglamento promulgado bajo la Ley y que tal puede ser deducida en cualquier tribunal federal de jurisdicción competente[575]. Al respecto, vale mencionar, eso sí, que se establece el deber de notificación previa, en el sentido de que, antes de presentar una demanda, los demandantes deben notificar al Comisionado Federal de Comercio (FTC) y al fiscal general del estado en el que residen[576].

Otra cuestión relevante al respecto es que la acción civil se puede presentar por violaciones de secciones específicas de la Ley, como las prohibiciones en el procesamiento de información sensible, las obligaciones de consentimiento, la protección de datos de niños y adolescentes, y las violaciones de derechos civiles[577]. En la misma línea, se señala que la acción civil permite a los demandantes buscar la indemnización compensatoria de los daños sufridos, medidas cautelares, una sentencia declarativa y costos del litigio[578].

Adicionalmente, tal normativa establece, en la misma sección, ciertos casos en que el acuerdo de arbitraje previo a que se susciten conflictos es nulo en ciertos casos, como cuando se trata de una persona menor de 18 años o cuando se trate de reclamos relacionados con violencia de género o de pareja o daño físico[579].

---

[574] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.8152 - American Data Privacy and Protection Act.* Washington D.C., Estados Unidos, 21 de junio de 2022. Sección 403.
[575] *Ibíd*.
[576] *Ibíd*.
[577] *Ibíd*.
[578] *Ibíd*.
[579] *Ibíd*.

3. Transparencia[580]

Al analizar el alcance de los deberes de transparencia en los Capítulos anteriores, se mencionó que en nuestro ordenamiento existe un principio de transparencia que rige plenamente en el ámbito del derecho del consumo, y que a partir de él es posible entender que la transparencia algorítmica constituye un comportamiento exigible para los proveedores. También se explicó el importante rol que juega la transparencia en relación con el debido tratamiento de datos personales, así como en la prevención de la discriminación y ejercicio de influencias indebidas en la autonomía del consumidor.

No obstante, se señaló que la opacidad de la IA dificulta que el proveedor pueda transparentar completamente el funcionamiento de los algoritmos. Asimismo, aun cuando el deber de profesionalidad ayude a que ciertos incentivos problemáticos no se materialicen, es complejo dilucidar, a falta de norma que lo regule, qué tanto debe transparentar un proveedor profesional respecto de su tecnología. Una transparencia nula no ayuda; pero una transparencia completa puede resultar contraproducente.

En ese sentido, resultan ilustradores los deberes específicos de transparencia informativa que la normativa europea y la estadounidense imponen a los actores que utilizan sistemas de IA. En efecto, definen con precisión los alcances de la transparencia y tienen en cuenta diversos intereses en juego.

A fin de ordenar el análisis, habrá una sección en la que se examinarán las normas de transparencia de los intermediarios y otra en la que se hará referencia a las disposiciones aplicables a quienes ofrecen el bien o servicio directamente, distinguiendo, a su vez, entre lo previsto en la normativa europea y en la estadounidense. Para finalizar, se expondrán los límites que admite la transparencia en ambos regímenes.

[580] Se previene al lector que, atendido el objeto de estudio de la presente memoria, solo se examinarán las normas que consagren deberes de transparencia de cara a los consumidores o usuarios. No se ahondará en normas que consagren deberes de transparencia respecto de organismos públicos, salvo que ello tenga alguna incidencia directa en los derechos de los consumidores (como, por ejemplo, que los organismos deban crear registros de libre acceso con la información que les fue proporcionada).

a. Transparencia de los Intermediarios

Unión Europea

En cuanto a la regulación de los proveedores de servicios intermediarios, destacan el DSA, el DMA y el Reglamento 2019/1150 UE. Las tres normativas persiguen aumentar la transparencia en la moderación de contenidos y, sobre todo, en el uso de herramientas automatizadas. Una de las principales preocupaciones dice relación con los sistemas de recomendación y el fenómeno de la clasificación.

Un sistema de recomendación es "*un sistema total o parcialmente automatizado y utilizado por una plataforma en línea para proponer en su interfaz en línea información específica para los destinatarios del servicio o priorizar dicha información, también como consecuencia de una búsqueda iniciada por el destinatario del servicio, o que determine de otro modo el orden relativo o la relevancia de la información presentada*"[581].

Por su parte, la clasificación refiere a "*la preeminencia relativa atribuida a los bienes o servicios ofrecidos mediante servicios de intermediación en línea o la relevancia atribuida a los resultados de búsqueda a través de motores de búsqueda en línea, tal y como los proveedores de servicios de intermediación en línea o los proveedores de motores de búsqueda en línea, respectivamente, los presentan, organizan o comunican, con independencia de los medios tecnológicos empleados para tal presentación, organización o comunicación*"[582].

Respecto de los sistemas de recomendación, el artículo 27 del DSA consagra una serie de deberes mínimos de transparencia que deben observar los prestadores de plataformas en línea que los emplean. El apartado 1 refiere a la obligación de informar, dentro de sus condiciones generales, y empleando un lenguaje claro y comprensible, cuáles son los parámetros principales utilizados en los sistemas de recomendación, así como cualquier

[581] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022. Artículo 3.
[582] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Bruselas, Bélgica, 2019. Artículo 2.

opción a disposición de los usuarios para modificar o influir en dichos parámetros principales[583].

Seguidamente, el artículo precisa que los parámetros principales son aquellos que explican "*por qué se sugiere determinada información al destinatario del servicio*"[584], y deben incluir, como mínimo: "*a) los criterios más significativos a la hora de determinar la información sugerida al destinatario del servicio, y b) las razones de la importancia relativa de dichos parámetros*"[585].

Por último, el precepto establece que, si el sistema de recomendación cuenta con varias opciones que determinan el orden relativo de la información, los prestadores de plataformas en línea deberán habilitar una funcionalidad que, en forma accesible, directa y sencilla, permita al destinatario del servicio seleccionar qué opción quiere que le aplique, así como cambiar su decisión en cualquier momento[586]. Cabe destacar que, en el evento que quien emplea el sistema sea una plataforma en línea o motor de búsqueda de muy gran tamaño[587], deberá ofrecer al menos una opción para cada uno de sus sistemas de recomendación que no se base en la elaboración de perfiles[588].

En el mismo sentido, el artículo 6 del DMA prevé que el consumidor siempre tendrá la posibilidad de modificar con facilidad la configuración del sistema operativo cuando este lo dirija en forma preferente a los productos que recomienda el propio proveedor[589]. Tampoco se restringirá su capacidad para elegir libremente los bienes y servicios[590].

---

583 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022. Artículo 27.

584 *Ibíd*.

585 *Ibíd.*

586 *Ibíd.*

587 Según indica el artículo 33 DSA, son plataformas en línea y motores de búsqueda en línea de muy gran tamaño, aquellas que tengan un promedio mensual de destinatarios del servicio activos en la Unión igual o superior a cuarenta y cinco millones –valor sujeto a variación según el tamaño de la población–, así como las que designe la Comisión.

588 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022. Artículo 38.

589 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/1925 sobre mercados disputables y equitativos en el sector digital. Bruselas, Bélgica, 2022. Artículo 6.3.

590 *Ibid.* Artículo 6.6.

Por otra parte, en lo que atañe a la clasificación, el artículo 5 del Reglamento 2019/1150 UE indica que los proveedores intermediarios deben transparentar "l*os parámetros principales que rigen la clasificación y los motivos por los que aquellos cuentan con una importancia relativa superior a la de otros parámetros"*[591]. Es decir, se encuentran en la obligación de informar y motivar "*los criterios generales, procesos [y] señales específicas incorporadas en los algoritmos u otros mecanismos de ajuste o degradación que se utilicen en la clasificación*"[592]. El apartado segundo establece igual obligación para los proveedores de motores de búsqueda en línea, pero agrega que la comunicación debe ser de acceso fácil y comprensible y mantenerse actualizada[593].

Luego, el apartado 3 del precepto indica que, si los proveedores están abiertos a la posibilidad de que la calificación pueda verse influida por el pago de remuneraciones directas o indirectas de parte de empresas o usuarios, ello también debe transparentarse, precisando los efectos concretos que el pago surte en la clasificación[594]. Así, cuando el consumidor reciba o sugerencias personalizadas de compra, sabrá si es que los oferentes han pagado al proveedor para que esto suceda[595].

Adicionalmente, el artículo 7 del Reglamento prevé que los proveedores deben informar a los consumidores sobre los tratos diferenciados que den o puedan dar en relación a los bienes y productos que ofrecen, transparentando las "*consideraciones económicas, comerciales o jurídicas que fundamentan el trato diferenciado*"[596], así como los criterios de clasificación asociados y la eventual incidencia del pago de remuneraciones[597]. Esto tiene por

[591] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Bruselas, Bélgica, 2019. Artículo 5.

[592] *Ibíd*. Considerando 24.

[593] *Ibíd.* Artículo 5.

[594] *Ibíd.*

[595] ARGELICH-COMELLES, Cristina. 2023. *Deberes de transparencia del Reglamento 2019/1150 (P2B Regulation) para prevenir la discriminación algorítmica del consumidor en los sistemas de prelación de ofertas. (Ranking Transparency Guidelines in Platform-To-Business Regulation to Prevent Algorithmic Discrimination of Consumers).* [en línea] Cuadernos de Derecho Transnacional, 15(1): 129-135. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4434518> [consulta: 26 diciembre 2023]. p. 134.

[596] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Bruselas, Bélgica, 2019. Artículo 7.

[597] *Ibid*.

objetivo evitar discriminaciones arbitrarias y propender a una neutralidad en el proceso de clasificación[598].

Finalmente, el artículo 6.5 del DMA dispone que no se "*tratará más favorablemente, ni en la clasificación ni en las funciones relacionadas de indexado y rastreo, a los servicios y productos ofrecidos por el propio guardián de acceso que a los servicios o productos similares de terceros. El guardián de acceso aplicará condiciones transparentes, equitativas y no discriminatorias a dicha clasificación*"[599].

Como puede observarse, se contempla una regulación detallada respecto de la transparencia algorítmica en el contexto de las recomendaciones personalizadas que se presentan al consumidor. En su conjunto, estas normas no solo permiten que los consumidores tengan una mayor información, sino que también podrían volver menos probable vulneraciones a su autonomía –pues se les permite elegir qué opción de clasificación quieren que les aplique– y discriminaciones arbitrarias –al exponerse todas las consideraciones del trato que reciben–[600].

Amén de la regulación respecto de los sistemas de recomendación y la clasificación, la normativa europea contempla deberes de transparencia en la moderación de contenidos. Al respecto, el artículo 14 del DSA dispone que los proveedores intermediarios deberán informar públicamente, utilizando un lenguaje claro y sencillo, las restricciones, políticas, herramientas, procedimientos y medidas que emplean para moderar los contenidos de sus plataformas, incluyendo la toma de decisiones mediante algoritmos[601].

Adicionalmente, el artículo 15 del DSA indica que estos proveedores deberán publicar, al menos una vez al año, informes claros y fácilmente comprensibles sobre cualquier actividad

---

[598] BERGQVIST, Christian, *Discrimination and self-favoring in the digital economy*. Universidad de Copenhagen, 4 de febrero de 2020, p. 3.

[599] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/1925 sobre mercados disputables y equitativos en el sector digital. Bruselas, Bélgica, 2022. Artículo 6.5.

[600] Cabe destacar que una cuestión es que al proveedor se le exija fundar las decisiones automatizadas sin más, y otra cuestión –que es lo que consagra esta normativa– es que deba explicarlas a la luz de todos los antecedentes que ha transparentado sobre su sistema. En el segundo caso, su argumentación necesariamente deberá condecirse con todo aquello que ha transparentado; mientras que en el primero, más allá de lo que indiquen las palabras, no existe un mayor control sobre la racionalidad, mérito y verdad de la argumentación.

[601] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Bruselas, Bélgica, 2019. Artículo 14.

de moderación de contenidos que hayan realizado durante el período pertinente[602]. Dentro del contenido mínimo que debe contener el informe, destaca la:

> "[I]*nformación significativa y comprensible sobre la actividad de moderación de contenidos realizada por iniciativa propia del prestador, incluido el uso de herramientas automatizadas, las medidas adoptadas para proporcionar formación y asistencia a las personas encargadas de la moderación de contenidos, el número y el tipo de medidas adoptadas que afecten a la disponibilidad, visibilidad y accesibilidad de la información proporcionada por los destinatarios del servicio y a la capacidad de los destinatarios para proporcionar información a través del servicio, y otras restricciones conexas del servicio (...)*"[603].

Luego, el precepto dispone que, si se han empleado herramientas automatizadas en la moderación de contenidos, debe incluirse en el informe "*una descripción cualitativa, una especificación de los fines precisos, los indicadores de la precisión y la posible tasa de error de los medios automatizados empleados para cumplir dichos fines, y las salvaguardias aplicadas*"[604].

Si el proveedor intermediario es una plataforma en línea, el régimen de transparencia expuesto se complementa con lo previsto en los artículos 25 y 26 del DSA. El primer precepto indica que los prestadores del servicio "*no diseñarán, organizarán ni gestionarán sus interfaces en línea de manera que engañen o manipulen a los destinatarios del servicio o de manera que distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar decisiones libres e informadas*"[605]. Así, se consagra una prohibición de utilización de *dark patterns* con el fin de resguardar la autonomía de los usuarios[606].

---

602 *Ibíd*. Artículo 15.
603 *Ibíd*.
604 *Ibíd*.
605 *Ibíd*. Artículo. 25.1.
606 DOMÍNGUEZ, Ana Garriga. *Las exigencias de transparencia para los sistemas algorítmicos de recomendación, selección de contenidos y publicidad en línea en el nuevo Reglamento Europeo de Servicios Digitales.* Revista española de la transparencia (17):137-164, jul-2023. p. 155.

A la luz de los principios de transparencia y lealtad consagrados en el artículo 5.1 letra a) del Reglamento General de Protección de Datos personales[607], la utilización de *dark patterns* ya podía entenderse proscrita a propósito del tratamiento de datos personales[608]. Sin embargo, el artículo 25 DSA pretende reconocer que estos engaños pueden utilizarse para lesionar otros derechos del consumidor –como, por ejemplo, la autonomía–, de modo que se prohíbe su uso en todos los ámbitos[609].

Por otro lado, el artículo 26 consagra deberes de transparencia en la presentación de anuncios publicitarios, que exigen a las plataformas identificar, en forma clara, concisa e inequívoca, la persona en cuyo nombre se realiza el anuncio[610], así como informar los principales parámetros utilizados para determinar quién será el destinatario de la publicidad, y, en su caso, sobre cómo cambiar esos parámetros[611]. Dichos deberes "*responden a la necesidad de clarificar el funcionamiento opaco y, generalmente, poco comprensible de cómo se realiza esta clase de publicidad, de cómo se produce la focalización y la selección del momento en que esta se ofrece*"[612].

Adicionalmente, la norma proscribe la realización de anuncios que se basen en la elaboración de perfiles[613] si es que los datos personales que se tratan revelan "*el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical",* o corresponden a *"datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física*"[614]. Vale decir, se prohíbe la publicidad dirigida que

---

607 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Bruselas, Bélgica, 2016. Artículo 5.

608 *Ibíd*., pp. 155-156

609 *Ibíd*., pp. 155-156

610 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Bruselas, Bélgica, 2019. Artículo 26.

611 *Ibid.*

612 DOMÍNGUEZ, op. cit., p. 156.

613 Según el artículo 4.4 del RGPD, la elaboración de perfiles se define como "*toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*".

614 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Bruselas, Bélgica, 2016. Artículo 9.1. Remitido expresamente por el artículo 26 apartado 1, letra d) del DSA.

se realice atendiendo a ciertas condiciones, opiniones o aspectos sensibles de la vida del usuario.

En suma, la normativa europea prevé una regulación exhaustiva y delimitada respecto de los deberes de transparencia de los intermediarios, que trata materias relativas a los sistemas de recomendación, la moderación de contenidos, los *dark patterns*, la publicidad y la elaboración de perfiles. Estos deberes resultan aplicables aun cuando el producto o servicio no posee IA dentro de sus componentes, siempre y cuando se utilice IA o alguna tecnología automatizada para comercializarlos.

Lo destacable de las normas es que no solo precisan con claridad qué es exactamente lo que debe transparentar el intermediario, sino que lo hacen procurando resguardar los derechos de los consumidores. En efecto, (i) la regulación de los sistemas de recomendación y a la prohibición de *dark patterns* puede vincularse la protección de la autonomía; (ii) la regulación sobre publicidad y elaboración de perfiles, a la protección de la privacidad; y (iii) la regulación sobre tratos diferenciados y moderación de contenidos, a la protección de la integridad.

Estados Unidos

En el caso de Estados Unidos, las obligaciones de transparencia aplicables a los intermediarios se encuentran abordadas concretamente en dos propuestas normativas: la "*Digital Services Oversight and Safety Act of 2022*"[615] y la "*Algorithmic Justice and Online Platform Transparency Act*"[616].

Según indican los considerandos de la Algorithmic Justice and Online Platform Transparency Act, la necesidad de regular la transparencia de los intermediarios descansa en varias premisas que podríamos resumir de la siguiente forma: (i) las plataformas emplean *dark patterns* que permiten manipular a los usuarios, especialmente si ya han recopilado información sobre ellos; (ii) dichos dark patterns son combinados con el uso de algoritmos opacos, de manera que no resulta clara la forma en que se guía la conducta de los usuarios;

[615] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.6796 - Digital Services Oversight and Safety Act of 2022*. Washington D.C., Estados Unidos, 18 de febrero de 2022.
[616] CONGRESO de los Estados Unidos (Estados Unidos). *S.2325 - Algorithmic Justice and Online Platform Transparency Act.* Washington D.C., Estados Unidos, de 13 de julio de 2023.

(iii) es frecuente que los algoritmos utilizados por las plataformas no sean sometidos a pruebas y, por tanto, sean propensos a afectar derechos de los usuarios; y, (iv) es socialmente inaceptable que existan resultados lesivos sin poder conocer ni controlar la forma en que estos se producen[617].

Como consecuencia de lo anterior, la normativa propone obligar a los intermediarios a comunicar a los usuarios cierta información respecto del funcionamiento de los sistemas automatizados empleados, poniendo especial –mas no exclusivo– énfasis en aquellos que tengan como finalidad promocionar un contenido el usuario[618]. Al efecto, la sección 4.1 de la Algorithmic Justice and Online Platform Transparency Act establece que, respecto de cada proceso algorítmico que empleen, las plataformas en línea deberán informar en forma clara, accesible y no engañosa a los usuarios:

> "*(i) Las categorías de información personal que la plataforma en línea recopila o crea a propósito del tipo de proceso algorítmico.*
>
> *(ii) La manera en que la plataforma en línea recoge o crea dicha información personal.*
>
> *(iii) La forma en que la plataforma en línea utiliza dicha información personal en el tipo de proceso algorítmico.*
>
> *(iv) el método mediante el cual el tipo de proceso algorítmico da prioridad, asigna peso o clasifica diferentes categorías de información personal para retener, amplificar, recomendar o promover contenidos (incluido un grupo) a un usuario*"[619].

Adicionalmente, el intermediario deberá hacer llegar a las autoridades administrativas un registro que describa el tipo de información personal utilizada por el proceso algorítmico, el método que emplea para clasificar o ponderar la información y la forma en que se entrena el sistema –en especial, para cuidar que haya exactitud, imparcialidad y no se produzcan resultados arbitrariamente discriminatorios–[620]. Si bien este registro no es comunicado

---

[617] CONGRESO de los Estados Unidos (Estados Unidos). *S.2325 - Algorithmic Justice and Online Platform Transparency Act.* Washington D.C., Estados Unidos, de 13 de julio de 2023. Sección 2.
[618] DI PORTO, Fabiana., 2023. *Algorithmic disclosure rules.* Artificial Intelligence and Law, 31(1):13-51, noviembre 2023. p. 16.
[619] CONGRESO de los Estados Unidos (Estados Unidos). *S.2325 - Algorithmic Justice and Online Platform Transparency Act.* Washington D.C., Estados Unidos, de 13 de julio de 2023. Sección 4.1.
[620] *Ibíd.* Sección 4.2.

directamente a los consumidores, su contenido es bastante similar a aquello que se les informará obligatoriamente en virtud de la norma citada más arriba. De este modo, se permite que exista una "doble transparencia".

En cuanto a las actividades de moderación de contenidos que efectúe el intermediario, la normativa también prevé que deberá realizarse un reporte. Sin embargo, a diferencia del reporte sobre procesos algorítmicos, este será publicado en la plataforma y estará disponible abiertamente para el público, sin que se obligue al usuario a crear una cuenta para consultarlo[621].

En concreto, en relación con la materia que ahora nos convoca, es relevante considerar que el reporte, amén de detallar la intensidad con la que se moderaron los contenidos y la política implementada, deberá explicar si la moderación se produjo mediante prácticas automatizadas, trabajo humano por parte de la plataforma en línea, intervención por parte de cualquier persona que no trabaje como empleado remunerado de la plataforma en línea, o cualquier combinación de los mismos[622]. Vale decir, existe un deber de transparencia en orden a informar de la circunstancia de empleo de herramientas automatizadas en la moderación de contenidos.

En un sentido similar, la sección 6(a) de la *Digital Services Oversight and Safety Act of 2022* establece que todos los proveedores intermediarios que proporcionen servicios de alojamiento deberán dar aviso, dentro de sus normas comunitarias, sobre "*cualquier restricción que impongan con respecto a la información proporcionada por los usuarios del servicio, haciendo mención a cualquier política, procedimiento, medida o herramienta utilizada con fines de moderación de contenidos, incluyendo el uso toma de decisiones algorítmica y la revisión humana*"[623]. Toda esta información deberá estar en la plataforma del proveedor y ser de libre acceso al público, facilitándola en un lenguaje claro e inequívoco[624].

La sección 9 de la *Digital Services Oversight and Safety Act of 2022* agrega que, si la plataforma en cuestión es de gran tamaño y utiliza sistemas de recomendación para interactuar

[621] *Ibíd*. Sección 4.2 (ii).
[622] *Ibíd*. Sección 4.2 B.
[623] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.6796 - Digital Services Oversight and Safety Act of 2022*. Washington D.C., Estados Unidos, 18 de febrero de 2022. Traducción libre de sección 6(a).
[624] *Ibíd*. Sección 6.2.

con los usuarios, deberá, de conformidad con un Reglamento que dictará en el corto plazo Comisión Federal de Comercio, informar en sus términos y condiciones respecto de:

> *"(A) las características, entradas o parámetros más destacados utilizados por el sistema de recomendación;*
>
> *(B) cómo se recopila o infiere cualquier información personal utilizada por el sistema de recomendación sobre un usuario de la plataforma, y las categorías de dicha información (incluidas las categorías demográficas, de comportamiento y cualquier otra definida por la Comisión); y*
>
> *(C) cualquier opción que el proveedor ponga a disposición de un usuario de la plataforma para modificar el perfil del usuario o influir en las características, entradas o parámetros utilizados por el sistema de recomendación"*[625]*.*

En fin, es relevante tener presente que lo expuesto en esta sección corresponde a deberes de transparencia especiales con los que los proveedores intermediarios deben cumplir por el solo hecho de ser tales. Al igual como ocurre en la Unión Europea, los intermediarios se encuentran sometidos a un doble régimen: (i) deberes de transparencia generales, con los que debe cumplir toda entidad que utiliza sistemas automatizados que desarrollan procesos de decisión críticos (vale decir, las obligaciones expuestas al momento de analizar el régimen de los intermediarios); y (ii) deberes de transparencia especiales que resultan aplicables únicamente a los intermediarios.

En otras palabras, en la medida en que se cumplan los respectivos requisitos, los proveedores directos solo se encuentran sometidos al régimen de transparencia general que aplica a los procesos de decisión críticos; mientras que los proveedores intermediarios deben cumplir tanto con las obligaciones generales de dicho estatuto como con las obligaciones particulares que les sean exigibles por detentar la calidad de intermediario.

b. Transparencia de los Prestadores directos del bien o servicio

Unión Europea

[625] *Ibíd*. Sección 9(a).

Los deberes de transparencia de los proveedores que ofrecen directamente sus bienes o servicios se encuentran previstos, en su mayoría, en la Propuesta de Ley de Inteligencia Artificial (en adelante, "AI ACT"). Para estos efectos, el cuerpo normativo distingue entre sistemas de IA de alto riesgo y sistemas de IA que no son de alto riesgo[626].

De conformidad al artículo 6.1 de la AI ACT, los sistemas de IA de alto riesgo son los que están destinados a actuar como componente de seguridad de un producto, o constituyan en sí mismo un producto, de aquellos incluidos en el Anexo II de la normativa (máquinas, juguetes, embarcaciones, aviaciones, equipos radioeléctricos, instalaciones de transporte por cable, productos sanitarios, entre otros), siempre que, de conformidad a la legislación de armonización de la Unión Europea, deban someterse a una evaluación de conformidad por parte de un tercero antes de su introducción en el mercado o puesta en servicio[627].

Asimismo, el artículo 6.2 dispone que también se considerarán sistemas de alto riesgo aquellos previstos en el Anexo III de la normativa[628]. Dicho Anexo es esencialmente actualizable, y contiene un listado que enumera los ámbitos en el empleo de sistemas de IA ha derivado en la materialización de riesgos o existe un elevado consenso en orden a que se materialicen en un futuro próximo[629].

Por el momento, el Anexo III refiere a sistemas de IA destinados a utilizarse en: (i) identificación biométrica; (ii) gestión y funcionamiento de infraestructuras esenciales, como el agua y el gas; (iii) la determinación del acceso a centros educacionales y de formación profesional; (iv) contratación de personal y evaluación de rendimiento laboral; (v) calificación crediticia; (vi) envío o establecimiento de prioridades en el envío de servicios de primera intervención en situaciones de emergencia; (vii) aplicación de la ley, relacionada

[626] Esta distinción es un asunto que, como se explicará, debiese ser propiamente analizado en la sección de "Otros Controles en el uso de la IA", pero se estimó conveniente abordar el asunto en este apartado para explicar a quién le resulta aplicable la regulación de transparencia contenida en la AI ACT.

[627] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículo 6.1.

[628] *Ibid.* Artículo 6.2.

[629] CASADO, Eduardo. *El enfoque europeo de Inteligencia Artificial.* [en línea] Revista de Derecho Administrativo, 2021, n° 20, p. 268-289 <https://dialnet.unirioja.es/servlet/articulo?codigo=8510535> [consulta: 09 octubre 2023]. p. 279.

principalmente al ámbito penal y a la obtención o evaluación de pruebas; (ix) gestión de la migración, asilo y control fronterizo; y (x) asistencia en la administración de justicia[630].

Respecto de la transparencia de los sistemas de IA de alto riesgo, se distingue entre información que debe ser difundida al público en general en plataformas de libre acceso, e información que es comunicada directamente al consumidor o destinatario que utilizará o interactuará con la IA[631].

En cuanto a la información a difundir, el artículo 51 de la AI ACT prevé que los sistemas de alto riesgo a los que alude el artículo 6.2 deben inscribirse en un registro[632], que dará lugar a una base de datos de libre acceso para el público[633]. En esta base habrá información relativa a la identificación del sistema, su finalidad prevista, su situación en el mercado (comercializado, puesto en servicio, etc.), autorizaciones administrativas e instrucciones de uso electrónicas[634].

A su vez, en cuanto a la información que se transparentará directamente al destinatario –y que aplica para todos los sistemas de IA de alto riesgo–, el artículo 13 de la AI ACT dispone que:

> "*1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de un modo que garantice que funcionan con un nivel de transparencia suficiente para que los usuarios interpreten y usen correctamente su información de salida. Se garantizará un tipo y un nivel de transparencia adecuados para que el usuario y el proveedor cumplan las obligaciones oportunas previstas en el capítulo 3 del presente título.*

630 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Anexo III.

631 HUESO, Lorenzo. Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida. [en línea] Revista española de la transparencia, n°. 16, p. 17-63 <https://dialnet.unirioja.es/servlet/articulo?codigo=8913030> [consulta: 23 noviembre 2023]. pp. 39-40.

632 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículo 51.

633 *Ibíd.* Artículo 60.3.

634 *Ibíd*., p.16. Anexo VIII. Cabe prevenir, sin embargo, que las instrucciones de uso electrónicas no serán públicas cuando sistemas de IA de alto riesgo de los que se trata, sean operativos en los ámbitos de la aplicación de la ley y la gestión de la migración, el asilo y el control fronterizo a que se refiere el Anexo III, puntos 1, 6 y 7.

2. Los sistemas de IA de alto riesgo irán acompañados de las instrucciones de uso correspondientes en un formato digital o de otro tipo adecuado, las cuales incluirán información concisa, completa, correcta y clara que sea pertinente, accesible y comprensible para los usuarios.

3. La información a que se refiere el apartado 2 especificará:

a) la identidad y los datos de contacto del proveedor y, en su caso, de su representante autorizado;

b) las características, capacidades y limitaciones del funcionamiento del sistema de IA de alto riesgo, y en particular:

i) su finalidad prevista;

ii) el nivel de precisión, solidez y ciberseguridad mencionado en el artículo 15 con respecto al cual se haya probado y validado el sistema de IA de alto riesgo y que puede esperarse de este, así como las circunstancias conocidas o previsibles que podrían afectar al nivel de precisión, solidez y ciberseguridad esperado;

iii) cualquier circunstancia conocida o previsible, asociada a la utilización del sistema de IA de alto riesgo conforme a su finalidad prevista o a un uso indebido razonablemente previsible, que pueda dar lugar a riesgos para la salud y la seguridad o los derechos fundamentales;

iv) su funcionamiento en relación con las personas o los grupos de personas en relación con los que se pretenda utilizar el sistema;

v) cuando proceda, especificaciones relativas a los datos de entrada, o cualquier otra información pertinente en relación con los conjuntos de datos de entrenamiento, validación y prueba usados, teniendo en cuenta la finalidad prevista del sistema de IA;

c) los cambios en el sistema de IA de alto riesgo y su funcionamiento predeterminados por el proveedor en el momento de efectuar la evaluación de la conformidad inicial, en su caso;

d) las medidas de vigilancia humana a que se hace referencia en el artículo 14, incluidas las medidas técnicas establecidas para facilitar la interpretación de la información de salida de los sistemas de IA por parte de los usuarios;

e) la vida útil prevista del sistema de IA de alto riesgo, así como las medidas de mantenimiento y cuidado necesarias para garantizar el correcto

funcionamiento de dicho sistema, también en lo que respecta a la actualización del software"[635].

Dentro del precepto, destaca la transparencia en el diseño de la tecnología misma, así como el deber de informar sobre sus características, capacidades, finalidades, limitaciones, riesgos, nivel de precisión, funcionamiento, datos usados (de entrenamiento, validación y prueba), medidas de vigilancia humana y vida útil.

Pese a que el artículo consagra un deber de transparencia amplio y delimitado, la doctrina ha advertido que resulta problemático que no se explique cuándo se entenderá que la tecnología fue diseñada con una "transparencia suficiente" ni quién decidirá si esta efectivamente permite a los usuarios "interpretar y usar correctamente" la información de salida[636]. Asimismo, se ha criticado que no imponga expresamente la obligación de difundir el proceso lógico mediante el que el sistema llega a los resultados[637]. Ahora bien, ambas críticas pueden ser rebatidas al menos parcialmente.

En cuanto a la no precisión de cuándo se entiende que la tecnología fue diseñada con una transparencia suficiente, la respuesta a ello se halla en el artículo 14 del mismo cuerpo normativo. Este precepto indica, en lo que ahora interesa, que "[*l]os sistemas de IA de alto riesgo deben diseñarse y desarrollarse de tal modo que su funcionamiento pueda ser vigilado por personas físicas*"[638]. Una interpretación coherente de las dos normas lleva a concluir que la tecnología habrá sido diseñada con la transparencia adecuada siempre que permita que su funcionamiento sea vigilado por personas físicas –y justamente esta vigilancia es lo que permite comprobarlo–.

En este sentido, se da una buena solución al problema de que los proveedores no sean capaces de transparentar el sistema. Al final del Capítulo anterior, se mencionó que cabe la

---

635 *Ibíd*. Artículo 13.

636 VAROŠANEC, Ida. *On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI*. [en línea] International Review of Law, Computers & Technology, 08 de abril de 2022, Vol. 36, n° 2 <https://www.tandfonline.com/doi/full/10.1080/13600869.2022.2060471> [consult: 17 noviembre 2023]. p. 103.

637 CASADO, Eduardo. *El enfoque europeo de Inteligencia Artificial.* [en línea] Revista de Derecho Administrativo, 2021, n° 20, p. 268-289 <https://dialnet.unirioja.es/servlet/articulo?codigo=8510535> [consulta: 09 octubre 2023]. p. 282.

638 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículo 14.1.

posibilidad de que los sistemas de IA sean tan complejos que el proveedor simplemente no pueda transparentarlos. Pues bien, acá, para evitar ese problema, se opta por una transparencia por diseño. En otras palabras, se hace frente al problema de la no explicación por la vía de asegurarse que no exista sistema que no pueda ser entendido por un humano a cargo.

En cuanto a la crítica de que la norma no imponga expresamente la obligación de difundir el proceso lógico mediante el que el sistema llega a los resultados, podría contra argumentarse que ello viene implícito en la parte que señala que debe informarse acerca de las características del funcionamiento. Pero es cierto que se presta para dudas.

Por otro lado, en lo que atañe a los sistemas de IA que no son de alto riesgo –vale decir, todos los que no encajen en los criterios a los que alude el artículo 6– , estos quedan sometidos a la adopción voluntaria de códigos de conducta por parte de sus operadores[639], sin que exista, por regla general, una obligación de transparencia a su respecto. En efecto, la AI ACT adopta un enfoque basado en el riesgo[640], que se caracteriza por prohíbir los sistemas de IA de riesgo "intolerable"[641], regular profusamente los sistemas de IA de alto riesgo y dar espacio a la autorregulación respecto de todos los otros sistemas.

En materia de transparencia, conviene, con todo, efectuar dos precisiones. En primer lugar, existe otra disposición que consagra pequeños deberes de transparencia que eventualmente también pueden ser extensibles a los operadores de sistemas de IA de bajo riesgo. Se trata del artículo 52 de la AI Act, que indica que todo proveedor que emplee sistemas de IA destinados a interactuar con personas físicas, debe informar a dichas personas respecto de la circunstancia de que están interactuando con un sistema de IA, salvo que ello resulte evidente atendido el contexto de la utilización[642].

---

639 *Ibíd.* Artículo 69.

640 CASADO, Eduardo. *El enfoque europeo de Inteligencia Artificial.* [en línea] Revista de Derecho Administrativo, 2021, n° 20, p. 268-289 <https://dialnet.unirioja.es/servlet/articulo?codigo=8510535> [consulta: 09 octubre 2023]. pp. 277-278.

641 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículo 5.

642 *Ibíd.* Artículo 52.1.

Adicionalmente, el precepto prevé que el proveedor deberá informar el funcionamiento de los sistemas de reconocimiento de emociones o categorización biométrica a las personas físicas que a él se expongan, a menos que exista autorización legal para utilizarlo en el contexto de investigaciones penales[643]. También, en el evento de que el sistema de IA genere contenido que se asemeje a personas, sonidos, imágenes o videos reales, y que pueda inducir al destinatario a pensar que el contenido es auténtico, el operador deberá informar que ha sido generado artificialmente –salvo autorización en contexto penal o que no comunicarlo resulte necesario para el ejercicio de ciertas garantías fundamentales–[644].

En segundo lugar, cabe precisar que, aun cuando la AI Act no establezca mayores deberes de transparencia respecto de los sistemas de IA de bajo riesgo, existe otra normativa que complementa el régimen de transparencia estudiado, y resulta aplicable a todos los sistemas de IA –sin importar el nivel de riesgo– que se empleen en el contexto de las relaciones de consumo.

La normativa en cuestión es la Directiva 2011/83 UE sobre derechos de los consumidores, que, luego de las reformas introducidas por la Directiva 2019/2161 UE –relativa a la modernización de las normas de protección de los consumidores de la Unión–, posee algunas disposiciones pertinentes sobre la materia.

Una de ellas es el artículo 5, que indica que, antes de que el consumidor quede vinculado por un contrato distinto de un contrato a distancia o uno celebrado fuera del establecimiento (esto es, por un contrato presencial[645]), deberá informarle en forma clara y comprensible, entre otras cosas, la funcionalidad, el contenido y las medidas de protección técnica de los bienes con elementos digitales y los servicios digitales[646], así como "*toda compatibilidad e interoperatividad pertinente de los bienes con elementos digitales, el contenido digital y los servicios digitales conocidos por el comerciante o que quepa esperar razonablemente que este pueda conocer*"[647].

---

643 *Ibíd.* Artículo 52.2.
644 *Ibíd.* Artículo 52.3.
645 Así se aclara en la Comunicación de la Comisión Europea "Directrices sobre la interpretación y la aplicación de la Directiva 2011/83/UE del Parlamento Europeo y del Consejo sobre los derechos de los consumidores".
646 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo. Bruselas, Bélgica, 2011. Artículo 5 letra g).
647 *Ibíd*. Artículo 5 letra h).

Otra disposición que resulta pertinente es el artículo 6, que regula los deberes de información previos a la celebración de un contrato a distancia o que tenga lugar fuera del establecimiento del comerciante. El precepto replica lo señalado respecto del artículo 5, pero agrega que, si el proveedor ha personalizado el precio del bien o servicio ofrecido basándose en la toma de decisiones automatizada, deberá informarle de ello al consumidor[648].

En fin, es interesante destacar que, para efectos de delimitar el ámbito de aplicación de la Directiva 2011/83 UE, se prevé que sus disposiciones no solo regirán en los contratos en que el consumidor pague al proveedor un precio por un bien o servicio ofrecido, sino también cuando el proveedor suministre o se comprometa a suministrar contenido digital que no se preste en un soporte material o un servicio digital al consumidor, y este último, por su parte, facilite o se comprometa a facilitar datos personales al proveedor[649]. De este modo, los deberes de transparencia consagrados en materia de consumo se hacen extensibles a los clientes potenciales.

Como puede observarse, las obligaciones de transparencia aplican un criterio de proporcionalidad, en el sentido de que se prevén deberes de información específicos que resultan aplicables únicamente si el riesgo del sistema de IA empleado lo amerita. En cualquier caso, los deberes de transparencia de los proveedores de alto riesgo que prestan el bien o servicio directamente siguen siendo menores que los de los intermediarios, en el entendido de que estos últimos transparentan bastante aun cuando el riesgo del sistema utilizado sea bajo –sin perjuicio de que, si llegase a ser de alto riesgo, los deberes debiesen ser complementados con lo analizado en esta sección–.

Estados Unidos

Al igual que en la Unión Europea, en Estados Unidos se ha propuesto normativa que consagra diversos deberes de transparencia aplicables a los proveedores que emplean IA. Ahora bien, antes de ahondar en los preceptos que contienen obligaciones de transparencia, conviene advertir que la justificación o el enfoque que se le ha dado a esta materia es diverso al adoptado por la Unión Europea.

[648] *Ibíd.* Artículo 6 letra e) bis.
[649] *Ibíd.* Artículo 3.1 bis.

En efecto, mientras en la Unión Europea las obligaciones de transparencia resultan aplicables únicamente a los sistemas de IA de alto riesgo (dejando de lado las hipótesis de los intermediarios), en Estados Unidos, por regla general –dependiendo del tamaño del proveedor–, el objeto del régimen son los sistemas de decisión automatizados que realicen "procesos de decisión críticos", con total independencia del riesgo asociado a la tecnología utilizada[650].

Según prevé la sección 2.8 de la "Algorithmic Accountability Act of 2023", una "decisión crítica" es toda decisión o sentencia que tenga cualquier efecto legal, material o de importancia significativa en la vida de un consumidor en relación con el acceso, el coste, las condiciones o la disponibilidad de: (i) la educación y formación profesional; (ii) el empleo o gestión de trabajadores; (iii) los servicios públicos esenciales; (iv) la planificación familiar; (v) los servicios financieros; (vi) la asistencia sanitaria; (vii) el alojamiento o vivienda; (ix) los servicios jurídicos; (x); o, cualquier otro servicios, programa u oportunidad que sea objeto de decisiones que tengan un efecto significativo similar en la vida del consumidor[651].

De este modo, el foco no radica en el riesgo potencial abstracto que posea el sistema de IA, sino en las repercusiones significativas que las decisiones automatizadas puedan tener en la vida de los consumidores. Si bien pareciera ser una diferencia sutil, posee al menos dos repercusiones significativas.

En primer lugar, la regulación estadounidense evita la "cuestión ontológica" de determinar qué es un sistema de IA y, en su lugar, atiende a una circunstancia de hecho: el grado de automatización en los procesos decisorios[652]. Ello resulta relevante si se tiene en cuenta que las definiciones de IA no son uniformes y pueden ir evolucionando con el tiempo. Así, el entender que el objeto de la regulación son las decisiones automatizadas –con

[650] MÖKANDER, J., JUNEJA, P., WATSON, D.S. y FLORIDI, L., 2022. *The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other?* [en línea] Minds and Machines, Agosto-2022, Vol. 32, n°. 4 <https://link.springer.com/article/10.1007/s11023-022-09612-y> [consulta: 18 octubre 2023]. pp. 752-753.

[651] CONGRESO de los Estados Unidos (Estados Unidos). *H.R. 5628 - Algorithmic Accountability Act of 2023.* Washington D.C., Estados Unidos, 21 de septiembre de 2023. Sección 2.8

[652] MÖKANDER, J., JUNEJA, P., WATSON, D.S. y FLORIDI, L., 2022. *The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other?* [en línea] Minds and Machines, Agosto-2022, Vol. 32, n°. 4 <https://link.springer.com/article/10.1007/s11023-022-09612-y> [consulta: 18 octubre 2023]. p. 753.

independencia de la tecnología a la que estén asociadas–, otorga una gran amplitud y permite que la normativa no quede inutilizada ante los eventuales desarrollos futuros[653].

En segundo lugar, lo que justifica la transparencia ya no es el riesgo abstracto que la tecnología pueda suponer en relación con el uso predestinado por el proveedor, sino los peligros concretos que se producen en el bienestar de los consumidores. Lo anterior implica atender a los derechos de los consumidores para efectos de determinar si resultan aplicables los deberes de transparencia, lo que para el espíritu de esta investigación es algo positivo. Asimismo, se permite que sean tenidas en cuenta situaciones en las que, si bien la decisión no fue tomada directamente por la IA, se utilizaron sistemas automatizados para apoyarlas, y a raíz de ese respaldo se llevó a cabo un acto humano que dañó a los consumidores[654].

Con todo, debe tenerse presente que estas obligaciones solo resultan aplicables a las grandes empresas. Se entiende por grandes empresas o "entidades cubiertas" aquellas que: (a) tengan un volumen de negocios anual superior a 50 millones de dólares, (b) tengan más de 250 millones de dólares de valor patrimonial, o (c) procesen la información de más de 1 millón de usuarios[655].

Esto último puede resultar criticable, por cuanto hay procesos de decisión críticos que, no obstante representar una enorme amenaza para los derechos de los consumidores, quedarán exentos de regulación por el solo hecho de no ser utilizados por una empresa grande. La doctrina ha señalado que es razonable excluir a las empresas PYME del régimen de transparencia, pero no limitarlo únicamente a empresas de enorme envergadura económica. Lo deseable sería un punto medio[656].

Pues bien, ya aclarado el ámbito de aplicación, se examinarán los deberes de transparencia específicos que prevé la normativa. En tal sentido, un primer aspecto interesante se encuentra en la sección 4 de la Algorithmic Accountability Act of 2023. Esta sección

---

653 *Ibíd.*, p. 753.

654 *Ibíd*., p. 753.

655 CONGRESO de los Estados Unidos (Estados Unidos). *H.R. 5628 - Algorithmic Accountability Act of 2023*, 21 de septiembre de 2023. Sección 2.7.

656 MÖKANDER, J., JUNEJA, P., WATSON, D.S. y FLORIDI, L., 2022. The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other? [en línea] Minds and Machines, Agosto-2022, Vol. 32, n°. 4 <https://link.springer.com/article/10.1007/s11023-022-09612-y> [consulta: 18 octubre 2023]. p. 754.

contempla deberes de evaluación de riesgos, por lo que será examinada más en detalle en la sección sobre “Otros controles en el uso de la IA”. Sin embargo, en lo que ahora interesa, en su numeral octavo indica que, al momento de evaluar los riesgos que puede ocasionar un sistema de decisión automatizada respecto de los derechos de los consumidores, deberá tenerse en cuenta:

> *“*[L]*a transparencia y explicabilidad de dicho sistema o proceso y en qué medida un consumidor puede impugnar, corregir o apelar una decisión u optar por no participar en dicho sistema o proceso, lo que incluye:*
>
> *(i) la información disponible para los consumidores o representantes o agentes de los consumidores sobre el sistema o proceso, como cualquier factor relevante que contribuya a una decisión concreta, incluida una explicación de qué factores contribuyentes, si se modificaran, harían que el sistema o proceso tomara una decisión diferente, y cómo puede acceder a dicha información dicho consumidor, representante o agente;*
>
> *(ii) documentación de cualquier reclamación, litigio, corrección, recurso o solicitud de exclusión voluntaria presentada a la entidad cubierta por un consumidor en relación con dicho sistema o proceso; y*
>
> *(iii) el proceso y el resultado de cualquier medida correctiva adoptada por la entidad cubierta para abordar las preocupaciones o los perjuicios de los consumidores*"[657].

Vale decir, la transparencia juega un rol fundamental al momento de evaluar qué tan riesgoso puede ser un sistema para los derechos de los consumidores, en el entendido de que, entre menos datos, explicaciones, libertades y antecedentes se tengan respecto del funcionamiento del sistema, más opaco será y hay mayores posibilidades de que su uso redunde en perjuicios para los consumidores.

Adicionalmente, la sección 5.1 de la Algorithmic Accountability Act of 2023 obliga a los proveedores que emplean IA, en la medida en que sean entidades cubiertas que trabajen con procesos de decisión críticos, a entregar a la Comisión Federal de Comercio (agencia

[657] CONGRESO de los Estados Unidos (Estados Unidos). *H.R. 5628 - Algorithmic Accountability Act of 2023*, 21 de septiembre de 2023. Sección 4.8 B.

norteamericana que protege los derechos de los consumidores y defiende la libre competencia) informes resumidos que refieran a aspectos como:

> *(i) la descripción de la decisión crítica; (ii) la finalidad prevista del sistema automatizado; (iii) los métodos y métricas que emplea el sistema en sus entrenamientos; (iv) la descripción de cuándo se está ante un rendimiento satisfactorio; (v) las limitaciones de uso del sistema; (vi) la declaración de si aplican o no medidas de transparencia y explicabilidad, y, en la afirmativa, cuáles; (vii) las posibles repercusiones negativas del sistema, así como las medidas que se utilizan para mitigarlas; (viii) los posibles riesgos para los consumidores; (ix) los protocolos de seguridad implementados; y (x) los aspectos que, según las evaluaciones de impacto, se han detectado como necesarios o beneficios para mejorar el rendimiento del sistema*[658].

Ahora bien, para efectos de analizar la transparencia de cara a los consumidores, lo interesante no es el hecho de que tal información deba ser entregada a un órgano administrativo, sino que la Comisión Federal de Comercio debe generar un registro de acceso público que contenga la información de los reportes en forma agregada y anonimizada[659].

Este repositorio de libre acceso deberá contener un subconjunto limitado de información sobre cada sistema automatizado de decisión y proceso de decisión crítico respecto de los que se haya recibido reportes[660]. Según indica la misma normativa, ello posee tres objetivos: (i) informar a los consumidores sobre el uso de sistemas de decisión automatizados y los procesos de decisión crítica; (ii) permitir a investigadores estudiar sobre la materia; y (iii) garantizar el cumplimiento de los requisitos de la Ley[661].

Empero, como puede advertirse, los consumidores solo tienen acceso a un conjunto restringido de información, y no a la totalidad de las estadísticas que fueron reportadas a la autoridad. Sobre el particular, la doctrina ha observado que la información que se pone a disposición pública se limita a posibilitar que las personas adquieran conocimiento de la

---

[658] *Ibíd*., sección 5.1
[659] *Ibíd*., sección 6(a).
[660] *Ibíd*., sección 6(b), numeral (i).
[661] *Ibíd*., sección 6B

existencia del sistema de recomendación y sobre cómo usarlo, mas no existe una transparencia real que les permita dimensionar los riesgos del sistema ni saber si han sido objeto de vulneración en alguno de sus derechos[662].

Ello resulta extraño si se tiene en cuenta que en una orden ejecutiva del año 2020, denominada "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government. Executive Order 13960, 2020", se había enfatizado en la necesidad de que los operadores sean transparentes "*a la hora de revelar la información pertinente sobre el uso que hacen de la IA a las partes interesadas, incluidos el Congreso y el público* (...)"[663].

En un mismo sentido, la "*Bipartisan Framework on AI Legislation*" –que se propuso el presente año–, indica que el Congreso debe promover los derechos de los consumidores exigiendo transparencia a las empresas que desarrollen y empleen sistemas de IA. También debe garantizar que la revelación de los datos de entrenamiento, las limitaciones, la precisión y la seguridad de los modelos empleados se comunique en forma directa a los usuarios, haciendo uso de un lenguaje sencillo y comprensible[664].

Con todo, desafortunadamente, más allá de los criterios interpretativos que puedan surgir a propósito de las directrices planteadas anteriormente, por el momento no es posible solucionar las deficiencias del régimen de transparencia aplicable a los prestadores directos que utilizan IA, toda vez que las únicas normativas federales adicionales que proponen o consagran deberes específicos de transparencia ("*Algorithmic Justice and Online Platform Transparency Act*"[665] y "*Digital Services Oversight and Safety Act of 2022*[666]") solo aplican para plataformas o intermediarios que moderan contenidos.

---

662 GURSOY, F., KENNEDY, R. y KAKADIARIS, I. *A critical assessment of the algorithmic accountability act of 2022.* [en línea] Available at SSRN 4193199 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4193199> [consulta: 14 noviembre 2023]. p. 6.

663 PRESIDENTE de Los Estados Unidos (Estados Unidos). *Executive Order N° 13.960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, 03 de diciembre de 2020. Sección 3 (h).

664 Senadores Richard Blumenthal & Josh Hawley (Estados Unidos), *Bipartisan Framework on Artificial Intelligence Legislation*, 08 de septiembre de 2023.

665 CONGRESO de los Estados Unidos (Estados Unidos). *S.2325 - Algorithmic Justice and Online Platform Transparency Act.* Washington D.C., Estados Unidos, de 13 de julio de 2023.

666 CONGRESO de los Estados Unidos (Estados Unidos). *H.R.6796 - Digital Services Oversight and Safety Act of 2022*. Washington D.C., Estados Unidos, 18 de febrero de 2022.

El problema tampoco es salvado por la Orden Ejecutiva del 30 de octubre del 2023 ("*Safe, Secure, and Trustworthy Artificial Intelligence. Executive Order 14.110*, 2023").[667]. En efecto, si bien esta normativa reconoce expresamente, en su sección 8, que los consumidores son un grupo digno de protección y que es importante que haya transparencia en los sistemas de IA, no hace más que "invitar a las agencias reguladoras independientes, cuando lo estimen oportuno", a hacer frente a los riesgos que se presenten para los consumidores y autoimponerse deberes de transparencia[668].

Desde luego, parece poco realista asumir que los proveedores aceptarán la "invitación a estimar oportuno" aplicar deberes de transparencia si no existe una obligatoriedad mínima en ese sentido. Sin perjuicio de ello, no es correcto indicar que ninguna normativa estadounidense –además de la Algorithmic Accountability Act– se preocupe por la transparencia. Tanto la Orden Ejecutiva del 30 de octubre como la "Transparent Automated Governance Act (2023)"[669] hacen alusión a la transparencia y establecen obligaciones. El problema es que no lo hacen de cara a los consumidores o del público en general, sino con el objeto de que el proveedor trate de desarrollar sistemas transparentes.

En otras palabras, en lugar de establecer obligaciones de transparencia en favor de los consumidores, se busca facilitar guías a los proveedores para que desarrollen y trabajen con tecnologías automatizadas que son transparentes por diseño; pero, una vez que ya utilizan sistemas transparentes, no fijan ninguna obligación específica en orden a que el proveedor deba comunicar o explicar datos sobre el sistema y su funcionamiento a los consumidores[670].

c. Límites a la transparencia

Con la expresión "límites a la transparencia", se alude a aquellos aspectos o datos de la IA que el proveedor no está obligado a comunicar. En ese sentido, atendido que ambas regulaciones se encargan de delimitar con precisión qué es lo que debe informar el proveedor,

[667] PRESIDENTE de los Estados Unidos (Estados Unidos). *Executive Order N° 14.110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 de octubre de 2023.
[668] *Ibíd*. Sección 8.
[669] *Ibíd*.
[670] Sobre este punto, resultan particularmente ilustrativas las secciones 3 y 4 de la Transparent Automated Governance Act (2023), que establecen "orientaciones o guías transparentes sobre gobernanza automatizada". Algo similar ocurre con la sección 4 de la Executive Order 14110, 2023,

un primer límite a la transparencia podemos hallarlo en forma indirecta: no existirá obligación de informar aquello que excede las hipótesis previstas en la normativa.

Así, por ejemplo, en la Unión Europea, un proveedor no intermediario que emplea un sistema de IA de bajo riesgo que no cabe en las hipótesis del artículo 52 de la AI Act, no deberá informar las características, las capacidades, las limitaciones, el funcionamiento, la finalidad ni los datos de entrenamiento de la tecnología empleada, pues no existe norma que lo obligue.

Sin perjuicio de ello, ambas normativas también contemplan límites a la transparencia que podríamos denominar como directos o extrínsecos, en tanto no son desprendidos a *contrario sensu* de la lectura de las causales, sino que se encuentran consagrados expresamente en la normativa. Se trata de motivos que eventualmente podrían justificar la reserva parcial o total de determinados antecedentes en pos de proteger otros intereses, aun habiéndose verificado un supuesto de hecho que da lugar a las obligaciones de transparencia.

Unión Europea

En el caso de la Unión Europea, los límites directos a la transparencia dicen relación con la confidencialidad de la información, la protección de derechos fundamentales y el bienestar de los consumidores. Así, por ejemplo, respecto de los deberes de transparencia previstos en la AI ACT, el artículo 70 señala que las autoridades y organismos respetarán la confidencialidad de los datos, asegurándose de que no se divulgue información que: (i) sea relativa a derechos de propiedad intelectual, confidencial empresarial o secretos comerciales; (ii) refiera procedimientos penales o administrativos; o (iii) pueda comprometer los intereses públicos o la seguridad nacional[671].

En un sentido similar, el artículo 14.4 del DSA establece que el cumplimiento de los deberes de transparencia en la moderación de contenidos debe verificarse sin transgredir "*los derechos e intereses legítimos de todas las partes implicadas, incluidos los derechos fundamentales de los destinatarios del servicio, como la libertad de expresión, la libertad y el*

[671] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículo 70.2.

pluralismo de los medios de comunicación y otros derechos y libertades fundamentales amparados por la Carta"[672].

Por su parte, a propósito de la transparencia algorítmica a la que están obligados los proveedores intermediarios, el artículo 5.6 del Reglamento 2019/1150 UE dispone que, para dar cumplimiento a ello, en caso alguno se exigirá a los proveedores revelar: (i) "*algoritmos o información que, dentro de un grado de certeza razonable, podría inducir a error a los consumidores o causarles un perjuicio mediante la manipulación de los resultados de las búsqueda*"[673]; (ii) información amparada por lo previsto en Directiva (UE) 2016/943, vale decir, secretos comerciales[674].

Si bien es criticable que esta última norma no precise ni entregue ejemplos sobre cuándo la revelación de algoritmos o información podría inducir razonablemente a error a los consumidores, en principio parece bien que se reconozca que una transparencia desmedida podría perjudicarlos. Además, el problema es salvado por la posterior Comunicación de la Comisión Europea sobre el Reglamento, que indica que:

> "[U]*n exceso de información no tiene por qué ser, en efecto, sinónimo de información importante para los usuarios. En consecuencia, los proveedores deben, por un lado, determinar y explicar adecuadamente los parámetros de clasificación principales y, por otro, no abrumar a los usuarios con descripciones largas o complicadas, o descripciones de parámetros distintos de los principales. El no suministrar demasiados detalles también debe ayudar a evitar el riesgo de inducir a error a los consumidores o causarles un perjuicio*"[675].

---

[672] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022. Artículo 14.4.

[673] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Bruselas, Bélgica, 2019. Artículo 5.6.

[674] *Ibíd*. Sobre este punto, cabe destacar que se ha sostenido que los secretos comerciales deben serlo en sentido estricto –es decir, que sean totalmente subsumibles en alguna de las hipótesis del artículo 2 de la Directiva–, sin que baste, por ejemplo, que la empresa argumente que nunca han revelado ninguno de sus parámetros o que la información en cuestión es delicada a efectos comerciales. Véase COMUNICACIÓN DE LA COMISIÓN Directrices sobre la transparencia de la clasificación con arreglo al Reglamento (EU) 2019/1150 del Parlamento Europeo y del Consejo, p. 14, considerando 82.

[675] COMUNICACIÓN DE LA COMISIÓN Directrices sobre la transparencia de la clasificación con arreglo al Reglamento (EU) 2019/1150 del Parlamento Europeo y del Consejo, p. 5. Considerando 25.

A ello se agrega la posibilidad de que los parámetros de clasificación hayan sido manipulados de mala fe por parte de terceros, en cuyo caso la revelación no solo podría frustrar la capacidad de actuación del proveedor, sino también dar percepciones equívocas al consumidor[676]. En tal sentido, la norma busca lograr un equilibrio entre el combate de conductas manipulativas, la transparencia y el bienestar de los consumidores[677]. El desafío que queda pendiente es generar criterios uniformes sobre la materia.

Estados Unidos

Los proyectos normativos de Estados Unidos también prevén "límites directos" a la transparencia. Al efecto, resulta importante la sección 6.3 de la *Digital Services Oversight and Safety Act of 2022,* que indica que la Comisión Federal de Comercio se asegurará de que el cumplimiento de la obligación de los proveedores en orden a elaborar informes o dar a conocer las condiciones generales de sus sistemas automatizados, no redunde en una vulneración de derechos o legítimos intereses de los propios proveedores ni de los usuarios de los servicios de alojamiento[678]. En ese sentido –indica–, se debe resguardar especialmente la protección de la información personal, la protección de la información confidencial y el mantenimiento de la seguridad de dichos servicios[679].

Por su parte, la Orden Ejecutiva sobre el Desarrollo y Uso Seguro y Confiable de la IA , de 30 de octubre de 2023, establece diversos resguardos para evitar que con ocasión del uso de IA o del cumplimiento de deberes asociados al empleo de sistemas automatizados, se transgredan derechos relacionados a la propiedad intelectual[680].

Como puede observarse, las normas contienen ciertos criterios similares a los de la Unión Europea, en cuanto establecen límites directos a la transparencia teniendo por fundamento la protección de cierta información confidencial. Sin embargo, se encuentran ausentes los límites directos relacionados con la protección de los consumidores y/o otros derechos fundamentales que puedan resultar pertinentes.

---

676 *Ibíd*., p. 3. Considerando 6

677 *Ibíd*., p. 14. Considerando 84.

678 CONGRESO de los Estados Unidos (Estados Unidos). *H.R.6796 - Digital Services Oversight and Safety Act of 2022.* Washington D.C., Estados Unidos, 18 de febrero de 2022. Sección 6.3, letra A.

679 *Ibíd.*

680 PRESIDENTE de los Estados Unidos (Estados Unidos). *Executive Order N° 14.110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 de octubre de 2023. Sección 5.2

Lo que resulta innovador, eso sí, es que se contemple como límite directo la protección de la seguridad de los servicios automatizados. Este criterio no está presente expresamente en la normativa europea –salvo en lo relativo a las intervenciones de mala fe por parte de terceros–, y podría ser relevante para efectos de evitar que, con motivo del cumplimiento de los deberes de transparencia, se produzcan fallas en las tecnologías que redunden en perjuicios para los consumidores que sean aún más graves que los que se ocasionarían si se restringiera la transparencia.

4. Auditoría algorítmica

Tal como se señaló en el Capítulo II, la auditoría algorítmica constituye un mecanismo para comprobar que los algoritmos son diseñados, desarrollados y utilizados de acuerdo con la norma jurídica vigente para garantizar que los principios éticos y jurídicos se reflejan en los sistemas de IA que toman decisiones sobre todos nosotros y, gracias a ellas, se hace la IA más transparente, explicable y eficaz. Del mismo modo, se fomenta la responsabilidad social de las empresas en el desarrollo y uso de algoritmos[681], ya que es una forma de prevenir y controlar los sesgos algorítmicos.

Unión Europea

Al respecto, la Unión Europea no contempla actualmente una regulación específica y detallada sobre la obligatoriedad de realizar auditorías algorítmicas de los proveedores que presten sus servicios mediante sistemas de IA o que comercialicen bienes o servicios que la empleen. Se trata aún de una materia relativamente emergente, sin una consagración explícita en la legislación de la Unión Europea.

Sin perjuicio de lo anterior, de las normas que a continuación se analizan es posible afirmar que la obligación para ciertos prestadores de servicios de gran tamaño de realizar

[681] MOTA, Eva y HERRERA, Esther. 2023. *Auditoría algorítmica en la inteligencia artificial en el sector público*. [en línea] Revista Digital Instituto de Investigaciones y Estudios Contables - FCE UNLP (17) <https://revistas.unlp.edu.ar/proyecciones/article/view/14782> [consulta: 09 septiembre 2023].

auditorías independientes conlleva también la obligación de auditar los algoritmos que emplean para la prestación de sus servicios.

Así las cosas, el DSA, el cual tiene por objeto mejorar el funcionamiento del mercado interior y garantizar un entorno en línea seguro y transparente[682] , y que resulta aplicable a los proveedores de servicios intermediarios –tales como mercados en línea, plataformas de economía colaborativa y tiendas de aplicaciones, entre otros–, estipula que "*los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño deben rendir cuentas, mediante auditorías independientes, del cumplimiento de las obligaciones establecidas en el presente Reglamento y, cuando sea pertinente, de cualquier compromiso complementario adquirido de conformidad con códigos de conducta y protocolos de crisis*"[683].

De esta manera, conforme dispone el artículo 37 del DSA, los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño se someterán, a su propia costa y al menos una vez al año, a auditorías independientes, con el objeto de evaluar el cumplimiento de sus obligaciones, las cuales se encuentran establecidas en el Capítulo III del propio reglamento, y de sus compromisos contraídos en virtud de los Códigos de Conductas adoptados[684].

Asimismo, el propio artículo 37 señala que:

> *"Los prestadores de plataformas en línea de muy gran tamaño y de motores de búsqueda en línea de muy gran tamaño proporcionarán a las organizaciones que lleven a cabo las auditorías en virtud del presente artículo la cooperación y la asistencia necesarias para permitirles llevar a cabo dichas auditorías de manera eficaz, eficiente y en tiempo oportuno, en particular dándoles acceso a todos los datos y locales pertinentes y respondiendo a sus*

[682] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022. C considerando 40.
[683] *Ibíd*. Considerando 92.
[684] *Ibid*. Artículo 37.

preguntas orales o escritas. Se abstendrán de obstaculizar, influir indebidamente o menoscabar la realización de la auditoría"[685].

Por su parte, el DMA, cuyo objetivo es "c*ontribuir al buen funcionamiento del mercado interior, estableciendo normas para garantizar la disputabilidad y la equidad de los mercados en el sector digital en general y garantizarlas a los usuarios profesionales y los usuarios finales de servicios básicos de plataforma prestados por guardianes de acceso en particular*"[686], establece, en su artículo 15, que los guardianes de acceso, esto es, grandes empresas prestadoras de servicios básicos de plataforma con un gran poder económico[687], deben presentar a la Comisión Europea, dentro de los seis meses siguientes a su designación, una descripción auditada independientemente de las técnicas para elaborar perfiles de los consumidores que apliquen en sus servicios básicos de plataforma.

En cuanto al RGPD, aquel no establece obligación alguna relativa al desarrollo de auditorías algorítmicas para las empresas que traten datos personales. Sin embargo, se ha señalado que la figura de la Evaluación de Impacto relativa a la Protección de Datos Personales del artículo 35 RGPD "*debe ser la base para crear auditorías periódicas de algoritmos, que analicen desde un punto de vista ético-jurídico el recorrido de todas sus fases: diseño, tratamiento, resultado; a través de agencias de certificación o expertos independientes, con la intención de eliminar sesgos y prevenir posibles efectos discriminatorios*"[688].

En la misma línea, cabe mencionar que el artículo 28 del RGPD señala que el encargado de tratamiento de datos debe poner a disposición del responsable de aquellos datos "t*oda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable*"[689].

---

685 *Ibíd*.

686 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/1925 sobre mercados disputables y equitativos en el sector digital. Bruselas, Bélgica, 2022. Considerando 7º.

687 *Ibid*. Considerando 3º.

688 EGUÍLUZ, Andoni. *Desafíos y retos que plantean las decisiones automatizadas y los perfilados para los derechos fundamentales.* [en línea] Estudios de Deusto: Revista de Derecho Público, 2020, Vol. 68, n° 2, p. 325-367 <https://dialnet.unirioja.es/servlet/articulo?codigo=7692059> [consulta: 25 noviembre 2023]. p.360.

689 PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Bruselas, Bélgica, 2016. Artículo 28.

De la misma manera, el RGPD señala entre las funciones del delegado de protección de datos "*supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes*"[690], lo cual termina por hacer un guiño a la conveniencia que implica para las empresas la utilización de este mecanismo, en tanto puede ser una herramienta útil para demostrar el cumplimiento del RGPD y para identificar y mitigar los riesgos asociados al tratamiento de datos personales.

En cuanto a la legislación propuesta en la Unión Europea, la AI ACT tampoco comprende obligación alguna para los proveedores que traten datos personales utilizando algoritmos de someterse periódicamente a auditorías algorítmicas. Sin perjuicio de lo anterior, el proyecto señala, a propósito de los sistemas de IA de alto riesgo independientes, "*que la intervención reguladora se encuentra en una fase temprana, que el sector de la IA es muy innovador y que apenas están empezando a acumularse los conocimientos necesarios para llevar a cabo auditorías*"[691], lo cual deja entrever que la auditoría algorítmica emerge como un instrumento esencial en la era de la IA.

Estados Unidos

En Estados Unidos, si bien existen algunas leyes que abordan en general lo que es la responsabilidad algorítmica, no se ha establecido una regulación específica y detallada sobre la obligatoriedad de realizar auditorías algorítmicas de los proveedores que presten sus servicios mediante sistemas de IA o que comercialicen bienes o servicios que la empleen.

En cuanto a la legislación actual, la *National Artificial Intelligence Initiative Act*, de 2020, señala en su sección 22A una serie de estándares aplicables para los sistemas de IA, entre los cuales contempla, en la e) de su literal B, que el Director del Instituto Nacional de Estándares y Tecnología debe apoyar la investigación de medición y el desarrollo de mejores

[690] *Ibíd*. Artículo 39.

[691] PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA (UE). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021, p.16.

prácticas y estándares voluntarios para sistemas de inteligencia artificial confiables, que pueden incluir "*mecanismos de auditoría y puntos de referencia para la precisión, transparencia, verificabilidad y garantía de seguridad de los sistemas de inteligencia artificial*"[692].

Asimismo, cabe mencionar que la Orden Ejecutiva sobre el desarrollo y uso seguro y confiable de la IA, de 30 de octubre de 2023, en su sección 4.1, acerca de la seguridad y protección de la tecnología de la IA, establece que:

> "[E]*l Secretario de Comercio, actuando a través del Director del Instituto Nacional de Estándares y Tecnología (NIST), en coordinación con el Secretario de Energía, el Secretario de Seguridad Nacional y los jefes de otras agencias relevantes que el Secretario de Comercio considere apropiado, deberá: (i) Establecer directrices y mejores prácticas, con el objetivo de promover estándares industriales consensuados, para desarrollar e implementar sistemas de IA seguros y confiables, que incluyen: (...) (C) lanzar una iniciativa para crear orientación y puntos de referencia para evaluar y auditar las capacidades de la IA, centrándose en las capacidades a través de las cuales la IA podría causar daño, como en las áreas de ciberseguridad y bioseguridad*"[693].

En la misma línea, la *Digital Services Oversight and Safety Act* dispone en su sección 7, acerca de evaluación de riesgos e informes de mitigación de riesgos, en su letra c),

> "[Q]*ue se requiere que los proveedores de una gran plataforma cubierta obtengan una auditoría anual de la evaluación de riesgos y las medidas de mitigación de riesgos documentadas por el proveedor en el informe más reciente presentado bajo la subsección (a) con respecto a la plataforma, la exactitud del informe de transparencia más reciente presentado bajo la sección (b) con*

[692] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.6216 - National Artificial Intelligence Initiative Act of 2020. Washington D.C., Estados Unidos, 12 de marzo de 2020.* Sección 22A.
[693] PRESIDENTE de los Estados Unidos (Estados Unidos). Executive Order N° 14.110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 30 de octubre de 2023. Sección 4.1.

respecto a la plataforma , y el cumplimiento por parte de la proveedor con respecto a la plataforma con las regulaciones emitidas bajo la sección 10 (...)"[694].

En cuanto a legislación propuesta, en el año 2022 se presentó ante el Congreso de Estados Unidos el proyecto de ley Algorithmic Accountability Act (En adelante "**AAA**"), el cual busca establecer una enmienda a la Ley Federal de Privacidad de 1974 (En adelante "**FPPA**") para establecer responsabilidades claras para los desarrolladores, proveedores y propietarios de sistemas de IA. Mediante este proyecto de ley, se ordena a la Comisión Federal de Comercio exigir evaluaciones de impacto de los sistemas de decisión automatizados y los procesos de decisión críticos[695].

Así las cosas, entre las materias que aborda este proyecto, en su sección 3 establece un sistema de evaluación de impacto de los sistemas de decisión automatizados y de los procesos de decisión crítica aumentados y, al respecto, en la letra g) de su literal B, establece:

*"[*A*] más tardar 2 años después de la fecha de promulgación de esta Ley, la Comisión deberá, en consulta con el Director del Instituto Nacional de Normas y Tecnología, el Director del Instituto Nacional Iniciativa de Inteligencia Artificial, el Director de la Oficina de Política Científica y Tecnológica, y otros partes interesadas pertinentes, incluidos los organismos de normalización, industria privada, academia, expertos en tecnología y defensores de los derechos civiles, los consumidores y los afectados comunidades, promulgar regulaciones, de conformidad con la sección 553 del título 5, Código de los Estados Unidos, que: (...) (G) exigir que cada entidad cubierta, al realizar la evaluación de impacto descrita en el subpárrafo (A), en la medida de lo posible, consultar significativamente (incluso a través de un diseño participativo, auditorías independientes o solicitando o incorporando comentarios) con partes interesadas internas relevantes (como empleados, equipos de ética y equipos de tecnología responsables) y partes interesadas externas independientes (como representantes y defensores de los afectados), grupos, sociedad civil y*

[694] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.6796 - Digital Services Oversight and Safety Act of 2022.* Washington D.C., Estados Unidos, 18 de febrero de 2022. Sección 7.
[695] CONGRESO de los Estados Unidos (Estados Unidos). *H.R. 5628 - Algorithmic Accountability Act of 2023*, 21 de septiembre de 2023, p.1.

defensores, y expertos en tecnología) tan frecuentemente como sea necesario"[696].

Como queda en entredicho, de manera similar a lo que ocurre con la Unión Europea, no existe una obligatoriedad legal para proveedores que utilicen IA en la prestación de sus servicios de realizar auditorías algorítmicas, menos periódicamente, pero sí es posible que aquello termine por serles exigible al momento de realizarles las auditorías correspondientes, sobre todo en lo que respecta a los proveedores de gran tamaño.

5. Otros controles en el uso de la IA

Como se explicó en su momento, el "control" de la IA implica que exista una regulación administrativa, institucional y/o jurídica respecto de su uso, que se asocia comúnmente a la intervención o vigilancia humana[697]. Así, si entendemos el concepto en un sentido amplio, casi todo lo analizado anteriormente en este Capítulo podría ser considerado como control de la IA, puesto que varias de las normas jurídicas hasta ahora examinadas obligan al proveedor –humano– a cumplir con deberes de información o diligencia al momento de emplear la tecnología, y diversos entes administrativos –también compuestos por humanos– están encargados de fiscalizar ese cumplimiento.

Sin embargo, se previene al lector que, para efectos de desarrollar el presente apartado, solo se tendrán a la vista normas que, si bien efectúan un control en el uso de la IA y resultan útiles para resguardar derechos de los consumidores, no dicen relación directa con los problemas analizados sobre responsabilidad civil ni con los regímenes de transparencia o tratamiento de datos personales, sino con deberes de diligencia más amplios. De ahí que el nombre del apartado refiera a "Otros controles".

El objetivo es que estos deberes de diligencia permitan dar luces sobre la clase de conductas concretas que debe desplegar un proveedor profesional. Como se explicó, en nuestro ordenamiento existe un deber de profesionalidad, en cuya virtud es posible exigir al

[696] *Ibíd*. Sección 3.
[697] HUESO, Lorenzo Cotino. *Riesgos e impactos del Big Data, la inteligencia artificial y la robótica: enfoques, modelos y principios de la respuesta del derecho*. Revista general de Derecho administrativo. (50): pp.15-18, 2019.

proveedor que observe un comportamiento cuidadoso y consistente con el estándar de buena fe. El problema es que su aplicación resulta sencilla únicamente cuando se habla de omisiones o conductas negativas, vale decir, de aquello a lo que debe abstenerse de hacer el proveedor (influir maliciosamente en la autonomía, descuidar datos personales, discriminar intencional y arbitrariamente, etc.).

En cambio, cuando pensamos en conductas positivas, si bien es claro que estas deben ir motivadas por una buena intención y por el debido resguardo de los derechos de los consumidores, es complejo proyectarlas en deberes concretos. En efecto, existe la posibilidad de que pasemos el límite y las conductas ya no sean profesionales, sino desproporcionadas o incluso imposibles de cumplir.

Parte de esa labor depuradora se ha realizado satisfactoriamente a lo largo de los apartados anteriores, al examinar, por ejemplo, hasta qué punto debe transparentar el proveedor. Pero, dada la especificidad de tales materias, por el momento sigue siendo difícil desentrañar qué conductas generales –más allá de lo relativo a la transparencia– son extraíbles a partir del deber de profesionalidad. Por ello, conviene tener a la vista otros controles genéricos que se han implementado en la Unión Europea y en Estados Unidos, y que son reveladores del buen cuidado preventivo que deben adoptar los operadores.

Unión Europea

Primeramente, la normativa europea contiene disposiciones relacionadas con el control de riesgos de los sistemas de IA. A propósito del apartado de transparencia, se abordó la definición de sistemas de IA de alto riesgo, sus características y las obligaciones de información. No obstante, no se ha ahondado mayormente en los criterios para prohibir el uso de IA, en los deberes de evaluación y reducción de riesgo de los proveedores intermediarios, ni en los deberes de gestión de riesgo por parte de quienes utilizan sistemas de IA de alto riesgo.

En cuanto a los sistemas de IA prohibidos, el artículo 5 de la AI ACT recoge una causal que está directamente vinculada con los derechos de los consumidores. Se trata proscripción de sistemas que se sirvan "*de técnicas subliminales que trasciendan la conciencia de una persona para alterar de manera sustancial su comportamiento de un modo que provoque o*

sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra"[698]. Si bien su ámbito de aplicación no se limita al consumo, de su texto se colige la imposibilidad de que los proveedores empleen sistemas de IA que afecten sustancialmente la autonomía del consumidor y le ocasionen o lo expongan a daños.

Respecto de los deberes de evaluación y reducción de riesgo de los proveedores intermediarios, el artículo 34 del DSA prevé que todas las plataformas y motores de búsqueda de muy gran tamaño deberán detectar, analizar y evaluar con diligencia los riesgos del diseño o funcionamiento de su servicio, haciendo especial énfasis en los sistemas algorítmicos[699]. Asimismo, se precisa que evaluación de riesgos deberá referir, entre otras cosas, a:

> "[C]*ualquier efecto negativo real o previsible para el ejercicio de los derechos fundamentales, en particular los relativos a la dignidad humana amparada por el artículo 1 de la Carta, al respeto de la vida privada y familiar amparada por el artículo 7 de la Carta, a la protección de los datos de carácter personal amparada por el artículo 8 de la Carta, a la libertad de expresión e información, incluida la libertad y el pluralismo de los medios de comunicación, amparada por el artículo 11 de la Carta, a la no discriminación amparada por el artículo 21 de la Carta, a los derechos del niño amparados por el artículo 24 de la Carta y a un nivel elevado de protección de los consumidores, amparado por el artículo 38 de la Carta*"[700].

La sola inclusión de derechos fundamentales como la dignidad humana, el respeto de la vida privada y la libertad de expresión brinda tutela a los consumidores, ya que estos son derechos con los todos cuentan por el solo hecho de ser personas. Sin embargo, la protección resulta aún más indiscutible y extendida al mencionarse expresamente que deben identificarse riesgos que atenten en contra del "*nivel elevado de protección de los consumidores*".

---

[698] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículo 5.1 letra a).
[699] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022. Artículo 34.
[700] *Ibíd*.

El artículo 35 del DSA añade que, una vez que se ha realizado la evaluación de riesgos, los intermediarios deben llevar adelante una serie de medidas razonables, proporcionadas y efectivas para reducirlos[701]. Entre ellas se mencionan: (i) "*la adaptación del diseño, las características o el funcionamiento de sus servicios, incluidas sus interfaces en línea*"[702]; (ii) "*la realización de pruebas y la adaptación de sus sistemas algorítmicos, incluidos sus sistemas de recomendación*"[703]; (iii) "*la adopción de medidas de concienciación y la adaptación de su interfaz en línea con el fin de proporcionar más información a los destinatarios del servicio*"[704]; etc.

Por su parte, en cuanto a los deberes de gestión de riesgos, el artículo 9 de la AI Act expresa que todo operador que trabaje con un sistema de IA de alto riesgo –sea un intermediario o un proveedor directo–, debe establecer, implantar, documentar y mantener un sistema de gestión de riesgos, que "*consistirá en un proceso iterativo continuo que se llevará a cabo durante todo el ciclo de vida de un sistema de IA de alto riesgo, el cual requerirá actualizaciones sistemáticas periódicas*"[705]. El objetivo de ello es identificar y reducir a un nivel aceptable aquellos riesgos que no han logrado ser mitigados mediante el cumplimiento de otros deberes normativos[706].

Este sistema deberá constar de cuatro etapas: (i) identificación y análisis de riesgos conocidos y previsibles que se vinculen al sistema empleado; (ii) estimación y evaluación de riesgos que puedan surgir con ocasión de la utilización del sistema conforme a su finalidad prevista, así como cuando se le dé un uso indebido pero que sea razonablemente previsible; (iii) evaluación de riesgos que podrían surgir a partir del análisis de los datos que emplee el

[701] *Ibíd*. Artículo 35.
[702] *Ibíd.*
[703] *Ibíd.*
[704] *Ibíd.*
[705] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículo 9.
[706] SCHUETT, Jonas. *Risk management in the artificial intelligence act.* [en línea] European Journal of Risk Regulation, 08 de febrero de 2023, <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risk-management-in-the-artificial-intelligence-act/2E4D5707E65EFB3251A76E288BA74068> [consulta: 01 diciembre 2023]. En concreto, el autor señala que el regulador está consciente de que, por mucho que el operador cumpla con todos los otros deberes establecidos en el Capítulo II del cuerpo normativo (manejo de datos, registros, transparencia, ciberseguridad, solidez, etc.), es probable que aún subsistan riesgos. En tal sentido, la función del artículo 9 es que dichos riesgos puedan ser identificados y posteriormente abordados.

sistema de seguimiento posterior a la comercialización; y (iv) gestión adecuada de todos los riesgos identificados, analizados y evaluados[707].

Luego, el precepto establece que al momento de reducir y eliminar dichos riesgos, "*se tendrán en la debida consideración los conocimientos técnicos, la experiencia, la educación y la formación que se espera que posea el usuario, así como el entorno en el que está previsto que se utilice el sistema*"[708]. Así, se reconoce que el uso de los sistemas de IA está imbricado a un determinado contexto socio-técnico, y el proceso de mitigación de riesgos debe ser adecuado a él[709]. Esto podría resultar interesante si se tiene en cuenta que el consumidor medio no posee conocimientos técnicos, experiencia, educación ni formación sobre IA.

Adicionalmente, la norma prevé que los sistemas de IA deberán ser sometidos a procesos de prueba en forma previa a ser introducidos en el mercado o puestos en servicio. Las pruebas persiguen determinar cuáles son las medidas de gestión de riesgo más adecuadas, así como comprobar que la IA sea apta para su finalidad prevista y dé cumplimiento a los deberes normativos fijados para los sistemas de alto riesgo[710].

El hecho de que el cumplimiento de la finalidad prevista sea sometido a prueba es altamente importante, por cuanto, si solo se utilizaran datos de entrenamiento, se correría el riesgo de que el desempeño efectivo del sistema sea distinto al esperado, dando lugar a lo que se conoce como "*distributional shift*"[711]. Por otra parte, las pruebas suponen que el sistema sea probado exactamente en el mismo entorno para el que está pensado funcionar, lo que otorga una mayor fiabilidad y permite detectar eventuales incongruencias con los procesos de entrenamiento[712].

---

[707] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículo 9.
[708] *Ibíd*.
[709] SCHUETT, op. cit., p.14.
[710] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículos 5 a 9.
[711] SCHUETT, Jonas. *Risk management in the artificial intelligence act.* [en línea] European Journal of Risk Regulation, 08 de febrero de 2023, <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risk-management-in-the-artificial-intelligence-act/2E4D5707E65EFB3251A76E288BA74068> [consulta: 01 diciembre 2023]. p. 15.
[712] *Ibíd.*

Ahora bien, cabe observar que estas pruebas técnicas difícilmente puedan ser realizadas por un proveedor que se desempeña profesionalmente en ámbitos distintos a la tecnología –y que solo recurre a la IA en forma accesoria para potenciar o facilitar su negocio–. En ese sentido, es de esperar que sean encargadas en su totalidad o en parte a empresas externas expertas en la materia. Esto no es impedido por la norma. Más aún, pareciere resultar deseable y más eficiente, siempre y cuando el proveedor siga siendo responsable del cumplimiento de todos los requisitos a los que refiere el precepto[713].

Además de los deberes de monitoreo y reducción directa de riesgos, existen controles asociados al registro, supervigilancia y rendimiento de la IA. En lo que respecta al registro, los operadores de sistemas de IA de alto riesgo deben redactar una documentación técnica en la que quede constancia del cumplimiento de los deberes normativos[714]. Así también, deben diseñar el sistema de IA incluyendo una función que permita registrar automáticamente sus eventos, de manera que se garantice la trazabilidad de su funcionamiento durante el ciclo de vida que resulte adecuado –atendiendo a la finalidad prevista para su uso–[715].

En cuanto a la supervigilancia, el artículo 14.1 de la AI Act indica que los "*sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de una herramienta de interfaz humano-máquina adecuada, entre otras cosas*"[716]. Resulta interesante que no solo se consagre un deber de vigilancia humana efectiva en el funcionamiento de los sistemas, sino también la obligación de diseñar y desarrollar las tecnologías de manera tal que permitan dicha vigilancia.

Así, se adopta un enfoque esencialmente preventivo, toda vez que la factibilidad de la vigilancia humana se asegura desde el diseño. A mayor abundamiento, las medidas de vigilancia deben ser definidas –y, de ser posible, incorporadas– en forma previa a la introducción al mercado o puesta en servicio del sistema[717].

---

[713] *Ibíd*., p. 16.

[714] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículos 11 y 18.

[715] *Ibíd*. Artículo 12.

[716] *Ibíd*. Artículo 14.

[717] *Ibíd*.

Estas medidas han de permitir a la persona encargada de la vigilancia entender por completo las capacidades y limitaciones de la IA empleada, controlar su funcionamiento, intervenir o interrumpir el sistema en forma sencilla, interpretar, invalidar y revertir la información de salida, y dimensionar los sesgos de automatización[718].

Adicionalmente, se establece expresamente que el objetivo de que exista una vigilancia humana es prevenir o reducir al mínimo los peligros para la salud, seguridad o derechos fundamentales que puedan surgir cuando el sistema de IA se utiliza conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible, especialmente si los riesgos no han podido ser mitigados mediante otros deberes normativos[719]. En ese sentido, este precepto cumpliría un rol parecido al del artículo 9 de la AI Act, pero destacando la relevancia del control humano.

Cabe señalar que la supervigilancia se extiende a todo el proceso de postventa. En efecto, el artículo 61 de la AI ACT prevé que los proveedores que empleen sistemas de IA de alto riesgo deben establecer un sistema de seguimiento posterior a la comercialización, que permita recabar, analizar y documentar, en forma activa y sistemática, el funcionamiento del sistema durante toda su vida útil, con el objeto de evaluar si los sistemas empleados han cumplido con los diversos deberes normativos[720].

Por último, en lo que refiere al control de rendimiento, el artículo 17 de la AI ACT dispone que los proveedores que empleen sistemas de IA de alto riesgo deben implementar un sistema que, junto con velar por el cumplimiento a los diversos deberes previstos en el cuerpo normativo, prevea técnicas, procedimientos y actuaciones que permitan asegurar la calidad del sistema utilizado[721].

Asimismo, a modo de incentivar en control en la calidad de los sistemas de IA empleados, el Considerando 37 de la Directiva sobre responsabilidad por los daños causados por productos defectuosos indica que:

[718] *Ibíd*.
[719] *Ibíd*.
[720] *Ibíd*. Artículo 61.
[721] *Ibíd.* Artículo 17.1, y, en particular, la letra b).

> "[D]*ado que las tecnologías digitales permiten a los fabricantes ejercer control más allá del momento de la introducción del producto en el mercado o de la puesta en servicio, los fabricantes deben seguir siendo responsables de las deficiencias que se produzcan después de ese momento como resultado de programas informáticos o servicios conexos que estén bajo su control, ya sea en forma de mejoras o actualizaciones o de algoritmos de aprendizaje automático*"[722].

En línea con ello, posteriormente el artículo 6 de la Directiva establece que, para efectos de evaluar la defectuosidad de un producto, deberá tenerse especialmente en cuenta si es que este posee la posibilidad de seguir aprendiendo después de su despliegue al mercado, en cuyo caso el fabricante no podrá desentenderse automáticamente de su funcionamiento[723]. De esta forma, quien diseña un sistema de IA sabrá de antemano que deberá ser especialmente cauteloso con el control de los riesgos y la calidad de su tecnología.

En suma, existen diversas disposiciones que permiten controlar el uso de la IA recurriendo a deberes distintos de la transparencia y el tratamiento de datos personales. Estas normas van asociadas, principalmente, al cuidado del riesgo y funcionamiento de la IA, atendiendo a la finalidad prevista para el uso del sistema. A su vez, las diligencias exigidas al proveedor en el ejercicio de su actividad dan bastantes luces respecto de qué conductas positivas son factibles de concebir como obligatorias en virtud del deber de profesionalidad. Sin perjuicio de ello, a continuación se invita a realizar dos reflexiones.

En primer lugar, la regulación europea, salvo en casos excepcionales en los que se refiere al "uso indebido razonablemente previsible", pareciera ser bastante tajante en orden a que la finalidad que el mismo proveedor prevé para el sistema es la que debe guiar todos los procesos de monitoreo, prueba, entrenamiento y reducción o eliminación de riesgos. Esa misma lógica se replica para efectos de determinar si un sistema de IA es alto riesgo o bajo riesgo. A la postre, lo importante siempre es atender al destino fijado por el proveedor[724].

---

[722] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos. Bruselas, Bélgica, 2022. Considerando 37.

[723] *Ibíd*. Artículo 6 letra c).

[724] HELBERGER, N. y DIAKOPOULOS, N. *ChatGPT and the AI Act.* [en línea] Internet Policy Review, 16 Feb 2023, Vol. 12, n° 1 <https://policyreview.info/essay/chatgpt-and-ai-act> [consulta: 26 noviembre 2023]. p. 3.

Pues bien, en ese escenario, surge la pregunta de si no debiesen jugar un rol más protagónico los usos normales o probables que se espera que den los consumidores a la tecnología –que, por lo demás, no tienen por qué ser indebidos–, puesto que, a fin de cuentas, son ellos quienes interactúan directamente con la IA. A mayor abundamiento, respecto de IAs de propósito general, como los *chatbots*, no es el proveedor, sino más bien el usuario o consumidor quien determina cómo utilizará el sistema. Y justamente el uso efectivo es lo que termina por condicionar el bienestar y la integridad de los intereses que la normativa dice proteger[725].

Al respecto, los autores de la presente Memoria sostienen que, atendido el sinfín de usos que los consumidores podrían dar a cada tecnología, parece irreal que la categorización de un sistema de IA como alto o bajo riesgo se haga teniendo en cuenta cada uno de ellos. Sin embargo, lo anterior no obsta a que, junto con considerar la finalidad que el proveedor destinará al sistema, se tenga a la vista, al menos, un uso probable alternativo que puedan darle los consumidores y que no califique como indebido. Esto debiese resultar menos discutible si de lo que se trata no es de la calificación del riesgo de la IA, sino de las pruebas o de la minimización de riesgos posteriores.

En segundo lugar, es frecuente que, al pensar en qué clase de conductas es razonable exigir a los proveedores en virtud del deber de profesionalidad en esta materia, se parta de la premisa de que son ellos quienes deberán ejecutarlas. Empero, no se puede obviar que, dado que los proveedores no suelen ser quiénes desarrollaron la tecnología, es altamente probable que recurran a asistencia especializada para cumplir con aquellos deberes normativos que parezcan más complejos[726]. ¿Supone ello acaso un incumplimiento? ¿Debemos solo exigir conductas que el proveedor pueda cumplir por sí solo?

La respuesta a ambas preguntas pareciera ser negativa. No se aprecia cuál es el problema de que el proveedor contrate a un tercero –bajo su propio riesgo– para poder cumplir con los estándares normativos. Y, dado que existe esa posibilidad, tampoco resulta razonable

[725] *Ibíd*., p. 3

[726] SCHUETT, Jonas. R*isk management in the artificial intelligence act.* [en línea] European Journal of Risk Regulation, 08 de febrero de 2023, <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risk-management-in-the-artificial-intelligence-act/2E4D5707E65EFB3251A76E288BA74068> [consulta: 01 diciembre 2023]. p. 15.

establecer exigencias poco protectoras únicamente para permitir que el proveedor cumpla fácilmente por su propia cuenta. Se trata de un balance de intereses, cuyo equilibrio, en opinión de estos autores, está bien logrado en la normativa europea.

Lo anterior, por cuanto la mayor parte de las obligaciones aplican solo si el proveedor es (i) de muy grande tamaño, (ii) es intermediario de plataformas o motores de búsqueda –que suelen tener varios recursos–, u (iii) optó libremente por realizar una actividad riesgosa. Vale decir, existe proporcionalidad en el sentido de que, en muchos casos, quienes emplean IA simplemente no se sujetarán a mayor carga o control que la de dirigir su tecnología.

No se trata de imponer al proveedor obligaciones injustificadas de buscar ayuda siempre para poder satisfacer los deberes normativos. Pero, si se considera que las hipótesis en las que el agente se somete a los deberes dicen relación con grandes empresas o con quienes decidieron a voluntad realizar una actividad peligrosa, hace sentido que las medidas sean algo más onerosas que aquello que el proveedor probablemente podría cumplir por su propia cuenta.

Zanjado lo anterior, cabe agregar que, si aceptamos como algo pacífico que el proveedor en muchos casos recurrirá a la asistencia de un tercero experto, hay que ajustar la regulación a ese fenómeno. Una buena idea podría ser consagrar un régimen de *culpa in eligendo*, en el que, si el tercero falla en sus labores y gracias a ello se produce una infracción o se generan daños al consumidor, el proveedor responderá directamente por ser garante de su elección de contratación; pero podrá posteriormente, si fuere el caso, repetir en contra de quién causó el daño directamente[727].

Estados Unidos

Al igual que en la Unión Europea, en Estados Unidos se contemplan “otros controles en el uso de la IA” que no dicen relación propiamente tal con la responsabilidad civil, ni la transparencia ni el tratamiento de datos personales, sino con evaluaciones de impacto o de riesgo que

[727] Es un régimen similar al que existe en nuestro país respecto del proveedor que emplea sistemas de vigilancia desarrollados por un tercero. Véase: ISLER, Erika. *Derecho del consumo. Nociones fundamentales*. Valencia, Tirant lo Blanch, 2021. 217p.

persiguen que los sistemas automatizados que se utilicen sean aptos para entrar al mercado –ajustando, por cierto, lo que se entiende por "aptitud" a las características propias de la IA–.

Respecto de las evaluaciones de impacto o de riesgo, existe una lata normativa en diferentes leyes federales del país norteamericano que se preocupan de regular la materia. En este apartado se pondrá énfasis específicamente en tres cuerpos normativos: la *Executive Order N° 13.960 on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, de 2020[728]; la *Digital Services Oversight and Safety Act, de 2022*[729]; y, *Executive Order N° 14.110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, de 2023[730].

De la *Executive Order N° 13.960 on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* interesa para estos efectos la sección 3, que establece una serie de principios para el uso de la IA en el gobierno federal. Al respecto, la norma dispone que las agencias deben tomar medidas para garantizar que la IA en el gobierno federal sea:

1. Sea utilizada de manera justa, imparcial y no discriminatoria;
2. Sea transparente y que los resultados de la IA puedan ser auditados;
3. Sea segura y resistente a ataques; y,
4. Sea responsable y que se puedan identificar y remediar los errores[731].

Por su parte, la sección 5.3 de la Orden mencionada establece que las agencias deben tomar medidas para garantizar que la IA en el gobierno federal sea utilizada de manera justa, imparcial y no discriminatoria, transparente, segura, resistente a ataques, responsable, y que los resultados de la IA puedan ser auditados[732].

Respecto de la materia, la *Digital Services Oversight and Safety Act* establece en su sección 7 una serie de requisitos detallados para la evaluación de riesgos e informes de

[728] PRESIDENTE de los Estados Unidos (Estados Unidos). *Executive Order N° 13.960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government,* 03 de diciembre de 2020.
[729] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.6796 - Digital Services Oversight and Safety Act of 2022*. Washington D.C., Estados Unidos, 18 de febrero de 2022.
[730] PRESIDENTE de los Estados Unidos (Estados Unidos). *Executive Order N° 14.110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 de octubre de 2023.
[731] PRESIDENTE de los Estados Unidos (Estados Unidos). *Executive Order N° 13.960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government,* 03 de diciembre de 2020. Sección 3.
[732] *Ibíd*.

mitigación de riesgos para grandes plataformas cubiertas[733]. Asimismo, ordena a la Comisión emitir regulaciones que requieran que un proveedor de una gran plataforma cubierta realice evaluaciones de riesgos con respecto a la plataforma y, basándose en estas evaluaciones, presente informes de evaluación de riesgos y mitigación de riesgos a la Comisión, lo cuales deben identificar, analizar y evaluar los riesgos sistémicos significativos derivados del funcionamiento y uso de la plataforma, incluyendo los riesgos sistémicos[734].

Además, en aquel cuerpo legal se detallan medidas específicas de mitigación de riesgos, como la integración de procesos de modelado de amenazas y pruebas de red, adaptación de sistemas de moderación de contenido, medidas dirigidas a limitar la visualización de anuncios, entre otras[735].

Adicionalmente, señala que se requerirá que los proveedores obtengan una auditoría anual de las medidas de evaluación y mitigación de riesgos documentadas, la precisión de los informes de transparencia y el cumplimiento con las regulaciones, realizada por una organización independiente con experiencia en gestión de riesgos[736].

En la misma línea, la *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, en relación con la seguridad, establece que la IA debe ser evaluada de manera robusta, confiable, repetible y estandarizada, con políticas, instituciones y mecanismos para probar, comprender y mitigar los riesgos de estos sistemas antes de su uso[737].

También se refiere a la necesidad de abordar los riesgos de seguridad más apremiantes de los sistemas de IA, incluidos los relacionados con la biotecnología, la ciberseguridad, la infraestructura crítica y otros peligros para la seguridad nacional, y menciona la importancia de desarrollar mecanismos efectivos de etiquetado y procedencia del contenido para que los estadounidenses puedan determinar cuándo el contenido es generado utilizando IA y cuándo no lo es.

---

[733] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.6796 - Digital Services Oversight and Safety Act of 2022*. Washington D.C., Estados Unidos, 18 de febrero de 2022. Sección 7.
[734] *Ibíd*.
[735] *Ibíd*.
[736] *Ibíd*.
[737] *Ibíd*.

En cuanto a la legislación propuesta, la *Algorithmic Justice and Online Platform Transparency Act* establece en su sección 3A que la Comisión Federal de Comercio (FTC) debe promulgar regulaciones que requieran a cada entidad cubierta por el proyecto realizar una evaluación del impacto de cualquier sistema automatizado de toma de decisiones o proceso aumentado de toma de decisiones críticas.[738] Así las cosas, la letra H, por ejemplo, señala dentro de las materias a abordar, regulación que propenda a que cada entidad cubierta intente eliminar o mitigar, de manera oportuna, cualquier impacto realizado por un proceso de decisión crítica aumentada que demuestre un probable impacto negativo material que tenga efectos legales o similares significativos en la vida de un consumidor[739].

Al respecto, el proyecto dispone en su sección 4 que, al realizar cualquier evaluación de impacto para un sistema de decisión automatizado o un proceso de decisión crítico aumentado, la entidad deberá -entre otras cosas-, en la medida de lo posible, apoyar y llevar a cabo una formación y educación continuas para todos los empleados, contratistas u otros agentes pertinentes en relación con cualquier impacto negativo material documentado sobre los consumidores de sistemas automatizados de decisión o procesos de decisión crítica aumentados similares y cualquier método mejorado de desarrollo o realización de una evaluación de impacto para dicho sistema o proceso basado en las mejores prácticas del sector y las propuestas y publicaciones pertinentes de expertos, como defensores, periodistas y académicos[740].

Asimismo, la sección citada dispone que la entidad deberá también evaluar los derechos de los consumidores, por ejemplo, evaluando en qué medida la entidad cubierta proporciona a los consumidores un aviso claro de que se utilizará dicho sistema o proceso y un mecanismo de exclusión voluntaria de dicho uso; evaluando la transparencia y explicabilidad de dicho sistema o proceso y el grado en que un consumidor puede impugnar, corregir o apelar una decisión o excluirse voluntariamente de dicho sistema o proceso; y, describiendo en qué medida cualquier tercero receptor de decisiones recibe una copia o tiene

[738] CONGRESO de los Estados Unidos (Estados Unidos). *S.2325 - Algorithmic Justice and Online Platform Transparency Act.* Washington D.C., Estados Unidos, de 13 de julio de 2023. Sección 3.
[739] *Ibíd*.
[740] *Ibíd*. Sección 4.

acceso a los resultados de dicho sistema o proceso y la categoría de dicho tercero receptor de decisiones[741].

En tercer lugar, se recomienda a la empresa que realiza la evaluación de impacto identificar cualquier probable impacto negativo material del sistema automatizado de toma de decisiones o del proceso aumentado de toma de decisiones críticas sobre los consumidores y evaluar cualquier estrategia de mitigación aplicable, como, por ejemplo, mediante:

1. La identificación y medición de cualquier probable impacto negativo material del sistema o proceso sobre los consumidores, incluida la documentación de las medidas adoptadas para identificar y medir dicho impacto;
2. La documentación de cualquier medida adoptada para eliminar o mitigar razonablemente cualquier probable impacto negativo material identificado, incluidas medidas como la retirada del sistema o proceso del mercado o la finalización de su desarrollo;
3. Con respecto a los probables impactos negativos materiales identificados, documentar qué impactos se dejaron sin mitigar y la justificación de la inacción, incluidos detalles sobre el interés imperioso y no discriminatorio que los justifica y por qué dicho interés no puede satisfacerse por otros medios (por ejemplo, cuando existe una compensación equitativa de suma cero entre los impactos sobre 2 o más consumidores o cuando la acción mitigadora requerida violaría los derechos civiles u otras leyes); y
4. Documentar los protocolos o prácticas estándar utilizados para identificar, medir, mitigar o eliminar cualquier posible impacto negativo material sobre los consumidores y cómo se informa y forma a los equipos o al personal pertinente sobre dichos protocolos o prácticas[742].

En pos de complementar lo que vienen a significar las evaluaciones de riesgo o de impacto, resulta importantísimo mencionar dos proyectos de ley que vienen a mejorar la regulación en torno a la IA, prohibiendo ciertas conductas y estableciendo evaluaciones de rendimiento, cuestión completamente innovadora.

[741] *Ibíd*.
[742] *Ibíd*.

Así las cosas, la Algorithmic Justice and Online Platform Transparency Act, en su sección 4, establece como requisito para la realización de una evaluación de impacto para un sistema automatizado de toma de decisiones o proceso aumentado de toma de decisiones críticas, que la entidad realice pruebas y evaluaciones continuas del rendimiento actual e histórico del sistema en cuestión utilizando medidas como conjuntos de datos de referencia, ejemplos representativos de los datos históricos de la entidad cubierta y otras normas, documentando, entre otras cosas:

1. Una descripción de lo que se considera un rendimiento satisfactorio y los métodos y parámetros técnicos y empresariales utilizados por la entidad cubierta para evaluar el rendimiento;
2. Una revisión del rendimiento de dicho sistema o proceso en condiciones de prueba o una explicación de por qué no se realizaron dichas pruebas de rendimiento;
3. Una revisión del rendimiento de dicho sistema o proceso en condiciones de despliegue o una explicación de por qué no se revisó el rendimiento en condiciones de despliegue; y,
4. Una comparación del rendimiento de dicho sistema o proceso en condiciones de despliegue con las condiciones de ensayo o una explicación de por qué no fue posible dicha comparación"[743].

Por su parte, la Algorithmic Accountability Act de 2023 consagra conductas prohibidas para las plataformas en línea. Al respecto, señala que es ilegal para una plataforma en línea emplear cualquier característica de diseño de plataforma en línea patentada, incluido un proceso algorítmico, o de otro modo procesar la información personal de un individuo de manera que segregue, discrimine o de otro modo haga no disponibles los bienes, servicios, instalaciones, privilegios, ventajas o alojamientos de cualquier lugar de alojamiento público sobre la base de la raza, color, etnia, religión, origen nacional, sexo, género, identidad de género, orientación sexual, estado familiar, información biométrica o discapacidad real o percibida de un individuo o clase de individuos[744].

[743] *Ibíd*.
[744] CONGRESO de los Estados Unidos (Estados Unidos). *H.R. 5628 - Algorithmic Accountability Act of 2023.* Washington D.C., Estados Unidos, 21 de septiembre de 2023.

Asimismo, el proyecto de ley también establece otras conductas prohibidas, como la discriminación en prácticas publicitarias y privación intencional del derecho al voto de las personas. Ahora bien, sin perjuicio de lo anterior, la norma incluye excepciones para pruebas internas de buena fe y publicidad dirigida a poblaciones subrepresentadas de manera justa y no engañosa.

II. Estándares para Chile

En el apartado anterior del presente Capítulo, se examinó la normativa europea y la normativa estadounidense a propósito de (i) la responsabilidad civil de la IA, (ii) la protección de los datos personales de los consumidores ante tratamientos automatizados, (iii) los deberes de transparencia, (iv) la auditoría algorítmica y (v) otros controles en el uso de la IA. El objetivo de ello fue exponer cómo se ha abordado en otras legislaciones –que suelen ser más desarrolladas– ciertos problemas que, según se expuso en el Capítulo III, la regulación chilena no permite solucionar en forma satisfactoria.

Al momento de examinar la normativa extranjera, no solo se hizo una reproducción de los preceptos pertinentes, sino que también se precisó su sentido y alcance, haciendo énfasis en el grado de protección brindado a los consumidores. Asimismo, se destacaron algunos aspectos positivos y negativos de cada régimen, procurando brindar un enfoque comparativo.

En esta instancia, el cometido no dice relación con decidir qué régimen en su conjunto es superior. En efecto, los autores de esta Memoria creen que no se trata de posicionar una normativa completa por sobre la otra, sino de analizar, estándar por estándar, qué normas sería útil tener a la vista en nuestro país, con total prescindencia de si dichas normas corresponden a un mismo régimen o no.

En otras palabras, en lugar de comprometerse por completo con una normativa, la idea es buscar inspiraciones que puedan ser de ayuda a nuestro país, teniendo a la vista lo mejor de cada uno de los regímenes estudiados. Lo anterior, con el propósito de realizar una serie de propuestas normativas concretas cuya implementación contribuya sustancialmente a mejorar el nivel de protección de los consumidores.

Pues bien, dicho eso, se advierte al lector que, aunque el presente subcapítulo pretende ser técnico, seguirá un enfoque esencialmente reflexivo, puesto que los autores se permitirán emitir opiniones fundadas acerca de la conveniencia o inconveniencia de replicar en Chile los estándares analizados en el apartado anterior, así como sobre la idoneidad de los diversos instrumentos jurídicos para consolidar un nuevo régimen.

Atendido que no existen trabajos doctrinarios que se hayan pronunciado sobre cómo han de ser replicados en nuestro país los regímenes de protección de los consumidores ante el uso de IA consagrados en la Unión Europea y en Estados Unidos, ni sobre cuál es el mejor instrumento jurídico para reformar nuestro ordenamiento, en el presente subcapítulo se recurrirá principalmente –mas no en forma excluyente– a todo lo que se ha aprendido y reflexionado a lo largo de la investigación.

Este subcapítulo se dividirá en dos secciones. En la primera de ellas se analizará, respecto de cada de los estándares examinados en el subcapítulo anterior, qué normas, interpretaciones o principios de la Unión Europea y de Estados Unidos sería deseable consagrar en Chile, teniendo en cuenta la regulación nacional actual y sus deficiencias. De este modo, el apartado se subdividirá en: (i) responsabilidad civil de la IA; (ii) protección de datos personales; (iii) transparencia, (iv) auditoría algorítmica y (v) otros controles en el uso de la IA.

Por su parte, en la segunda sección se determinará qué mecanismos o instrumentos jurídicos (reformas a leyes ya existentes, creación de nuevas leyes, dictación de un reglamento, suscripción de tratados internacionales, *soft law*, entre otros) resultan más idóneos para introducir la regulación que se propone.

1. Análisis en base a los estándares internacionales

I. Responsabilidad Civil de la IA

Al momento de examinar los problemas de responsabilidad derivados del uso de IA, se mencionó que nuestra normativa presenta cuatro aspectos problemáticos para el consumidor: (i) la dificultad de tener que identificar al agente presuntamente responsable; (ii) la inexistencia

de un régimen de responsabilidad claro de las plataformas intermediarias; (iii) la contingencia de someterse y probar un derecho extranjero cuando el hecho dañoso tuvo su origen en un Estado distinto al chileno; (iv) y la necesidad de probar el vínculo causal sin que opere ninguna adecuación.

En cuanto a los regímenes estudiados sobre esta materia, nos encontramos, por un lado, con la regulación del ordenamiento estadounidense, que contiene muy pocas normas destinadas a regular los problemas de responsabilidad civil a los que puede dar origen el uso de la IA, de modo que la protección al consumidor descansa principalmente en interpretaciones extensivas de la magistratura; y, por otro, con la regulación europea, que propone abordar todos estos problemas mediante un régimen normativo especial, que los jueces han de seguir directamente sin necesidad de recurrir a criterios laxos.

Teniendo a la vista todo lo analizado en el Capítulo II respecto de las dificultades que las reglas generales de responsabilidad civil de nuestro ordenamiento presentan para adecuarse a las particularidades de la IA, y considerando que Chile posee un sistema de derecho continental en el que los precedentes jurisprudenciales, al menos en principio, carecen de valor extensivo y vinculante, pareciera ser que lo más óptimo para nuestro país es consagrar un régimen normativo similar al propuesto en la Unión Europea.

En efecto, una delimitación y adecuación normativa en esos términos facilitaría al consumidor la identificación del agente responsable y la prueba del vínculo causal cuando resulte dañado por IA, otorgándole un alto grado de certeza jurídica. Ahora bien, como se señaló en su momento, las normas europeas que rigen a este respecto facilitan el acceso a la prueba al consumidor y permiten que operen presunciones, pero ello es así solo el consumidor logra demostrar la infracción concreta del proveedor y su probabilidad de incidencia en los daños.

Para evitar que esto genere desprotección en los consumidores, proponemos complementar el régimen europeo, explicitando que la sola infracción a una norma que tiene por finalidad evitar la producción de ciertos daños es suficiente para que pueda considerarse razonablemente probable que, en el evento de que dichos daños se materialicen, la culpa influyó en ello. De este modo, el consumidor solo deberá acreditar la infracción del proveedor y la finalidad del precepto infringido, sin necesidad de demostrar la probabilidad cierta de que

una acción u omisión del proceso de toma de decisión de la IA haya derivado en la ocasión de los perjuicios que se alegan.

Por otro lado, cabe destacar que la normativa europea evita que el consumidor se encuentre obligado a recurrir a derecho extranjero para hacer efectivo su derecho a indemnización, pues indica que los daños siempre podrán perseguirse al amparo de la normativa en donde se han ocasionado los daños, con prescindencia del domicilio del proveedor o del lugar en que tuvo lugar la fabricación del sistema dañoso.

En Chile, esto último solo puede ser logrado mediante norma jurídica expresa, ya que, mientras no exista norma interna, la determinación del tribunal competente y del derecho aplicable seguirá quedando a merced del tratado internacional que existe sobre la materia (Código de Bustamante)[745].

Por su parte, los criterios estadounidenses, si bien hacen sentido en un sistema propio del *common law*, no serían adecuados en nuestro ordenamiento, toda vez que, a la luz de lo previsto en el artículo 3 del Código Civil chileno[746], nada garantiza que los jueces vayan a adoptar criterios extensivos o adecuaciones al régimen de responsabilidad general en tanto en cuanto ello no esté consagrado expresamente en la ley.

Con todo, respecto del tema específico de la responsabilidad de los intermediarios, si lo que se quiere es proteger a los consumidores y evitar que las plataformas posean una inmunidad amplia al momento de utilizar IA, podría resultar más conveniente –en comparación con los criterios europeos– tomar como inspiración la normativa estadounidense, y, particularmente, la interpretación doctrinaria y las propuestas que se han desarrollado a propósito del alcance de la sección 230 de la Communications Decency Act of 1996[747].

---

[745] Por lo demás, cabe tener presente que este Código es un Anexo de la Convención de la Habana de 1928, que solo fue ratificada por países americanos, de modo que la situación seguiría siendo compleja si el proveedor llegase a desempeñar sus funciones en otro continente.

[746] Este artículo señala: "*Sólo toca al legislador explicar o interpretar la ley de un modo generalmente obligatorio. Las sentencias judiciales no tienen fuerza obligatoria sino respecto de las causas en que actualmente se pronunciaren*". DFL 1, que Fija Texto Refundido, Coordinado y Sistematizado del Código Civil; de la Ley Nº4.808, Sobre Registro Civil, de la Ley Nº17.344, que Autoriza Cambio de Nombres y Apellidos, de la Ley N°16.618, Ley de Menores, de la Ley N°14.908, sobre Abandono de Familia y Pago de Pensiones Alimenticias, y de la Ley N°16.271, de Impuesto a las Herencias, Asignaciones y Donaciones, Santiago, Ministerio de Justicia, 30 de mayo de 2000. Artículo 3.

[747] CONGRESO de los Estados Unidos (Estados Unidos). Communications Decency Act of 1996. Washington D.C., Estados Unidos, 08 de febrero de 1996.

Al efecto, recordemos que en Estados Unidos se ha señalado que el hecho de que el proveedor utilice algoritmos de recomendación u otros sistemas automatizados no es razón suficiente para entender que queda cubierto de una presunción de exención de responsabilidad, toda vez que carece de neutralidad suficiente frente a su uso.

Considerando que la delimitación de la responsabilidad de los intermediarios en nuestro ordenamiento es más difícil de construir que la responsabilidad del proveedor directo –incluso si se incorporasen las normas europeas–, la consagración de una exención amplia dificultaría aún más a los consumidores hacer valer su derecho a indemnización. Por ello, estos autores se inclinan por indicar que, si bien el régimen de responsabilidad europeo contiene disposiciones que se adecúan mejor a las necesidades de nuestro ordenamiento, en lo que atañe a la responsabilidad de los intermediarios es más conveniente recurrir como inspiración a los criterios estadounidenses.

Ahora bien, vale tener presente que los criterios norteamericanos que evitan la operación de una exención de responsabilidad amplia para los intermediarios que emplean IA, han sido desarrollados por la doctrina y aún no poseen reconocimiento legal. Ello puede hacer sentido en un sistema jurídico de *common law*, pero en un ordenamiento como el nuestro, lo recomendable es que se deje constancia legal del criterio. En ese sentido, más que replicar la regla de la sección 230, lo que hay que tener a la vista es el desarrollo que se ha generado al respecto.

Asimismo, cabe destacar que en Europa, si bien las reglas previstas en los artículos 4 a 6 del DSA otorgan menor protección frente al uso de IA, se ha desarrollado una interpretación doctrinaria que entiende, en base al artículo 7 del mismo cuerpo normativo, que el intermediario solo puede ser exonerado de responsabilidad si fue diligente en el cumplimiento del resto de las obligaciones de transparencia e información que prevé la normativa[748]. En ese sentido, podría recurrirse a este criterio para complementar el régimen.

En suma, para solucionar los problemas de responsabilidad de la IA a los que da lugar la normativa chilena, lo óptimo es incorporar, por una parte, las normas europeas relativas a

[748] DE MIGUEL ASENSIO, Pedro. *Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales*. La Ley Unión Europea. (109), p. 10.

la identificación del agente, delimitación de la protección territorial del consumidor y prueba de la causalidad (con las precisiones que se indicaron); y, por otra, los criterios estadounidenses desarrollados en torno a la responsabilidad de los intermediarios, pero asegurándose de que queden plasmados en normas legales y complementando con la doctrina europea.

II. Protección de datos personales

Como ya se mencionó, en el Capítulo II, al momento de examinar lo que ocurre en el ordenamiento jurídico chileno entre el derecho a la vida privada y el tratamiento de datos personales, se identificaron tres materias que han sido abordadas de manera compleja o, más bien, difusa, por el legislador: (i) obligaciones de los proveedores que tratan datos personales; (ii) tratamiento automatizado de datos personales; y (iii) tutela de los consumidores en materia de protección de datos.

En lo que respecta a las obligaciones de los proveedores, es posible señalar enfáticamente que la normativa europea -actual- es mucho más exhaustiva, en tanto se preocupa de regular de manera detallada una serie de obligaciones, entre las que se encuentran las de información, de seguridad y de evaluación de impacto, y, además, pone especial énfasis en aquellos casos en que se trata de industrias de alto riesgo y respecto de los guardianes de acceso.

Por su parte, la normativa norteamericana, a juicio de los autores de esta Memoria, no contempla una sistematización de las obligaciones que pesan sobre aquellos proveedores que tratan datos personales, sino que se enfocan, en general, en delegar a diversas entidades la emisión de regulaciones en la materia. Ahora bien, aquello no significa que Estados Unidos no se preocupe de la materia. De hecho, el Proyecto de Ley ADPPA viene no solo a regular la protección de datos personales, sino que, aún más específicamente, viene a hacerlo en contexto de la IA, lo que podría representar una mejora en términos de claridad y enfoque.

Lo anterior, en tanto la propuesta, como se señaló en la sección anterior, tiene dentro de sus objetivos objetivo proporcionar derechos fundamentales de privacidad de datos a los consumidores[749], propósito en virtud del cual establece una serie de principios que los

[749] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.8152 - American Data Privacy and Protection Act.* Washington D.C., Estados Unidos, 21 de junio de 2021, p.1.

proveedores deben respetar al tratar datos personales, tales como minimización de datos, deberes de lealtad, protección por diseño, lealtad a las personas físicas en materia de fijación de precios, transparencia y seguridad, entre otros[750].

En cuanto a la elaboración de perfiles y publicidad personalizada, es dable afirmar que ninguno de los dos ordenamientos contempla una regulación suficientemente protectora de los consumidores en el asunto –al menos no en la práctica–. Por un lado, la legislación de la UE se preocupa de otorgar a los consumidores el derecho a no ser objeto de decisiones basadas únicamente en el tratamiento de datos automatizados, pero contempla excepciones tan amplias que, finalmente, se convierten en la regla general.

Y, respecto a la publicidad personalizada, aquella solo está regulada a propósito de los prestadores de plataformas en línea, por lo cual, a contrario sensu, tal normativa no se aplica a quienes no prestan sus servicios por tal vía, pero sí los publicitan por aquel medio, lo que es, a todas luces, insuficiente en la actualidad, en que la publicidad en papel está, prácticamente, obsoleta.

Por su parte, la normativa estadounidense no contempla normas positivas en la materia, sin perjuicio de que, mediante la ADPPA, se pretende establecer una serie de disposiciones específicas respecto a la toma de decisiones automatizadas y, asimismo, regular lo que es la publicidad personalizada. Al respecto, resulta aconsejable tener a la vista aquellas disposiciones que establecen una serie de requisitos para proporcionar publicidad dirigida y, también, aquellas que otorgan a los titulares de datos personales los derechos de (i) optar por no recibir publicidad personalizada; y, (ii) oponerse a la transferencia de sus datos.

En cuanto a lo que es la tutela de los consumidores relativa a sus datos personales, la normativa de la UE contempla una serie de derechos bastante específicos que permite a los consumidores decidir qué hacer con sus datos y, más importante aún, se otorga a los consumidores derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna y, también, contra un responsable o encargado del tratamiento de sus datos personales.

---

[750] *Ibíd*.

Por el contrario, en Estados Unidos no se contempla un régimen específico de tutela de los consumidores en caso de que sus derechos relativos a los datos personales de los que son titulares. Más bien, aquello pretende regularse recién con la entrada en vigencia de la ADPPA, que establece a los titulares de datos el derecho a ejercer una acción civil contra una empresa o proveedor de servicios por una violación de la Ley o un reglamento promulgado bajo la Ley y que tal puede ser presentada en cualquier tribunal federal de jurisdicción competente.

En este contexto, es fundamental tener en consideración, a la hora de regular la materia en el ordenamiento jurídico chileno, que, si bien Unión Europea ha demostrado un enfoque más proactivo y detallado en la protección de los datos personales de los consumidores, Estados Unidos está avanzando hacia una regulación más específica, especialmente en el contexto de la IA.

Lo anterior, dado que la elección del régimen más adecuado para Chile debe considerar no solo la claridad y exhaustividad de las regulaciones, sino también su capacidad para proteger efectivamente los derechos de los consumidores en un entorno cada vez más influenciado por la IA. En ese sentido, es deseable mezclar la exhaustividad y detalle de la Unión Europea, con el enfoque focalizado a las tecnologías automatizadas y el consumo que adopta Estados Unidos.

III. Transparencia

Para efectos se prever qué estándares resultaría más óptimo replicar de cara a una futura regulación en Chile, se distinguirá entre la transparencia exigible a los prestadores directos del servicio y aquella exigible a los intermediarios, ya que tanto la regulación europea como la regulación norteamericana coinciden en que el grado de transparencia debido varía según si la entidad comercializa bienes propios o de terceros.

En cuanto a la transparencia debida por los prestadores directos del servicio, el ámbito de aplicación de la misma pareciera estar mejor logrado en la normativa estadounidense, por cuanto precisa que los deberes aplican a todo tratamiento automatizado que efectúe procesos de decisión críticos, con independencia de la denominación que se le dé a la tecnología y del

riesgo abstracto que, desde el punto de vista de la destinación pensada por el proveedor, se asocie al sistema empleado[751].

En cambio, en la Unión Europea, la transparencia aplica únicamente si el proveedor aplica sistemas de IA de alto riesgo. Considerando la crítica que se formuló sobre la forma en que se efectúa tal categorización, así como el hecho de que la referencia a "sistemas automatizados" –en lugar de "IA"– permite hacer frente a eventuales evoluciones tecnológicas o cambios de paradigma, conviene que en Chile el ámbito de aplicación de los deberes de transparencia siga los lineamientos propuestos en Estados Unidos.

Con todo, una cuestión es analizar el ámbito de aplicación de los deberes de transparencia, y otra cuestión es ver qué deberes concretos de transparencia resulta deseable exigir al proveedor. Si bien no se discute que el ámbito de aplicación está mejor precisado en la normativa estadounidense, los deberes de transparencia en sí están bastante más desarrollados en la regulación europea.

En efecto, en Europa se busca obligar a los proveedores a comunicar directamente a los consumidores información pertinente sobre sus sistemas de IA y el funcionamiento de los algoritmos de recomendación, lo que les permite adquirir conciencia acerca de la tecnología con la que están interactuando y los eventuales riesgos a los que se ven expuestos sus derechos.

En Estados Unidos, en tanto, la transparencia es más indirecta, desde que la información es comunicada, en su mayoría, a las autoridades administrativas, y estas emiten informes restringidos, limitados y censurados que contienen la información a la que finalmente accederá el consumidor. Vale decir, en Estados Unidos la mayor parte de los deberes de transparencia no suponen la comunicación de información por parte del proveedor hacia el consumidor. En su lugar, son los órganos administrativos quienes reciben reportes del proveedor, y luego se encargan de filtrar y limitar lo que llegará a conocimiento del consumidor.

[751] MÖKANDER, J., JUNEJA, P., WATSON, D.S. y FLORIDI, L., 2022. The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other? [en línea] Minds and Machines, Agosto-2022, Vol. 32, n°. 4 <https://link.springer.com/article/10.1007/s11023-022-09612-y> [consulta: 18 octubre 2023]. p. 753.

Desde luego, puede resultar útil que diversos organismos públicos especializados tengan acceso a la información de los sistemas de IA empleados por los proveedores, pues, a fin de cuentas, al tratarse de entidades técnicas, es probable que entiendan y utilicen esa información de un mejor modo que los consumidores.

No obstante, no debe olvidarse que quienes se exponen directamente a los riesgos de la tecnología no son los organismos públicos, sino los propios consumidores. En ese sentido, parece un tanto paternalista encargar a los organismos la protección de los consumidores sin siquiera permitir que estos últimos sepan con precisión de qué y cómo se les está protegiendo.

Además, la transparencia administrativa y la transparencia al público no son excluyentes entre sí. Tal como demuestra la normativa europea, es perfectamente posible que toda la información –quizás con algún grado sutil de diferencia– sea conocida tanto por los organismos públicos como por los consumidores.

En consecuencia, no hace falta evitar que los consumidores accedan a la información para que los organismos públicos se preocupen de protegerlos. Por el contrario, si lo que se quiere es que los consumidores entiendan y sean verdaderamente autónomos, lo mínimo es permitir que ellos también tomen conocimiento de la información, procurando mezclar ambos enfoques.

A mayor abundamiento, cuando la información del funcionamiento del sistema IA es comunicada a los usuarios en forma indirecta y restringida, no hay transparencia algorítmica propiamente tal, puesto que esta supone que las decisiones tomadas por los algoritmos sean visibles para quienes se ven directamente afectados por su funcionamiento –vale decir, los consumidores–[752]. Y en este caso, la visibilidad completa solo llegaría a conocimiento de las autoridades. Para evitar tal problema, el régimen de transparencia que se consolide en Chile debe permitir que los consumidores tengan un acceso directo a la información –dejando a salvo, por cierto, ciertos antecedentes confidenciales–.

[752] BELL, Andrew; STOYANOVICH, Julia; NOV, Oded. *Algorithmic Transparency Playbook*. [en línea] Center for Responsible AI. 2022 <https://dataresponsibly.github.io/algorithmic-transparency-playbook/resources/transparency_playbook_camera_ready.pdf> [consulta: 12 noviembre 2023]. p. 5.

Por otra parte, en cuanto a la transparencia exigible a los proveedores intermediarios, ambos regímenes son buenos, en el sentido de que establecen con precisión cierta información relevante que el intermediario debe comunicar directamente a los usuarios, en circunstancias que nuestro ordenamiento dice muy poco sobre la materia. Así, en las normativas extranjeras encontramos, principalmente, deberes de transparencia en relación a los sistemas de recomendación, clasificación, perfilamiento y moderación de contenidos.

Antes de describir las diferencias de cada régimen y dilucidar qué normas se ajustan mejor a los desafíos que presenta la regulación chilena, conviene advertir que tanto la normativa europea como la estadounidense coinciden en que a los intermediarios les resulta exigible una transparencia mayor que a los prestadores directos.

En efecto, en ambos casos, los intermediarios no solo quedan sujetos a los deberes generales de transparencia aplicables a los prestadores directos –en la medida en que usen procesos de decisión críticos o sistemas de IA de alto riesgo, dependiendo del régimen–, sino también a ciertos deberes de transparencia especiales. Estos autores creen que tal enfoque legislativo es correcto y debe ser replicado en Chile por tres razones.

En primer lugar, atendido que las normas chilenas sobre responsabilidad de los intermediarios son bastante difusas[753], y lo seguirán parcialmente siendo aun en el evento que se incorporen los criterios internacionales estudiados, resulta deseable que, como contrapartida, se exija a las plataformas un mayor nivel de transparencia que a aquellos prestadores directos cuyas delimitaciones de responsabilidad son más claras.

En segundo lugar, cabe tener en cuenta que el régimen de protección previsto en la LPDC, según se precisó en el capítulo I de la presente Memoria, resulta aplicable únicamente en las interacciones entre proveedores y consumidores. Por consiguiente, el consumidor solo gozará de los derechos previstos en tal normativa cuando el intermediario sea, a su turno, un proveedor.

[753] Para un estudio acabado sobre las dificultades que ofrece el régimen de responsabilidad de los intermediarios y las diversas exigencias que prevé el artículo 43 LPDC actual para su configuración, véase: ZUMARÁN, M.G. y ALONZO, MEJÍAS. El proveedor intermediario de servicios y su responsabilidad. Un estudio del artículo 43 de la Ley 19.496. en línea] Revista de Derecho, 2021, Vol. 34, n° 2, pp. 29-50 <https://www.scielo.cl/scielo.php?pid=S0718-09502021000200029&script=sci_arttext&tlng=pt> [consulta: 03 noviembre 2023]. pp. 39-46.

Al respecto, el artículo 1 Nº2 de la LPDC establece que son proveedores "*las personas naturales o jurídicas, de carácter público o privado, que habitualmente desarrollen actividades de producción, fabricación, importación, construcción, distribución o comercialización de bienes o de prestación de servicios a consumidores, por las que se cobre precio o tarifa*"[754].

Si bien es esperable que, merced de la amplitud de la definición, en la mayoría de los casos quien intermedia pueda ser calificado como un proveedor, también es posible que la plataforma no reúna todos los requisitos de la definición (por ejemplo, debido a que no cobra precio ni tarifa por su servicio). De ser así, los consumidores quedarían desprotegidos no solo por la imposibilidad de perseguir la responsabilidad civil del intermediario, sino porque no aplicará ninguno de los derechos y deberes previstos en la LPDC. Al existir tal contingencia de desamparo, se justifica que los intermediarios deban una mayor transparencia que los proveedores directos respecto de los sistemas de IA que emplean.

En tercer lugar, la propia actividad de intermediación suscita dudas acerca de la neutralidad que pueda tener la plataforma al utilizar tecnologías automatizadas. En el caso de los proveedores directos, no es una novedad que empleará sus tecnologías para promocionar sus propios bienes o servicios; mientras que en el caso de los intermediarios, no queda claro si en su labor de acercar a las partes[755], tendrá alguna prioridad o preferencia en la clasificación y/o en la selección de aquellos proveedores que desea conectar con el consumidor. De ahí que se vuelva deseable una mayor transparencia sobre los sistemas y criterios empleados.

Pues bien, aclarada la necesidad de que en Chile se siga la idea de que los intermediarios deben cumplir con mayores deberes de transparencia, corresponde examinar qué exigencias especiales de transparencia previstas en la normativa extranjera resulta más atingente replicar en Chile a la luz de las particularidades de nuestra normativa.

Al respecto, ha de advertirse que el régimen europeo es un tanto más completo que el estadounidense, toda vez que se preocupa de tratar expresamente el fenómeno de la clasificación. Además, el nivel de información que se exige comunicar a los usuarios es mayor;

[754] CHILE. Ley Nº 19.496 que Establece Normas sobre Protección de los Derechos de los Consumidores, Santiago, Ministerio Secretaría General de la Presidencia, 07 de febrero de 1997. Artículo 1 Nº2.
[755] PALOMARES, Elena. *La intermediación en los contratos de consumo.* Tesis (Doctorado en Derecho con mención en Doctorado Europeo). Barcelona, España. Universidad de Barcelona, Facultad de Derecho, 2014. pp. 105-108.

lo que permite –o al menos vuelve probable– que los consumidores entiendan en forma más íntegra las implicancias del sistema automatizado con el que interactúan.

Considerando la desprotección de los consumidores chilenos ante los intermediarios, estos autores estiman conveniente que en nuestro país se consagren deberes especiales de transparencia similares a los de la Unión Europea. De este modo, los usuarios podrán tener certezas sobre el grado de neutralidad del proveedor.

Sin perjuicio de lo anterior, a fin de fortalecer la posición de los consumidores frente a todo tipo de plataformas, lo deseable sería que, junto con las reformas que introduzcan deberes de transparencia, se reforme el concepto de proveedor, a fin de permitir que los intermediarios encajen en la definición a todo evento. Se volverá sobre este punto al abordar las “Propuestas para Chile” en la parte final del presente subcapítulo.

IV. Auditoría algorítmica

Al momento de analizar el alcance de la auditoría algorítmica en este Capítulo, se explicó que ni el régimen europeo ni el régimen norteamericano establecen una obligatoriedad general de que los proveedores se sometan a auditorías algorítmicas. Ambos sistemas contemplan únicamente algunas hipótesis específicas en las cuales la auditoría podría ser exigible. Estas hipótesis se vinculan a plataformas de muy gran tamaño –sea por sus ingresos, por la cantidad de datos que manejan o por los usuarios asociados–.

En ese sentido, no encontramos diferencias significativas entre las normativas, puesto que tanto en la Unión Europea como en Estados Unidos las auditorías algorítmicas poseen un alcance restringido. Si bien la normativa europea pareciera ser más explícita, la causal que justifica someterse a auditorías es prácticamente la misma en ambos ordenamientos: ser una plataforma de muy gran tamaño.

Habida cuenta de lo anterior, surge la pregunta de si ese es el estándar que debiésemos tener a la vista, o, en cambio, corresponde otorgar un alcance distinto en nuestro ordenamiento. No es una pregunta fácil de contestar considerando que se trata de una materia emergente, respecto de la cual aún existe un exiguo desarrollo legislativo. Empero, si se hace un balance entre lo examinado en el Capítulo II y lo hallado en la normativa extranjera

estudiada, es posible aventurarse a señalar que hay dos premisas sobre las cuales debiese descansar un buen régimen.

En primer lugar, ha de tenerse presente que la auditoría algorítmica constituye algo beneficioso para los consumidores. En efecto, permite que exista un control sobre el grado de justicia y equidad de los algoritmos empleados, de modo que los consumidores y/o los organismos públicos puedan dimensionar los riesgos que el sistema presenta en la práctica[756].

En segundo lugar, debe aplicarse un principio de proporcionalidad. Si bien no se discute que la auditoría algorítmica es beneficiosa para los consumidores, por temas de costo y tiempo no parece razonable que esta conducta sea exigible a toda clase de proveedores, ya que los proveedores pequeños o que emplean sistemas sin ningún tipo de riesgo deberán rendir complejas cuentas, en circunstancias que de ello podría no derivarse ningún beneficio social.

Por lo mismo, tanto la normativa estadounidense como la europea buscan un equilibrio: obligan a hacer auditorías algorítmicas –pues los legisladores entienden que es algo que beneficia a los consumidores–, pero solamente la convierten en una conducta exigible en aquellos casos en que realmente se justifique establecer dicha obligación. Ello ocurrirá cuando se está ante plataformas de muy gran tamaño.

A los autores de la presente Memoria les parece bien dicho criterio de proporcionalidad, pero estiman que admite críticas y puede ser complementado sin temor a incurrir en costos injustificados. Una buena idea podría ser entender que no solo aplica a plataformas de gran tamaño, sino a todo proveedor de gran tamaño. Vale decir, recoger en nuestro ordenamiento el criterio del tamaño de la entidad, pero hacerlo extensible no solo a las plataformas intermediarias, sino también a quienes prestan directamente el servicio.

En el apartado anterior sobre transparencia, se siguió la postura de que los intermediarios deben estar sujetos a mayores deberes que los prestadores directos. No se ha desistido de tal planteamiento. Sin embargo, ha de tenerse en consideración que las auditorías

[756] KASSIR, Sara. *Algorithmic Auditing: The Key to Making Machine Learning in the Public Interest*. [en línea] IBM Center for The Business of Government. Viewpoints. Winter 2019/2020. <https://www.businessofgovernment.org/sites/default/files/Algorithmic%20Auditing.pdf> [consulta: 11 noviembre 2023]

algorítmicas persiguen, entre otras cosas, evaluar impactos en materia de precisión, sesgos, justicia, discriminación, privacidad y seguridad, así como brindar recomendaciones sobre métricas específicas[757]. Vale decir, lo que está en juego es la seguridad e integridad de los propios usuarios.

Esta seguridad se ve expuesta tanto en sistemas empleados por intermediarios como en aquellos utilizados por prestadores directos. Y siendo así, no se aprecia razón para entender que las entidades de gran tamaño estarán sujetas a auditorías únicamente si son plataformas o intermediarios, máxime considerando que la normativa chilena actual no establece ningún grado de protección en este sentido, incluso si se ha configurado una relación de consumo.

Así también, junto con atender al tamaño de la entidad, resultaría útil tener presente el riesgo del sistema de IA empleado, ya que habrá situaciones en las que, no obstante que el proveedor sea pequeño, la tecnología empleada resultará muy lesiva, en cuyo caso los riesgos podrán ser incluso de mayor entidad que los ocasionados por una empresa que maneja grandes volúmenes de información.

Por último, un aspecto que las normativas extranjeras abordan a propósito de los límites de la transparencia, pero que no replican respecto de la obligación de realizar auditorías algorítmicas, es la eventual confidencialidad de los resultados y las tensiones que su publicidad produce con la propiedad intelectual y los secretos comerciales o empresariales.

Al respecto, aun cuando las normativas de inspiración no lo expliciten, es menester que el régimen consagrado en Chile propenda a un equilibrio entre el conocimiento de los resultados de la auditoría y la confidencialidad de los resultados. Ello no supone entender que las auditorías nunca serán públicas. Por el contrario, por regla general, debiesen serlo, y para restringir su publicidad no bastará con que el titular aduzca que la información contenida en la auditoría es secreta o confidencial[758], sino que deberá concurrir alguna causal específica (por

[757] ARÁNGUIZ, Matías. *Auditoría algorítmica para sistemas de toma o soporte de decisiones.* Washington DC, Banco Interamericano de Desarrollo, 2020. pp. 4-6.
[758] AZUAJE, Michelle y FINOL, Daniel. *Transparencia algorítmica y la propiedad intelectual e industrial: tensiones y soluciones*. La Propiedad Inmaterial (30): p 122, 2020.

ejemplo, que su revelación afecte el desenvolvimiento competitivo de la empresa[759], incida adversamente en la continuidad operacional del sistema o afecte la eficacia del servicio[760]).

Pero todavía una regla de ese estilo sigue siendo perfectible. En efecto, si la auditoría llegase a contener información respecto de la que incurre causal de reserva o confidencialidad, ello no debiese suponer la falta de publicidad total de la auditoría. Lo deseable, en cambio, es que se permita la publicidad parcial de la auditoría, eliminando o censurando específicamente aquellos antecedentes que son reservados o confidenciales.

De este modo, se lograría un buen equilibrio entre el derecho a la confidencialidad y el deber de transparencia que recae en las auditorías. Es una solución similar a la que adopta nuestro ordenamiento en litigios de libre competencia. En esta sede, cada vez que hay un documento confidencial, se ordena la elaboración de versiones públicas en las que deben censurarse únicamente los pasajes confidenciales del documento, dejando al descubierto aquellos antecedentes que no lo son[761]. Así, se distingue según la naturaleza de la información y se logra un equilibrio entre los intereses en juego.

V. Otros controles en el uso de la IA

En la primera parte del Capítulo IV, se explicó que esta materia, al incluir todo tipo de control en el uso de la IA (administrativo, legal, humano, etc.) que no diga relación con la responsabilidad civil, la transparencia, la auditoría algorítmica ni los datos personales, puede ser bastante amplia.

Sin embargo, teniendo en cuenta los derechos de los consumidores que no quedan del todo cubiertos con los otros deberes, así como lo que indica la regulación comparada al respecto, en general, se asocia a la proscripción de ciertos sistemas de IA cuyo uso puede resultar muy dañino, y a deberes de diligencia que el proveedor debe observar al emplear aquellas tecnologías que sí están permitidas.

---

[759] *Ibíd*., p. 122.
[760] ARÁNGUIZ, Matías. *Auditoría algorítmica para sistemas de toma o soporte de decisiones.* Washington DC, Banco Interamericano de Desarrollo, 2020. p. 14.
[761] Véase artículo 22 DL 211 y Auto Acordado 16/2017 TDLC.

En cuanto a la proscripción de ciertos sistemas de IA, tanto la regulación norteamericana como la regulación europea identifican tecnologías automatizadas cuyo uso no será permitido debido a su alto riesgo. En el caso de Estados Unidos, las prohibiciones van asociadas a aquellos sistemas automatizados que segreguen, discriminen o de otro modo hagan no disponibles ciertos bienes, servicios o ventajas sobre la base de la raza, color, etnia, religión, origen nacional, sexo, género, identidad de género, orientación sexual, estado familiar, información biométrica o discapacidad real o percibida de un individuo o clase de individuos. Vale decir, restringe la prohibición a los sistemas que discriminan en forma arbitraria.

En cambio, en el caso de la Unión Europea, las prohibiciones se vinculan a aquellos sistemas que representan un riesgo para derechos que van más allá de la proscripción de la discriminación arbitraria. En efecto, no solo se protegen derechos civiles, sino también la autonomía e integridad del consumidor, al prohibir el uso "*de técnicas subliminales que trasciendan la conciencia de una persona para alterar de manera sustancial su comportamiento de un modo que provoque o sea probable que provoque perjuicios físicos o psicológicos a esa persona o a otra*"[762].

En aras de alcanzar un mayor grado de protección de los consumidores, resulta deseable replicar en Chile el enfoque adoptado por la Unión Europea, ya que, junto con prohibir sistemas riesgosos para ciertos derechos civiles, impide el uso de sistemas que pueden afectar algunos derechos importantes de los consumidores –aun cuando no sean derechos civiles o fundamentales propiamente tal–. De este modo, la regla de prohibición tiene en cuenta el bienestar directo de los usuarios, lo que contribuye a que exista una mayor protección hacia quienes interactúan con las tecnologías de IA.

Sin embargo, la consagración legal de este enfoque basado en el riesgo ha recibido ciertas críticas por parte de la doctrina. En concreto, se ha señalado que la calificación del riesgo atiende únicamente al fin que el proveedor prevé para el sistema, sin considerar el uso razonablemente probable que se espera que adopten los consumidores[763]. Los autores de

[762] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021. Artículo 5.1 letra a).
[763] HELBERGER, N. y DIAKOPOULOS, N. *ChatGPT and the AI Act.* [en línea] Internet Policy Review, 16 Feb 2023, Vol. 12, n° 1 <https://policyreview.info/essay/chatgpt-and-ai-act> [consulta: 26 noviembre 2023]. p. 3. Sobre este

esta Memoria proponen replicar la norma europea, pero complementarla a la vista de esta crítica. Una buena forma podría ser que el riesgo se califique atendiendo al impacto probable en los derechos de los consumidores y a un uso alternativo que se espera que le den.

Por otro lado, en cuanto a los deberes de diligencia, ambos sistemas se preocupan de establecer obligaciones de evaluar riesgos e impactos, tanto en forma previa a introducir el sistema de IA al mercado como una vez que este ya se encuentra en funcionamiento. Sin embargo, ocurre algo similar a lo que pasa con los deberes de prohibición.

Si bien las normativas coinciden en que los proveedores que emplean IA deben mitigar los peligros para los derechos civiles de los usuarios y garantizar que los sistemas sean idóneos para su uso, hay una (en este caso la estadounidense) que propone reglas específicas que, junto con procurar proteger derechos civiles, atienden directamente a los derechos de los consumidores.

Vale decir, las normativas son similares, pero la estadounidense busca consagrar deberes de diligencia adicionales destinados a proteger directamente los derechos de los consumidores. A modo de ejemplo, la sección 3A letra H de la *Algorithmic Justice and Online Platform Transparency Ac*t, que es una propuesta normativa en curso, indica que los proveedores que queden cubiertos por la legislación deben realizar evaluaciones de impacto tendientes a detectar y eliminar o mitigar, de manera oportuna, cualquier proceso de decisión crítica que demuestre un probable efecto negativo material, jurídico o significativo en la vida de un consumidor[764].

Así las cosas, los autores de la presente Memoria defienden la postura de que en Chile deben consagrarse normas que refieran, por una parte, a la prohibición de usar ciertos sistemas de IA, adoptando un enfoque basado en el riesgo, pero explicitando que dicho riesgo debe ser determinado en base a los derechos de los consumidores[765]. y, por otra, al cumplimiento de deberes de diligencia que permiten detectar y eliminar o mitigar riesgos,

punto, nos remitimos a lo analizado en el subcapítulo anterior al momento de examinar las normas de "Otros controles de la IA" de la Unión Europea.

[764] CONGRESO de los Estados Unidos (Estados Unidos). *S.2325 - Algorithmic Justice and Online Platform Transparency Act.* Washington D.C., Estados Unidos, de 13 de julio de 2023. Sección 3A.

[765] HELBERGER, N. y DIAKOPOULOS, N. *ChatGPT and the AI Act.* [en línea] Internet Policy Review, 16 Feb 2023, Vol. 12, n° 1 <https://policyreview.info/essay/chatgpt-and-ai-act> [consulta: 26 noviembre 2023]. p. 3.

procurando resguardar la autonomía, la privacidad y la integridad de los consumidores, que son los derechos potencialmente más afectados según de examinó en el Capítulo II.

Sin perjuicio de lo anterior, la normativa chilena ha de ser complementada en un aspecto del que las normativas europeas y norteamericanas no se hacen cargo. Se trata de tener presente que, si bien las obligaciones de diligencia recaen jurídicamente en el proveedor, es altamente probablemente que estos recurran a asistencia especializada para cumplir con algunos de tales deberes, puesto que lo habitual es que la tecnología haya sido desarrollada por expertos cuyo giro profesional se vincula a la informática[766].

La doctrina europea llega a la conclusión de que la normativa continental no impide tal delegación, de modo que no hay óbice para que el proveedor pida ayuda o encargue a un tercero experto el cumplimiento de ciertas diligencias tecnológicas que exige la normativa[767]. Los autores de la presente Memoria creen que en Chile tampoco debiese prohibirse la subcontratación o la ayuda en el cumplimiento de deberes normativos, según se argumentó en el subcapítulo anterior.

Pero el problema es que, dado que existe esa posibilidad –y que es de esperar que sea lo más frecuente–, surge la pregunta de qué puede hacer el consumidor si el proveedor encargó el cumplimiento normativo de ciertas diligencias y el tercero incumplió o perjudicó directamente al usuario. Es algo que en un ordenamiento jurídico de derecho continental como el nuestro, difícilmente podría dejarse a la discreción de los tribunales.

Al respecto, una buena idea podría ser consagrar un régimen de *culpa in eligendo*, en el que, si el tercero falla en sus labores y gracias a ello se produce una infracción o se generan daños al consumidor, el proveedor responderá directamente por ser garante de su elección de contratación; pero podrá posteriormente, si fuere el caso, repetir en contra de quién causó el daño directamente[768]. Vale decir, que el consumidor siempre pueda reclamar directamente

[766] SCHUETT, Jonas. Risk management in the artificial intelligence act. [en línea] European Journal of Risk Regulation, 08 de febrero de 2023, <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risk-management-in-the-artificial-intelligence-act/2E4D5707E65EFB3251A76E288BA74068> [consulta: 01 diciembre 2023]. p. 15.

[767] *Ibíd.*, 15.

[768] Es un régimen similar al que existe en nuestro país respecto del proveedor que emplea sistemas de vigilancia desarrollados por un tercero. Lo que se propone es crear una norma adicional que lo haga extensible a la delegación de labores relacionadas con el control de la IA. Véase: ISLER, Erika. *Derecho del consumo. Nociones fundamentales*. Valencia, Tirant lo Blanch, 2021. 217p.

ante el proveedor, pero este, a su vez, cuente con la posibilidad de exigir su responsabilidad al tercero que incumplió con las labores encargadas.

2. Propuestas para Chile

En el apartado anterior, se realizó una comparación entre las normas europeas y las normas estadounidenses, examinando en forma crítica si es que los estándares allí propuestos son adecuados, y analizando prospectivamente cómo funcionarían en el evento que sean incorporados a nuestro ordenamiento –considerando las particularidades de las normas chilenas ya vigentes–.

El objetivo de ello fue dilucidar cuál sería el contenido óptimo de un futuro régimen para Chile, que tenga en cuenta lo mejor de cada una de las normativas extranjeras estudiadas y complemente en ciertos aspectos importantes no regulados (por ejemplo, la responsabilidad por delegación en el cumplimiento de los deberes) o que admiten mejoras (por ejemplo, el alcance de las auditorías algorítmicas).

En esta instancia, el cometido dice relación con determinar la forma específica en que debiera materializarse tal contenido. Esto supone cumplir con dos pasos: en primer lugar, definir el o los instrumentos jurídicos que resulten más idóneos para introducir el nuevo régimen; y, en segundo lugar, concretizar las propuestas.

A. Instrumento Jurídico

Luego de haber determinado el contenido del nuevo régimen, surge la pregunta de qué herramientas han de utilizarse para consolidarlo (dictación de una ley nueva, dictación de un reglamento, reformas a leyes ya existentes, dictación de circulares interpretativas, incentivar la autorregulación, etc.).

Podría pensarse que basta con dictar una ley que contenga todos los estándares, derechos y deberes examinados. Sin embargo, según ha señalado la doctrina, el problema de prever una regulación legal exhaustiva sobre la IA es que las leyes son rígidas, lentas y

conservadoras, en circunstancias que esta tecnología es incipiente, cambiante y se encuentra en constante evolución[769].

Por consiguiente, aun cuando a la luz de lo estudiado en esta Memoria pueda resultar idóneo consagrar ciertos deberes y derechos especiales en la ley, existe el riesgo de que una respuesta legal extensa dificulte la innovación, no se haga cargo de problemas que se detecten en un futuro próximo y/o no se adapte a la celeridad propia de las nuevas tecnologías[770].

Ahora bien, por otro lado, si es que los derechos y deberes especiales se consagran en normas jurídicas de menor jerarquía o alcance (por ejemplo, un Reglamento o una Circular Interpretativa), o simplemente forman parte de una guía de buenas prácticas que se espera que las empresas observen, se corre el riesgo de que los consumidores se expongan a un alto grado de desprotección. En efecto, se trataría de reglas fácilmente derrotables, que incluso podrían entenderse tácitamente derogadas si entran en contradicción con normas legales.

Así las cosas, surge la necesidad de lograr un equilibrio. La regulación no debe ser excesivamente rígida, pero tampoco es dable que, con ocasión de permitir una fácil adaptación del régimen, la protección efectiva de los consumidores termine siendo una mera expectativa. A fin de hacer frente a esta tensión, existen una serie de prácticas o técnicas regulatorias que podrían implementarse en Chile.

La primera de ellas es que la IA se regule en la ley, pero consagrando principalmente máximas, principios y derechos de carácter programático, de modo que sea posible resolver escenarios no previstos por el legislador[771]. Por su parte, el detalle de los derechos y obligaciones puede quedar previsto en reglamentos a los que la ley haga expresa remisión. Así, se garantiza que una buena parte de la protección frente al uso de sistemas de IA posea rango legal, y, al mismo tiempo, pueda ser fácilmente adecuada o concretizada mediante un instrumento jurídico (Reglamento) que es bastante más flexible.

---

769 ZAROR, Danielle. *¿Por qué resulta tan problemático regular la tecnología?* En: AZUAJE Pirela, M (coord.). *Introducción a la ética y el derecho de la inteligencia artificial*. Madrid, Wolters Kluwer-La Ley, 2023. 245p.

770 ARAYA Paz, Carlos. *Desafíos legales de la inteligencia artificial en Chile.* Revista chilena de derecho y tecnología. 9 (2): pp. 282-283, 2020.

771 ZAROR, Danielle. *¿Por qué resulta tan problemático regular la tecnología?* En: AZUAJE Pirela, M (coord.). *Introducción a la ética y el derecho de la inteligencia artificial*. Madrid, Wolters Kluwer-La Ley, 2023. 246p.

Una segunda opción es que la regulación se haga por medio de una ley más exhaustiva, pero que tenga una vigencia temporal de entre uno a cinco años. Esto se conoce como *sunset law*. Es un tipo de regulación flexible que destaca por obligar al legislador a evaluar la idoneidad de la ley una vez que ha transcurrido el plazo pactado[772]. En caso de ser necesario, la ley se ajusta y comienza a regir nuevamente por un período determinado; si no, se mantiene el mismo texto y sigue rigiendo por un nuevo período fijo. De este modo, se permite que exista flexibilidad y que la norma se adecúe a la evolución y nuevos conocimientos que existan respecto de la tecnología[773].

Una tercera opción es permitir la creación de *sandbox* regulatorios, vale decir, de espacios de experimentación en los que los proveedores pueden operar temporalmente bajo ciertas reglas que están siendo sometidas a evaluación[774]. Son una especie de "prueba piloto" de norma, que permite que las empresas continúen innovando en sus productos a la vez que se evalúa el impacto o desempeño de determinadas reglas[775].

¿Qué técnica sería deseable utilizar en Chile? A juicio de los autores de la presente Memoria, lo más óptimo es combinar los enfoques regulatorios, aprovechando las ventajas de cada sistema. En concreto, se propone crear una Ley General de IA con vigencia temporal (*sunset law*), que contenga principios pero, al mismo tiempo, establezca con suficiente precisión ciertas reglas que por su relevancia han de poseer rango legal directo. Estas reglas –se propone– deberían ser aquellas relativas al régimen especial de responsabilidad para la IA, así como las referidas a deberes genéricos de transparencia, cuidado en el tratamiento de datos personales, auditoría algorítmica y otros controles.

Por su parte, los deberes más específicos pueden ser precisados en un Reglamento, e ir siendo probados mediante *sandbox* regulatorios. Este enfoque multidimensional se estima óptimo puesto que permite que los agentes del mercado tengan un rol en la regulación,

---

772 ARAYA Paz, Carlos. *Desafíos legales de la inteligencia artificial en Chile.* Revista chilena de derecho y tecnología. 9 (2): 257-290, 2020. p. 284.
773 *Ibíd*., p. 284.
774 FENWICK, Mark; VERMEULEN, Erik PM; CORRALES, Marcelo. *Business and regulatory responses to artificial intelligence: Dynamic regulation, innovation ecosystems and the strategic management of disruptive technology.* Robotics, AI and the Future of Law. Singapore: Springer Singapore, 2018, pp. 82-90.
775 ARAYA Paz, Carlos. *Desafíos legales de la inteligencia artificial en Chile.* Revista chilena de derecho y tecnología. 9 (2): p. 284, 2020.

combinando instrumentos jurídicos y procurando alcanzar la mayor protección posible para los consumidores.

Ahora bien, considerando que la propia técnica del *sunset law* permite que exista flexibilidad, lo ideal es que la ley sea relativamente autosuficiente, y el Reglamento solo explique o aclare las manifestaciones más específicas de aquellas obligaciones que fueron consagradas expresamente en la ley.

Adicionalmente, debe tenerse presente que, aunque se propone que se dicte una Ley y un Reglamento general de IA, también hay ciertas cuestiones que por su especialidad deben ser introducidas mediante reformas a la LPDC, al Reglamento de Comercio Electrónico y a la LPVP –o al respectivo proyecto de ley que crea la agencia de datos personales, si fuese aprobado–.

La futura Ley General de IA debería hacer mención a todos los deberes genéricos y consagrar expresamente el régimen especial de responsabilidad, pero los deberes de información o transparencia y los deberes específicos en el tratamiento de datos personales han de ser regulados en detalle en la LPDC y en la legislación sobre datos personales, respectivamente. La propuesta de contenido concreto de la Ley de IA y de las reformas serán examinadas a continuación.

B. Contenido concreto

En el apartado de “Análisis en base a los estándares internacionales”, se realizó una aproximación crítica a los regímenes propuestos en la Unión Europea y en Estados Unidos, determinando, respecto de cada uno de los problemas que no logran ser adecuadamente cubiertos por nuestra normativa, cuál es la mejor combinación de normas y enfoques para solucionarlos.

En algunos casos, la respuesta óptima venía dada por una sola de las normativas; en otros, por una combinación de ambas y/o por reglas adicionales que, si bien no han sido propuestas legalmente, ayudan a perfeccionar el régimen. En ese sentido, cobraron relevancia no solo las normas, sino también ciertos criterios doctrinarios.

Luego de ello, se determinaron los instrumentos jurídicos más idóneos para incorporar tal régimen. Estos instrumentos responden a un enfoque regulatorio flexible y multidimensional, que consiste en una Ley General de vigencia temporal, en un Reglamento de esa Ley y en reformas a ciertas normativas especiales de nuestro ordenamiento.

Por su parte, el presente apartado no tiene por objeto reproducir esas conclusiones ni volver a analizar las normas extranjeras, sino tomar como base el contenido que –según se argumentó en su momento– debe prever la nueva regulación chilena, sistematizarlo y explicar el modo específico en que ha de concretizarse.

Con todo, se previene al lector que, aunque se detallará cómo debiese tomar forma el contenido de la futura regulación y se propondrán reformas específicas a la LPDC, al Reglamento de Comercio Electrónico y al Proyecto de Ley sobre Datos Personales, no se pretende recomendar el articulado exacto que ha de adoptar la futura Ley general de IA o su respectivo reglamento. En cuanto a esto último, solo se abordarán los principales lineamientos y se hará referencia a determinados artículos cuya incorporación se estima esencial.

Ley General de IA

La presente investigación ha estudiado el impacto de la IA en el ámbito específico de las relaciones de consumo. Empero, no se puede desconocer que muchos de los deberes, situaciones o desafíos que supone la materia en esta sede dicen relación con el uso de IA en general, y, por lo mismo, debiesen resultar aplicables más allá de si se está en una relación de consumo o no.

Ello ocurre con la mayor parte de la normativa de responsabilidad civil de la IA, de tratamiento de datos personales, de transparencia, de auditoría algorítmica y de otros controles en el uso de la tecnología. En efecto, son cuestiones que, si bien resultan muy atingentes en las relaciones de consumo, difícilmente podrían estar totalmente reguladas en la normativa sectorial de derecho del consumidor, por cuanto su alcance va bastante más allá. De ahí que, junto con las respectivas reformas a la legislación de protección al consumidor, deban impulsarse reformas a la legislación de datos personales y abogar por la dictación de una Ley general de IA.

Ahora bien, lo anterior es sin perjuicio de que resulte deseable que existan ciertas reglas específicas a propósito de las relaciones de consumo, que tengan por función complementar y adecuar el régimen general de la IA a las particularidades que se presentan en esta clase de interacciones.

Pues bien, en cuanto al régimen general que debería preverse en la futura Ley General de IA, a juicio de estos autores, este cuerpo normativo debiese comenzar incluyendo un precepto que indique que el campo de aplicación de la ley es la IA o "cualquier tipo de tecnología automatizada". De este modo, siguiendo el criterio estadounidense, se prescinde de definiciones formales y se permite que la Ley cubra eventuales desarrollos futuros. Asimismo, debiese aclarar que, para que una tecnología quede sujeta a la Ley, lo importante es que sea utilizada o produzca efectos en Chile, con total prescindencia del domicilio de la entidad respectiva o del lugar de fabricación.

En seguida, la Ley debiese señalar que adoptará un enfoque basado en el riesgo, en el sentido de que regulará los tratamientos automatizados únicamente cuando estos efectúen procesos de decisión críticos o puedan considerarse como una "tecnología de alto riesgo", estableciendo también causales de prohibición. En cuanto a la calificación del riesgo, se sugiere tener en cuenta lo previsto en la AI Act, pero, adicionalmente, precisar que el riesgo se mide no solo en función del uso o destino aducido por quien pretende emplearla, sino atendiendo, al menos, a un uso alternativo y razonablemente probable que puedan darle los usuarios finales o consumidores[776].

Asimismo, dentro de los preceptos introductorios, se sugiere indicar que quien emplea la IA o tecnología automatizada puede delegar el cumplimiento de determinadas obligaciones normativas que, por su naturaleza, exigen conocimientos altamente especializados para poder cumplirlas (por ejemplo, algunos deberes de transparencia que sean complejos)[777]. Así, se evita caer en el problema de que el usuario acceda únicamente a la información que quien usa la tecnología está en condiciones de explicar. Ahora bien, debiera explicitarse que quien

[776] HELBERGER, N. y DIAKOPOULOS, N. *ChatGPT and the AI Act.* [en línea] Internet Policy Review, 16 Feb 2023, Vol. 12, n° 1 <https://policyreview.info/essay/chatgpt-and-ai-act> [consulta: 26 noviembre 2023]. p. 3.

[777] SCHUETT, Jonas. Risk management in the artificial intelligence act. [en línea] European Journal of Risk Regulation, 08 de febrero de 2023, <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risk-management-in-the-artificial-intelligence-act/2E4D5707E65EFB3251A76E288BA74068> [consulta: 01 diciembre 2023]. p. 15.

delega seguirá siendo responsable por el incumplimiento de los deberes, consagrando una regla de *culpa in eligendo*.

Por otro lado, debería consagrarse un sistema especial de responsabilidad que facilite la identificación del presunto agente responsable y la prueba de la causalidad a quien pretende buscar una indemnización. Como se señaló en su momento, se sugiere que este sistema sea tal cual está propuesto en la Unión Europea, pero aclarando que la sola infracción a una norma que tiene por finalidad evitar la producción de ciertos daños es suficiente para que pueda considerarse razonablemente probable que, en el evento de que dichos daños se materialicen, la culpa influyó en ello.

Adicionalmente, se sugiere consagrar deberes genéricos de transparencia y de cuidado en el tratamiento de datos personales, tales como la obligación de explicar el funcionamiento de las tecnologías empleadas y la forma en que se emplean los datos recopilados de los usuarios. Estos deberes, según se argumentó, han de ser precisados con algo más de detalle en el respectivo Reglamento de la Ley, dando ejemplos concretos y teniendo a la vista las obligaciones de información examinadas en su momento.

Junto con ello, es menester que se precise que la transparencia no solo implica comunicar la información sobre los sistemas utilizados, sino también –pensando en los fabricantes– diseñar únicamente tecnología que puedan ser supervisadas y entendidas por humanos.

Sobre la transparencia, también es importante que la Ley indique que esta será directa no solo hacia las autoridades, sino también hacia los usuarios. Vale decir, debe permitirse que los usuarios puedan acceder directamente a la información referida a las tecnologías empleadas; sin perjuicio de que pueda restringirse la publicidad de ciertos antecedentes si concurren causales de reserva o confidencialidad.

A juicio de estos autores, la Ley debe precisar únicamente los deberes de transparencia aplicables a la generalidad de entidades que emplean tecnologías automatizadas, sin establecer deberes especiales adicionales para los intermediarios. Se sugiere que estos últimos sean específicamente abordados mediante una reforma al Reglamento de Comercio Electrónico, según se detallará posteriormente.

En cuanto a las auditorías algorítmicas, se sugiere consagrar su obligatoriedad siguiendo el criterio del tamaño de la entidad, pero, a diferencia de los regímenes internacionales, sería deseable que se indique: (i) que, junto con el tamaño de la entidad, es causal para someterse a auditoría el utilizar un sistema con procesos de decisión crítico altamente peligroso; (ii) que, si concurre alguno de los dos requisitos expuestos, la entidad debe someterse a auditoría algorítmica aun si no fuese un intermediario.

Por último, en cuanto a otros controles en el uso de IA, se sugiere establecer obligaciones de realizar evaluaciones de riesgo, impacto y rendimiento, tanto en forma previa a introducir el sistema al mercado como durante el período en que este se utilice. Ello debiese consagrarse en términos similares a los regímenes estudiados, pero explicitando que las evaluaciones no solo buscan evitar riesgos hacia derechos civiles, sino también hacia cualquier otro derecho sectorial relevante, incluyendo los de los consumidores. Se recomienda seguir ese mismo criterio para determinar qué sistemas están proscritos.

Reformas a la LPDC

Como se indicó, el alcance de las diversas obligaciones atribuibles a las entidades que usan IA justifica que estas estén previstas, en su mayoría, en una legislación especial sobre las tecnologías automatizadas. Sin embargo, existen ciertos aspectos que, junto con regularse a propósito del uso generalizado de la tecnología, deben ser adecuados o complementados teniendo a la vista las particularidades de las relaciones de consumo.

Por ello, en opinión de los autores de la presente Memoria, la futura ley de IA debe ser complementada con reformas al texto actual de la LPDC. A continuación se propondrán reformas específicas a ciertos preceptos, y se sugerirá la incorporación de normas nuevas que regulan supuestos de hecho no previstos en el texto actual.

Una primera cuestión importante dice relación con la necesidad de modificar la definición de “consumidor” (artículo 1 Nº1 LPDC). El Proyecto de Ley “SERNAC Te Protege” va en el camino correcto al suprimir la exigencia de que medie un acto jurídico oneroso para que se configure una relación de consumo. No obstante, la definición continúa siendo perfectible.

En concreto, se sugiere precisar que no solo son consumidores quienes "*adquieren, utilizan, o disfrutan, como destinatarios finales, bienes o servicios*"[778], sino también quienes pretenden hacerlo. Si bien ya existe cierta doctrina que entiende que los actos que sirven de antecedente a la adquisición quedan amparados por la normativa[779], es importante consagrarlo legalmente, ya que muchas veces quien interactúa con la tecnología puede resultar dañado sin que haya alcanzado a verificarse una adquisición, uso o disfrute, y el texto legal expreso no ayuda a defender la postura de que queda amparado por la normativa.

En segundo lugar, se recomienda que la LPDC incorpore una norma que indique que el ámbito de aplicación territorial son todas las cuestiones que se susciten a propósito de las interacciones entre proveedores y consumidores en nuestro país. Una delimitación de ese estilo permitiría cubrir situaciones en que quien emplea la tecnología es una empresa con domicilio en el extranjero, pero que presta o comercializa bienes o servicios en el territorio chileno.

En tercer lugar, se sugiere que en el artículo 3 de la LPDC, así como se prevén derechos básicos especiales para los consumidores financieros, se consagren derechos especiales para los consumidores que interactúan directamente con tecnologías automatizadas. Dentro del catálogo debieran incluirse, como mínimo:

> "*(a) el derecho a ser informado sobre la circunstancia de estar actuando con un sistema de IA;*
>
> *(b) el derecho a recibir información veraz, completa y oportuna sobre el funcionamiento de la tecnología y las eventuales repercusiones en sus derechos como consumidor, incluso cuando esta se utilice únicamente para comercializar los bienes o servicios;*
>
> *(c) el derecho a saber qué datos personales emplea el sistema;*
>
> *(d) el derecho a interactuar únicamente con tecnologías que hayan sido sometidas a prueba y evaluaciones de impacto, riesgo y rendimiento de conformidad a lo previsto en la futura Ley general de IA; y*

[778] Ley Nº 19.496. CHILE. Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 07 de febrero de 1997. Artículo 1.
[779] MOMBERG Uribe, Rodrigo. *Ámbito de Aplicación de la Ley No 19.496 Sobre Protección de los Derechos de los Consumidores*. Revista de Derecho (Valdivia). 17: 2004, p.51.

(e) si la IA sea usa como asistente virtual, el derecho a acceder a un canal de atención que no se base únicamente en tecnología automatizadas; (f) el derecho a ampararse en la LPDC en aquellos casos en que se relacionó con el proveedor únicamente interactuando con el sistema de IA que él habilitó para tal efecto"[780].

La relevancia de consagrar derechos básicos estriba en que estos poseen una función esencialmente programática, de modo que ayudarían a interpretar todas las disposiciones de la ley a partir de ciertas máximas que no pueden ser vulneradas y se entienden como parte del espíritu de la legislación[781].

En cuarto lugar, se propone reformar el artículo 13 de la LPDC. Este precepto refiere a la prohibición de negativa de venta injustificada, indicando que "*Los proveedores no podrán negar injustificadamente la venta de bienes o la prestación de servicios comprendidos en sus respectivos giros en las condiciones ofrecidas*"[782]. Al respecto, considerando que es habitual que los proveedores empleen IA para tomar sus decisiones de venta, se sugiere añadir un segundo inciso que indique: "No se considerará justificada la negativa de venta por el solo hecho de que el proveedor acredite que la decisión fue tomada por un sistema automatizado"[783].

En quinto lugar, respecto del artículo 28 de la LPDC, que refiere a las reglas de publicidad engañosa, se propone consagrar expresamente que tales normas aplicarán aun cuando la publicidad en cuestión haya sido generada por un sistema de IA. Adicionalmente, teniendo como inspiración la sección 204 de la ADPPA de Estados Unidos[784], se sugiere incorporar un artículo 28 C que indique que, si la publicidad corresponde a una publicidad personalizada que fue generada a partir del tratamiento automatizado de datos, el proveedor deberá informar sobre dicha circunstancia al consumidor, otorgándole la opción de no ser objeto de publicidad personalizada.

---

[780] Propuesta propia que fue elaborada teniendo a la vista los estándares internacionales estudiados.

[781] ISLER, Erika. *Derecho del consumo. Nociones fundamentales*. Valencia, Tirant lo Blanch, 2021. 247p.

[782] Ley Nº 19.496. CHILE. Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 07 de febrero de 1997. Artículo 13.

[783] Propuesta propia.

[784] CONGRESO de los Estados Unidos (Estados Unidos). *H.R.8152 - American Data Privacy and Protection Act.* Washington D.C., Estados Unidos, 21 de junio de 2021. Sección 204.

En sexto lugar, se propone agregar un nuevo inciso al artículo 30 de la LPDC. Este precepto alude a los deberes de información respecto del precio. La idea de reforma consiste en prever que, en su caso, si el proveedor ha personalizado el precio del bien o servicio ofrecido basándose en la toma de decisiones automatizada, deberá informarle de ello al consumidor. De este modo, se consagraría una regla especial de transparencia idéntica a la previsto en el artículo 6 letra e) bis de la Directiva 2011/83 de la Unión Europea[785].

En séptimo lugar, se propone reformar el artículo 43 de la LPDC, relativo a la responsabilidad de los proveedores intermediarios. Como se comentó al momento de analizar el Proyecto de Ley SERNAC te protege, ya existe una propuesta de reforma respecto de este precepto, que indica que el proveedor intermediario no solo responderá cuando interviene en la prestación de servicios, sino también en la comercialización de bienes o servicios[786].

Sobre este punto, recordemos que el texto actual del artículo 43 indica que: "*El proveedor que actúe como intermediario en la prestación de un servicio responderá directamente frente al consumidor por el incumplimiento de las obligaciones contractuales, sin perjuicio de su derecho a repetir contra el prestador de los servicios o terceros que resulten responsables*"[787]. La propuesta de reforma contenida en el Proyecto de Ley solo cambia la frase "prestación de un servicio" por "comercialización de bienes o servicios", manteniendo idéntica el resto de la disposición.

Ello permite salvar uno de los principales problemas del artículo 43. Empero, todavía subsisten otros dos que, a juicio de estos autores, ameritan una modificación más profunda a su texto. El primer problema es que la disposición exige que el intermediario reúna, a su turno, la calidad de proveedor. Aunque lo esperable es que los intermediarios cumplan con los requisitos para ser calificados como proveedores, no siempre será así.

---

[785] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo. Bruselas, Bélgica, 2011. Artículo 6 letra e) bis.

[786] MINISTERIO de Economía, Fomento y Turismo (Chile). Proyecto de ley que mejora la protección de los derechos de las personas consumidoras en el ámbito de sus intereses individuales fortaleciendo al Servicio Nacional del Consumidor, y establece otras modificaciones que indica. Boletín N° 16.271-03. Santiago, Chile, septiembre del 2023, p. 40.

[787] Ley Nº 19.496. CHILE. Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 07 de febrero de 1997. Artículo 43.

A modo de ejemplo, esta exigencia puede derivar en que, por ejemplo, determinadas plataformas que no cobran precio o tarifa directa por la intermediación queden exentas de toda responsabilidad (por faltar un requisito para ser proveedor). En ese sentido, se propone eliminar la expresión “proveedor” de la definición.

El segundo problema es que el intermediario responde solo por el incumplimiento de sus obligaciones contractuales. Pero ¿qué pasa si el consumidor nunca suscribió un contrato con la plataforma intermediaria? En la práctica, ello podría constituir una eximente de responsabilidad, porque no habría incumplimiento alguno. Considerando que no siempre los consumidores suscriben contratos con los intermediarios, se sugiere eliminar tal exigencia del precepto, y simplemente prever que responderán por los daños causados. No es una extensión injustificada de responsabilidad si se tiene en cuenta que, en cualquier caso, podrá repetir en contra del prestador o tercero que resulte responsable.

Por último, se propone reformar el artículo 45 sobre productos peligrosos. En concreto, se plantea: (i) incluir expresamente la palabra “servicios”, de modo que no queden dudas sobre que estos también puede ser calificados como peligrosos –actualmente el precepto solo refiere a “productos peligrosos”; (ii) indicar que, si un sistema de tecnología automatizada fue calificado como de alto riesgo de conformidad con las reglas previstas en la futura Ley General de IA, se presumirá de derecho que representa un bien o servicio peligroso, según sea el caso.

Reformas al Reglamento de Comercio Electrónico

Junto con la dictación de la nueva Ley General de IA y las reformas a la LPDC, resulta deseable realizar reformas al Reglamento de Comercio Electrónico, con el objetivo de regular en detalle la responsabilidad de los intermediarios (enfatizando en quienes utilizan herramientas automatizadas) y consagrar deberes de transparencia adicionales para estas entidades. Si bien estas materias tienen que ver con el consumo, y, por tanto, podría pensarse que pueden ser directamente incluidas a la LPDC, hay tres razones por las que se estima conveniente que sean reguladas en el Reglamento de Comercio Electrónico.

En primer lugar, debe recordarse que la LPDC, salvo por lo previsto en su artículo 43, regula únicamente relaciones directas entre consumidores y proveedores. Por tanto, probablemente no resulte pacífica la inclusión de normas que establezcan obligaciones

específicas para intermediarios en su articulado, por estimarse que quedan fuera del ámbito de aplicación de la ley y que constituirían una extensión excesivamente amplia de los derechos de los consumidores.

No es el objetivo de la presente Memoria argumentar sobre la conveniencia o inconveniencia de hacer extensible la totalidad de la LPDC ante terceros intermediarios –más allá de lo indicado respecto del artículo 43–. Sin embargo, es relevante advertir que, así como existen razones para entender que el consumidor debe gozar de protección amplia más allá de con quien interactúe directamente, también es posible sostener que, dado que el intermediario es un agente neutro que tiene por función conectar a las partes y reducir los costos de transacción y las asimetrías de información, no se justifica imponerle las mismas obligaciones que a la contraparte directa[788].

Ahora bien, a juicio de estos autores, los avances de la tecnología han suscitado legítimas dudas sobre la efectividad del rol neutro del intermediario, por lo que deben establecerse deberes de transparencia y responsabilidad adicionales respecto de estas entidades. Pero, para evitar caer en problemas de aplicación de la LPDC, se estima conveniente que esta regulación esté contenida en el Reglamento de Comercio Electrónico, por ser una normativa que justamente viene a tratar cuestiones suscitadas a propósito de la intermediación y que son propias del comercio a distancia. En efecto, el considerando 5 de este cuerpo normativo indica:

> "*5. Que, el dinamismo de dichas tecnologías ha implicado también una evolución constante de los modelos de negocios y de los roles de los actores que interactúan en el comercio electrónico, observándose especialmente la existencia de terceros dedicados a conectar proveedores con consumidores, mediante plataformas electrónicas denominadas "Marketplace", que constituyen un eslabón esencial dentro del proceso. De este modo, es usual que dichas plataformas electrónicas sean operadas por terceros, lo que no obsta que en muchos casos sean operadas por los mismos proveedores. Tal situación, en que interviene más de un actor por parte de la oferta y venta del producto, ha provocado una falta de claridad sobre cómo deben cumplirse las normas de la*

[788] RODRÍGUEZ, N., VÁZQUEZ, J. y MARTÍNEZ, M. *El comercio electrónico y la asimetría de la información: una aproximación de los costes de transacción*. Revista galega de economía, 12(1): p. 14, 2003.

misma ley para garantizar los derechos de los consumidores en el comercio electrónico"[789].

En segundo lugar, se estima deseable que la regulación esté prevista en el Reglamento porque la actividad de intermediación se ha visto totalmente transformada por la tecnología, y es de esperar que lo siga siendo en un futuro[790]. En tal sentido, este instrumento jurídico permite flexibilidad suficiente para adecuar las obligaciones a los avances tecnológicos. Debe recordarse que las obligaciones que se propone incorporar hacen sentido a la luz del desarrollo actual de la materia, pero es probable que en algunos años más el régimen deba recibir modificaciones –dependiendo de cómo evolucionen las tecnologías empleadas–.

En tercer lugar, se propone incluir todas estas disposiciones en el Reglamento de Comercio Electrónico, debido a que es un instrumento jurídico extremadamente perfectible. Pese a la importancia de la materia a regular y al tenor de sus Considerandos, el Reglamento actual jamás hace referencia al empleo de tecnologías automatizadas, a la transparencia algorítmica, al uso de patrones oscuros (*dark patterns*) ni a la responsabilidad civil de las plataformas.

En efecto, detalla en forma óptima los deberes de transparencia o información en materia de contratación a distancia, pero circunscribe estos deberes a las características relevantes del bien o servicio comercializado, a la formación del consentimiento, a las obligaciones contractuales asumidas, a la integración publicitaria, al derecho a retracto y, en general, a la debida publicidad de los términos y condiciones[791].

No se discute que dichas obligaciones sean relevantes y estén adecuadamente desarrolladas por el Reglamento. Empero, a la luz del auge de las tecnologías automatizadas, y siguiendo los lineamientos estudiados de la Unión Europea y Estados Unidos, es necesario que dicho régimen también se haga cargo de detallar la transparencia debida al uso de tecnologías automatizadas y precisar los términos en que el intermediario responderá civilmente. No resulta dable que un instrumento jurídico que tenga por cometido hacerse cargo

[789] MINISTERIO de Economía, Fomento y Turismo (Chile). Decreto 6 que Aprueba Reglamento de Comercio Electrónico. Santiago, Chile, 23 de septiembre de 2021. Considerando 5.
[790] *Ibíd*., Considerando 4.
[791] *Ibíd*., artículos 7 a 20.

de los problemas del comercio electrónico no se pronuncie sobre dichos fenómenos, máxime si se considera que la materia no está regulada en ninguna otra norma.

Pues bien, ya aclarada la necesidad de actualizar este Reglamento, se expondrán las propuestas de reformas específicas. Una primera sugerencia es que el artículo 6 del Reglamento, que refiere a la entrega de información en línea, indique expresamente que esta información debe propiciarse no solo respecto del bien o servicio comercializado, sino también sobre las eventuales herramientas automatizadas de las que el intermediario haga uso.

En ese mismo sentido, se propone que en el artículo 8, que regula la información que el intermediario debe propiciar sobre el rol de la plataforma, se agreguen cuatro incisos. El primero de ellos exigirá que la plataforma informe si es que emplea sistemas de recomendación automatizados para mostrar bienes o servicios. De ser así, la plataforma debe explicar al consumidor –siguiendo el criterio del artículo 27 DSA de la Unión Europea–[792] cuáles son los parámetros principales de tales sistemas, e indicar las opciones a su disposición para modificar o influir en dichos parámetros.

En cuanto al segundo inciso, se propone que indique que el deber de informar a los consumidores sobre los parámetros principales supone explicar por qué se sugiere determinada información al destinatario del servicio, ahondando en los criterios más significativos y en su importancia.

Por su parte, se propone que el tercer inciso indique que los dos incisos anteriores resultan aplicables también respecto de los procesos de clasificación, entendiendo por clasificación "l*a preeminencia relativa atribuida a los bienes o servicios ofrecidos mediante servicios de intermediación en línea o la relevancia atribuida a los resultados de búsqueda a través de motores de búsqueda en línea, tal y como los proveedores de servicios de intermediación en línea o los proveedores de motores de búsqueda en línea, respectivamente, los presentan, organizan o comunican, con independencia de los medios tecnológicos empleados para tal presentación, organización o comunicación*"[793].

[792] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022. Artículo 27

[793] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Bruselas, Bélgica, 2019. Artículo 2.

Por último, se sugiere que el cuarto inciso imponga una prohibición general de utilizar *dark patterns* en el diseño de las plataformas. Para este efecto, podría consagrarse una regla similar a la del artículo 25 del DSA de la Unión Europea, indicando que, sin perjuicio de lo previsto en los incisos anteriores, las plataformas "*no diseñarán, organizarán ni gestionarán sus interfaces en línea de manera que engañen o manipulen a los destinatarios del servicio o de manera que distorsionen u obstaculicen sustancialmente de otro modo la capacidad de los destinatarios de su servicio de tomar decisiones libres e informadas*"[794].

Por otro lado, para finalizar con las obligaciones especiales de transparencia, se propone agregar un artículo nuevo que refiera a la profesionalidad y lealtad en el uso de tecnologías automatizadas. Este precepto sería una combinación de lo previsto en los artículos 5 y 7 del Reglamento 2019/1150 UE[795] y en la sección 4.1 de la *Algorithmic Justice and Online Platform Transparency Act* de Estados Unidos[796], constando de dos incisos.

El primer inciso indicará que las plataformas deben informar las consideraciones económicas, comerciales y/o jurídicas que justifican la decisión tomada por medio de herramientas automatizadas, procurando explicar los eventuales tratos diferenciados. Asimismo, las plataformas deben transparentar si es que reciben pagos de empresas o usuarios que venden sus productos o servicios, precisando los efectos concretos que dicho pago surte en la clasificación presentada al consumidor.

El segundo inciso referirá a la transparencia respecto de la forma en que las tecnologías emplean los datos personales de los usuarios, obligando a la plataforma a informar: (i) las categorías de información personal que la plataforma crea o recopila en el proceso algorítmico; (ii) cómo se utiliza dicha información personal; y (iii) qué método emplea en proceso algorítmico para clasificar o recomendar contenidos en base a la información personal recopilada.

[794] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022. Artículo. 25.1.
[795] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Bruselas, Bélgica, 2019. Artículos 5 y 7.
[796] CONGRESO de los Estados Unidos (Estados Unidos). *S.2325 - Algorithmic Justice and Online Platform Transparency Act.* Washington D.C., Estados Unidos, de 13 de julio de 2023. Sección 4.1.

En cuanto a las reglas de responsabilidad civil de los intermediarios, atendido que el Reglamento de Comercio Electrónico actual nada indica sobre la materia, se deben dictar normas nuevas que expliciten en qué medida la plataforma responde por daños que puedan efectuarse mediante la moderación de contenidos o empleo de herramientas automatizadas.

Antes de explicar en qué términos responden, debe establecerse la obligación de que las plataformas efectúen reportes públicos sobre las actividades de moderación de contenidos (incluyendo aquellas efectuadas por IA). Esto es algo que tampoco está regulado en nuestra normativa, y constituye un presupuesto para que el consumidor entienda cómo le fueron causados los daños.

Una vez establecida dicha obligación en el Reglamento, deben crearse normas que expliquen si la plataforma puede liberarse de responsabilidad por los actos que terceros desarrollen en este espacio. Sobre este punto, surge la pregunta de si lo más idóneo es el enfoque de los artículos 4 a 7 de la DSA de la Unión Europea o el previsto en la afamada sección 230 en Estados Unidos. Como se señaló en su oportunidad, a juicio de estos autores resulta más óptimo el criterio estadounidense, mas no su texto en sí, sino los precedentes y propuestas que se han desarrollado al respecto.

En ese sentido, en lugar de proponer copiar tal cual alguna de las reglas, se recomienda crear una norma distinta que dé cuenta de los criterios doctrinarios. El principal enfoque a recepcionar es la interpretación estadounidense que entiende que el contenido creado por algoritmos de recomendación no puede ser considerado como proveniente de un tercero y, por ende, no es susceptible de exención de responsabilidad[797].

Pero también debe destacarse el planteamiento desarrollado por la doctrina de la Unión Europea, en orden a que la exención de responsabilidad opera únicamente si la plataforma fue diligente en el cumplimiento de sus otras obligaciones, dentro de las cuales se encuentran los deberes de lealtad, transparencia e información[798]. Así pues, se propone incorporar una regla del siguiente estilo:

---

[797] TREMBLE, Catherine. *Wild Westworld: Section 230 of the CDA and Social Networks' Use of Machine-Learning Algorithms.* Fordham L. Rev. 86: 2017, p. 868.

[798] DE MIGUEL ASENSIO, Pedro. *Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales*. La Ley Unión Europea. (109), p. 10.

"Ninguna plataforma que realice servicios de intermediación será considerada como publicadora o emisora de contenidos generados por proveedores o usuarios que utilizan el espacio. En consecuencia, la plataforma podrá liberarse de responsabilidad civil si acredita que el contenido dañoso es directamente atribuible a un tercero.

Con todo, no se considerará como contenido proveniente de un tercero aquellas informaciones, decisiones o actos que sean generados por sistemas de tecnología automatizada empleados directamente por el intermediario".

Asimismo, la exención de responsabilidad prevista en el inciso primero solo operará si la plataforma acredita no haber infringido negligentemente ninguna de las otras obligaciones en favor del consumidor que se prevén en este Reglamento y en otras normativas que sean aplicables.

El hecho de que no opere la exención de responsabilidad no supone automáticamente la responsabilidad civil de la plataforma, pero permitirá presumir legalmente su acción u omisión negligente. Además, si la plataforma hubiese utilizado tecnologías automatizadas, regirá la presunción de causalidad a la que alude la Ley General de la IA"[799].

Reformas a la LPVP y al Proyecto de Ley que la modifica

Sumado a la dictación de la Ley General de IA –con su Reglamento– y a las reformas anteriores, es menester complementar el régimen de protección al consumidor con reformas expresas a la legislación de datos personales, que atendida su especialidad deben ser tratadas directamente en esta normativa sectorial.

Si bien actualmente en Chile está vigente la LPVP, las reformas que se propongan se enfocarán especialmente en el Proyecto de Ley que se encuentra en tramitación para modificarla, puesto que se trata de un texto más moderno que se espera que sea prontamente aprobado. Sin perjuicio de que el Proyecto de Ley se asemeja un tanto más a la RGPD y la

[799] El contenido de esta recomendación normativa es totalmente propio. Se ha generado sobre la base de los planteamientos doctrinarios desarrollados en Estados Unidos y en la Unión Europea, así como teniendo a la vista las reflexiones o críticas que se apuntaron en apartados anteriores.

ADPPA, todavía hay muchos aspectos que ameritan reformas adicionales de cara a lograr una efectiva protección de los datos personales de los consumidores.

En primer lugar, se sugiere restringir las causales generales que habilitan el tratamiento de datos personales. El Proyecto de Ley prevé que "[e]*s lícito el tratamiento de los datos personales que le conciernen al titular cuando otorgue su consentimiento para ello o lo autorice la ley*"[800]. El problema es que la ley autoriza el tratamiento de todos los datos que sean de fuente de acceso público. Este concepto, por su amplitud, redunda en que la licitud del tratamiento de datos sea la regla general, prescindiendo de la exigencia del consentimiento del titular –en este caso, el consumidor–. Por ello, es menester acotar el significado de lo que se considera como fuente de acceso público.

En segundo lugar, se propone consagrar expresamente el principio de la minimización de datos personales de manera similar a la sección 101 de la ADDPA. Según esta norma, una empresa no puede recopilar, procesar o transferir datos personales a menos que la recopilación, procesamiento o transferencia se limite a lo que sea razonablemente necesario y proporcional para proporcionar o mantener un producto o servicio específico solicitado por el individuo al que pertenecen los datos o efectuar ciertos propósitos permitidos de manera expresa[801].

En tercer lugar, se sugiere que, en cuanto al tratamiento automatizado de datos personales, se contemple una regulación específica relativa a la elaboración de perfiles y a la publicidad personalizada. Actualmente no se prevé ninguna regulación al respecto en la LPVP ni en el Proyecto de Ley respectivo, pese a que en la presente investigación se destacó como una de las prácticas más recurrentes a propósito del uso de IA en el consumo.

Sobre este punto, se propone incorporar un nuevo precepto que, inspirado en el artículo 26 del DSA y en la sección 204 de la ADPPA, conste de tres incisos. El primero de ellos debiera prohibir a los prestadores de plataformas en línea presentar a los destinatarios del servicio anuncios basados en la elaboración de perfiles utilizando datos que revelen el origen étnico o

[800] MINISTERIO Secretaría General de la Presidencia (Chile). Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N° 11.144-07. Santiago, Chile, marzo del 2017. p.19.

[801] CONGRESO de los Estados Unidos (Estados Unidos). H.R.8152 - American Data Privacy and Protection Act. Washington D.C., Estados Unidos, 21 de junio de 2022. Sección 102.

racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física[802].

Por su parte, el segundo inciso debiese otorgar a los titulares de datos personales el derecho a optar por no recibir publicidad personalizada. Este derecho, conforme lo consagra la sección 204 de la ADPPA, se refiere a la posibilidad de que un individuo se oponga a la transferencia de sus datos cubiertos a terceros con fines publicitarios y a la capacidad de optar por no recibir publicidad personalizada[803].

Por último, en términos más generales, se sugiere que el tercer inciso consagre la obligación de los proveedores de informar a los consumidores –que, para estos efectos, son titulares de datos personales– la existencia de decisiones automatizadas, incluida la elaboración de perfiles. De existir elaboración de perfiles, los proveedores deberán proporcionar información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. Esto va en línea con aquello previsto en el artículo 13 del RGPD.

Asimismo, se recomienda que, junto con este precepto, se incorpore un literal en el artículo 2º en que se defina lo que se entiende por elaboración de perfiles, con el propósito de que no queden vacíos interpretativos al respecto, de manera similar en que lo hace el RGPD en su artículo 4º.

La definición que se tendrá de inspiración para estos efectos, será que la elaboración de perfiles consiste en "*toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento*

[802] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022. Artículo 26.
[803] CONGRESO de los Estados Unidos (Estados Unidos). H.R.8152 - American Data Privacy and Protection Act. Washington D.C., Estados Unidos, 21 de junio de 2022. Sección 204.

profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física"[804].

En cuarto lugar, se propone ampliar el alcance del derecho a la portabilidad de los datos personales contemplado en el artículo 9 del Proyecto de Ley, de modo que no se entienda simplemente como un derecho a *"copiar y pegar" la información suministrada por el usuario"*[805], sino que abarque lo que se conoce como "portabilidad en tiempo real", la cual permite que dos productos o servicios puedan interconectarse y trabajar juntos a través de medios técnicos[806].

En quinto lugar, se sugiere modificar el inciso 2° del artículo 15 ter que introduce del Proyecto de Ley, relativo al tratamiento automatizado de grandes volúmenes de datos. Este precepto indica que: "*[e]l titular de datos tiene derecho a solicitar al responsable que ninguna decisión que le afecte de manera significativa se adopte* ***exclusivamente*** *basada en el tratamiento automatizado de sus datos, salvo que sea necesario para la celebración o ejecución de un contrato entre el titular y el responsable, exista consentimiento previo y explícito del titular o lo disponga la ley*"[807] (énfasis agregado).

En concreto, debiera modificarse la palabra "exclusivamente" por "mayoritariamente" o algún término similar. En ese sentido, el artículo incurre en la misma falla que el artículo 22 del RGPD, ya que su aplicación está supeditada a que la decisión que afecte a un individuo se base "exclusivamente" en un tratamiento automatizado de sus datos personales, de forma que si el tratamiento existe una sola intervención humana, ya no resulta aplicable la disposición. Lo ideal sería no restringirlo únicamente a las decisiones automatizadas.

En sexto lugar, se sugiere incorporar una norma similar al artículo 30 del RGPD, conforme al cual cada responsable de tratamiento de datos personales y su representante

---

[804] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Bruselas, Bélgica, 2016. Artículo 4.

[805] TAMAYO VELASCO, Jimena, et al. *Big data, competencia y protección de datos: el rol del Reglamento General de Protección de Datos en los modelos de negocio basados en la publicidad personalizada.* Revista de estudios europeos (78): 2021, p.198.

[806] *Ibíd.*, p.197.

[807] MINISTERIO Secretaría General de la Presidencia (Chile). Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N° 11.144-07. Santiago, Chile, marzo del 2017. p. 24.

deban mantener un registro, por escrito, de las actividades de tratamiento realizadas bajo su responsabilidad y, también, de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable[808]. Se trata de algo relevante no abordado por el Proyecto de Ley.

En séptimo lugar, se recomienda incluir un precepto que establezca la obligación preventiva de realizar una Evaluación de Impacto Algorítmica (En adelante "**EIA**") previa para todas las empresas que traten datos personales sensibles y/o de alto riesgo mediante sistemas de IA, a cargo de la Agencia de Protección de Datos Personales, con el propósito de evaluar los posibles impactos sociales de un sistema previo a que el sistema esté en uso[809].

Al respecto, cabe señalar que la EIA es un modelo prometedor de gobernanza algorítmica, debido a que incluye una descripción de los daños potenciales y reales de un sistema para identificar quién es responsable de su reparación[810]. Según ha señalado el jurista mexicano Jersaín Llamas,

> "*En esencia, la EIA ofrece un medio para describir, medir y asignar responsabilidad por los impactos sin la necesidad de codificar nociones científicas explícitas en la ley, por consiguiente, los regímenes de evaluación de impacto abordan en especial tres cuestiones, a saber: qué hace un sistema; quién puede hacer algo sobre lo que hace ese sistema; y quién debería tomar decisiones sobre lo que se le permite hacer al sistema, fomentando una transparencia y trazabilidad tecnológica y cumplimiento normativo para detectar y gestionar riesgos de la IA*"[811].

En octavo lugar, si bien puede resultar algo "redundante" teniendo en consideración que el ordenamiento jurídico es integral, los autores de la presente Memoria estiman necesario

---

[808] PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Bruselas, Bélgica, 2016. Artículo 30.

[809] LOVELACE, Ada; DATAKIND, U. K. *Examining the black box: Tools for assessing algorithmic systems*. [en línea] Technical report, AdaLovelace Institute, 2020 <https://ico. org. uk/media/about-theico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf> [consulta: 02 diciembre 2023]. p. 4.

[810] LLAMAS, Jersain, et al. Enfoques regulatorios para la Inteligencia Artificial (IA). Revista chilena de derecho, 2022, vol. 49, no 3, p. 31-62. p. 54.

[811] LLAMAS, Jersain, et al. Enfoques regulatorios para la Inteligencia Artificial (IA). Revista chilena de derecho, 2022, vol. 49, no 3, p. 31-62. p. 54.

incorporar una prohibición expresa de toda discriminación arbitraria en cualquiera de las fases de tratamiento de datos personales, esto es, en la recolección, procesamiento, almacenamiento, comunicación, transmisión y, en general, cualquier forma de utilización de los datos personales. En efecto, aquello facilitaría sustancialmente a los consumidores titulares de datos personales perseguir las responsabilidades que correspondan en caso de haber sido víctimas de discriminación en empleo de sus datos.

Por último, se sugiere incorporar un precepto que contemple expresamente la obligación para los proveedores de proteger los datos personales de sus consumidores desde el diseño y por defecto, inspirada en el artículo 25 del RGPD[812] y, también, en la sección 103 de la ADPPA, según la cual las empresas deben considerar la privacidad desde el inicio del proceso de diseño y desarrollo, en lugar de tratar de agregar medidas de privacidad después de que se haya creado el producto o servicio[813].

[812] *Ibíd*. Artículo 25.

[813] CONGRESO de los Estados Unidos (Estados Unidos). H.R.8152 - American Data Privacy and Protection Act. Washington D.C., Estados Unidos, 21 de junio de 2022. Sección 102. Sección 103.

CONCLUSIONES

Para abordar las conclusiones de la presente investigación, se hará un resumen e interpretación de los resultados obtenidos y luego se efectuarán ciertas reflexiones en torno a los principales hallazgos. Se estima conveniente seguir tal estructura debido a la gran cantidad de secciones y páginas que comprendió la presente Memoria.

La primera pregunta que pretendía contestar esta investigación es cómo afecta el empleo de IA por parte de los proveedores a los derechos de los consumidores que, a la luz de las particularidades de esta tecnología, resultan más relevantes. Luego de estudiar la evolución de las relaciones de consumo y las principales características de la IA, se observó que los derechos que pueden verse en mayor medida afectados son la autonomía, la privacidad y la integridad de los consumidores.

A partir de un examen específico de la interacción entre la IA y estos derechos, se demostró que las oportunidades que brinda la IA a los consumidores son significativas. En efecto, considerando la complejidad que caracteriza a los mercados actuales, la asistencia virtual, la reducción de los costos de transacción, la orientación y la prevención de daños resultan especialmente valiosas para los consumidores.

No obstante, el uso de IA también supone riesgos importantes hacia sus derechos, que se vinculan principalmente a las discriminaciones algorítmicas arbitrarias, la intensificación de los *dark patterns*, el tratamiento inadecuado de datos personales y la generación de situaciones de responsabilidad civil en que resulta difícil dilucidar quién debe responder.

Constatado lo anterior, se examinó que existen tres formas distintas de interpretar el balance entre beneficios y riesgos. Una de ellas era entender que los riesgos son tan superiores a los beneficios, que simplemente debe prohibirse el uso de IA en las relaciones de consumo. Una segunda opción era sostener que las grandes oportunidades que brinda la IA justifican permitir su uso sin mayor regulación. Una tercera opción, que es ecléctica y fue la que adoptaron estos autores, es que, por una parte, los beneficios de la IA en las relaciones de consumo sugieren permitir su empleo por parte de los proveedores, pero, por otra, los riesgos que ello ocasiona son tan significativos que no pueden ser ignorados.

Esta última postura hace sentido si se tienen en cuenta los enfoques regulatorios adoptados por la Unión Europea y Estados Unidos, que han permitido el uso de IA en los mercados haciéndose cargo de ciertos riesgos relevantes para los usuarios. Empero, el problema que se presenta en nuestro país es que la normativa chilena actual no permite responder en forma satisfactoria a todos los riesgos serios a los que se exponen los derechos de los consumidores, pues no existe una regulación específica que se ocupe de elevar su grado de protección cuando interactúan con esta tecnología.

En un comienzo, dado que los principales cuerpos normativos de protección a los consumidores (LPDC y Reglamento de Comercio Electrónico) no hacen referencia alguna a la IA o a los sistemas automatizados, y que el único documento que habla sobre la materia es una Circular Interpretativa que, además de no resultar vinculante, deja varios asuntos pendientes, se llegó a sospechar que el grado de protección en esta materia era prácticamente nulo. Sin embargo, un estudio acabado de las diversas herramientas que prevé nuestra legislación permitió constatar que no es así.

En efecto, a partir de los derechos de información, del principio de transparencia, del deber de profesionalidad y del control de cláusulas abusivas que contempla la LPDC, es posible construir, al menos, una mediana protección hacia los derechos de los consumidores. Es cierto que ninguna de esas herramientas fue generada para responder específicamente al problema de la IA, pero son recursos legales que, sin ser interpretados en forma extremadamente forzada, logran sentar algunas bases para proteger a los consumidores ante el uso de la tecnología.

Asimismo, esta protección se complementa con lo previsto en la LPVP, que, si bien está lejos de ser como el RGPD o el ADPPA, reconoce que el tratamiento de datos personales puede ser automatizado y contempla ciertas máximas que son extensibles al uso de IA, como la observancia de los principios de finalidad, de seguridad y de calidad en el uso de los datos.

Por lo demás, se espera que prontamente tengamos una regulación de datos personales más similar a las referencias internacionales citadas, en el evento que se apruebe el Proyecto de Ley que crea la Agencia de Datos Personales. Este Proyecto constituye un gran avance en orden a regular la elaboración de perfiles, la portabilidad y el derecho a no ser objeto de decisiones basadas en el tratamiento automatizado de datos personales, entre otras cosas.

Sin perjuicio de lo anterior, todavía hay muchos riesgos que no alcanzan a ser cubiertos por la normativa chilena, incluso si se aprobasen los proyectos de ley que actualmente se encuentran en discusión. Como principales problemas, podemos señalar que, en ausencia de orientación, resulta complejo para los proveedores saber qué transparentar respecto de sus algoritmos, ya que no existe ningún deber expreso que indique qué es lo que hay que informar exactamente.

Si bien en materia de consumo rige un principio de transparencia, es difícil dilucidar, no habiendo norma que lo ejemplifique, cómo se proyecta exactamente tal principio en relación con el uso de la IA. En efecto, una transparencia algorítmica nula no ayuda; mas una transparencia absoluta podría resultar contraproducente, tanto para los proveedores –por gastos de tiempo y riesgo de divulgar datos confidenciales– como para los consumidores –que quizás no necesitan toda esa información, o tenerla en exceso los confunda–[814]. De ahí que sea necesario precisar deberes de transparencia específicos para delimitar el alcance de los deberes de información.

Asimismo, tampoco queda claro cuáles son las obligaciones positivas concretas que se derivan del deber de profesionalidad de los proveedores. La aplicación del deber de profesionalidad sugiere que el proveedor que emplea tecnologías de IA debe ser cuidadoso, responsable y comportarse de buena fe. Esto último es sencillo de entender cuando hablamos de abstenciones o conductas negativas (por ejemplo, no influir maliciosamente en la autonomía), pero no pasa lo mismo cuando pensamos en conductas positivas, por cuanto, al igual que con la transparencia, surge la pregunta de cuál es el límite en que las obligaciones ya no son razonables o propias de un profesional, sino cuestiones contraproducentes o incluso imposibles de cumplir.

A ello debemos agregar la ausencia de regulación de la responsabilidad de las plataformas intermediarias en el control de contenidos, así como la nula adecuación a las reglas de responsabilidad extracontractual para los casos en que la IA comete daños. En principio podría parecer que no hace falta consagrar regímenes especiales. Sin embargo, el problema que se identificó es que, cuando esta tecnología comete daños, resulta complejo

[814] COMISIÓN EUROPEA. Comunicación “Directrices sobre la transparencia de la clasificación con arreglo al Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo”. p. 5. Considerando 25.

para el consumidor identificar al agente responsable de los daños, probar el nexo de causalidad y eventualmente verse obligado –en el caso chileno– a tener que probar derecho extranjero. Por ello, el derecho a la debida indemnización termina careciendo de efectividad.

Por último, sigue habiendo problemas en relación a la protección de datos personales. Como se indicó, el Proyecto de Ley chileno soluciona en buena medida los desafíos pendientes. No obstante, todavía subsisten algunos asuntos no abordados que sería deseable que se complementen, como por ejemplo, la regulación de la elaboración de perfiles y la publicidad personalizada, así como la aplicación de principios de minimización en el tratamiento de datos.

Tal como se adelantó en la Introducción, atendida la existencia de todas estas deficiencias, la segunda y principal pregunta que perseguía contestar la presente investigación es si, recurriendo a estándares desarrollados en la Unión Europea y en Estados Unidos –que son ordenamientos jurídicos algo más avanzados en la materia–, es posible hacer frente exitosamente a los desafíos pendientes.

En ese sentido, se examinaron diversas normas consagradas en la Unión Europea y Estados Unidos que referían a cinco desafíos identificados como pendientes: (i) regulación especial de responsabilidad; (ii) deberes de transparencia; (iii) auditorías algorítmicas –que en realidad encajan dentro de la transparencia, pero se examinó como tópico aparte por su relevancia–; (iv) protección de datos personales; y (v) otros controles en el uso de la IA –para determinar qué otras diligencias son propias de un proveedor profesional en dichos ordenamientos–.

Una vez estudiada toda la normativa extranjera, se realizó una comparación y se efectuó un análisis prospectivo en orden a determinar la combinación de normas que mejor funcionaría en Chile. También se examinó si es que tal combinación es suficiente por sí sola o, en cambio, podría complementarse en ciertos aspectos que, si bien no fueron tratados en la normativa internacional, son útiles para abordar exitosamente todos los desafíos.

Como resultado de ese ejercicio, se concluyó que, si se tiene a la vista ambas normativas y se mezclan en algunos aspectos, es posible consolidar un régimen que cubra adecuadamente casi todos los desafíos o riesgos que enfrentan actualmente los

consumidores. Con todo, hay ciertos ámbitos –como la regulación de las auditorías algorítmicas o de otros controles de la IA– que han de ser complementados, puesto que la combinación de normativas no lograba reducir totalmente los riesgos significativos hacia los consumidores. Para ello, se recurrió a propuestas propias o a ideas planteadas por la doctrina.

Adicionalmente, había algunos otros ámbitos en los que lo destacable del régimen extranjero no era la norma propiamente tal –o no solo ella–, sino la interpretación que la doctrina o jurisprudencia ha efectuado sobre la misma. Este fue el caso, por ejemplo, de la regulación de responsabilidad de los intermediarios, en el que, en lugar de replicar el texto de la afamada sección 230 de Estados Unidos, se sugirió crear en Chile una norma distinta que dé cuenta, en forma autosuficiente, de los criterios con que la doctrina ha interpretado la regla recientemente.

Finalmente, una vez dilucidado el contenido general del régimen que debiese adoptar Chile, se formularon propuestas concretas, precisando tanto los instrumentos jurídicos que debieran introducir el régimen como su contenido específico, incluyendo la reforma a algunos preceptos de la LPDC, del Reglamento de Comercio Electrónico y del Proyecto de Ley sobre Datos Personales.

Se estimó que, junto con las reformas, debe dictarse una Ley General de IA y su respectivo Reglamento. Para evitar regular la tecnología en forma rígida, se propuso que esta ley fuese del tipo *sunset law* y permitiese la realización de *sandbox* regulatorios. Esto trae como consecuencia que, incluso si el texto de la ley fuese exhaustivo, se dé dinamismo a la regulación por la vía de posibilitar su revisión en plazos fijos breves. Sin perjuicio de ello, de igual manera se sugirió que las manifestaciones concretas de ciertos deberes de transparencia u otros controles sean precisados detalladamente en el Reglamento de la Ley General.

Ya expuestos e interpretados los resultados de cada uno de los capítulos, los autores de la presente Memoria efectuarán ciertas reflexiones que se suscitan a propósito de los hallazgos.

Un primer aspecto que se quiere destacar es que, a menudo, se piensa que el derecho del consumidor comprende un catálogo de derechos taxativo, de suerte que el consumidor

queda amparado únicamente ante aquello que esté expresamente regulado en la ley. El tercer Capítulo de esta Investigación es una prueba clara de lo equivocado de tal planteamiento.

La preocupación de evaluar la idoneidad de la protección del consumidor ante el surgimiento de nuevas tecnologías supone no solo una revisión exhaustiva del conjunto de derechos establecidos a su favor, sino también de las diversas herramientas interpretativas o axiológicas genéricas que prevé la ley.

Puede ser, como ocurrió en el Tercer Capítulo, que dichas herramientas permitan adaptarse a supuestos no previstos por el legislador, y brindar protección al consumidor aun cuando la tecnología no aparezca mencionada expresamente en ninguna parte de la ley. En este caso, la protección otorgada era insuficiente y debieron formularse propuestas para complementarla. Sin embargo, lo que se quiere transmitir es que hay un contenido axiológico que alimenta la normativa de protección al consumidor y que, si está bien definido, puede amparar al consumidor en una cantidad amplia de supuestos, lo que posee especial relevancia de cara a la evolución tecnológica.

Si bien se espera que el régimen de protección al consumidor en esta materia sea actualizado, se anima a los operadores jurídicos a que, mientras ello no ocurra, se recurra a conceptos axiológicos como el deber de profesionalidad, principio de transparencia y control de cláusulas abusivas que se opongan a la buena fe, para efectos de evitar que los consumidores se encuentren totalmente desprotegidos al interactuar con la IA.

En segundo lugar, cabe tener presente que la normativa sugerida para Chile tiene como inspiración las normas estudiadas de Estados Unidos y la Unión Europea, pero también recurre a la doctrina que se ha escrito sobre la materia. En ese sentido, no se propone simplemente una combinación de textos legales, sino la consolidación de un régimen que tenga en cuenta criterios interpretativos valiosos que han surgido a propósito del uso de IA y la protección de los consumidores. Ello demuestra que, muchas veces, quienes logran identificar los problemas que experimentan las tecnologías son los propios agentes del mercado.

Por consiguiente, aun cuando, por la entidad de los riesgos, sea tentador delegar la respuesta completa al legislador y a la administración estatal, para conseguir una normativa

óptima es necesario mezclar enfoques. Esto supone que al legislar se dé especial relevancia a los resultados arrojados por los *sandbox* regulatorios y se incentive la autorregulación.

No se trata de no normar el asunto y dejar que cada empresa actúe del modo que estime conveniente, sino de normarlo, pero, al mismo tiempo, permitir que los agentes del mercado puedan formular sus propuestas e ir dirigiendo con algún grado de discrecionalidad leve su actuar. De este modo, la interpretación legal será enriquecida y, una vez que termine el período fijo de vigencia de la *sunset law*, será más sencillo saber cómo adecuarla.

En ese sentido, es menester entender que la técnica del *sunset law* de por sí es un enfoque regulatorio flexible, pero se vuelve aún más flexible cuando es complementada con *sandbox* regulatorios, toda vez que, mientras se revisa el desempeño de ciertas reglas, se van realizado pruebas que evalúan qué tan viables serían normas estatales nuevas o incluso ciertos criterios propuestos por la doctrina o las propias empresas. Eso es lo valioso de adoptar una modesta propuesta como la contenida en la presente Memoria, que, junto con proponer reformas y contenido, abre cauce a que su complementación futura sea sencilla.

Por último, y en directa relación con lo anterior, el principal aporte de esta investigación probablemente no sea el contenido del régimen recomendado. Si bien lo deseable es que resulte de utilidad, se tenga a la vista y se adopte prontamente en Chile, es de esperar que los artículos propuestos no tengan vigencia y utilidad perpetua, atendido lo rápido que evolucionan las tecnologías automatizadas. Hace veinte años una investigación como la actual no habría tenido mucho sentido. Hoy lo tiene. Quizás veinte años después los problemas o interrogantes sean otras. Pero hay algo de esta investigación que esperamos que quede.

Desde luego, es reconfortante pensar en su aporte para solucionar problemas urgentes para los consumidores en el corto plazo, así como para brindar criterios interpretativos que ayudarán a la defensa de sus derechos incluso antes de que se actualice el régimen. Sin embargo, lo que se espera que permanezca por más tiempo es la idea de que, así como la regulación de las tecnologías debe ser flexible y exige adecuaciones, la normativa de protección a los consumidores también.

En efecto, la forma en que se relacionan los humanos varía según el avance de las tecnologías. Ello se puede apreciar, más antiguamente, con el surgimiento de la comunicación

a distancia, y, más recientemente, con el auge de la IA. Las tecnologías cambian y evolucionan, pero la idea que siempre se mantiene es que toda tecnología posee el potencial de reconfigurar la forma en que interactúan los humanos.

En ese sentido, siendo las interacciones entre consumidores y proveedores interacciones humanas, son propensas a configurarse de un modo distinto cada vez que surgen nuevas tecnologías. Esto exige revisar si el grado de protección que se otorga a los consumidores sigue siendo efectivo o no. En la presente instancia, se hizo dicho análisis a propósito de la IA, y se concluyó que la protección nacional no es suficiente, pero podría serlo si se observan propuestas doctrinarias y legales internacionales.

En un futuro, puede que las preguntas sean otras. Es cierto. Y puede que las respuestas también. En cualquier caso, lo importante es saber que todo auge de nuevas tecnologías debiese, cuando menos, despertar la preocupación de si ello afecta en algún modo la protección de los consumidores.

En suma, la presente Memoria ha tenido por principal objetivo evaluar si los desafíos que presenta la normativa chilena en cuanto al resguardo total de los derechos de los consumidores frente al uso de IA, pueden ser cubiertos recurriendo a estándares internacionales. La respuesta es afirmativa, pero siempre y cuando las normas extranjeras estudiadas, de ser replicadas en nuestro país, sean complementadas en ciertos aspectos con las interpretaciones o propuestas doctrinarias que se abordaron. Asimismo, se reflexionó en torno a tres puntos que van más allá de la conclusión principal.

El primer aspecto es que el carácter axiológico de la normativa de protección al consumidor permite protegerlo parcialmente incluso de supuestos de hecho no regulados, lo que posee especial relevancia en el contexto de la tecnología. El segundo aspecto refiere a la necesidad de incentivar la autorregulación como recurso complementario a la normativa principal y, en general, de atender los resultados de los *sandbox* regulatorios y la opinión de la comunidad. El mensaje final es que, más allá de que el régimen recomendado no sea perpetuo, debiera evaluarse la necesidad de ajustar la protección de los consumidores cada vez que una tecnología cambie las formas de interacción humana.

BIBLIOGRAFÍA

ABRAHAM, M. y EDELMAN, D. *Customer Experience in the Age of AI.* [en línea] Harvard Business Review. March-April 2022. <https://hbr.org/2022/03/customer-experience-in-the-age-of-ai> [consulta: 30 agosto 2023].

AMAYUELAS, E.A., 2020. *La responsabilidad de los intermediarios en Internet ¿puertos seguros a prueba de futuro?.* Cuadernos de Derecho Transnacional, 12(1): p. 808-837.

ANDRÉ, Quentin, et al. *Consumer choice and autonomy in the age of artificial intelligence and big data. Customer needs and solutions,* 2018, vol. 5, p. 28-37.

ANIC, Ivan-Damir, ŠKARE, Vatroslav y KURSAN, Ivana. 2019. *The determinants and effects of online privacy concerns in the context of e-commerce*. Electronic Commerce Research and Applications, 36 (100868).

ANGUITA, Pedro. *La protección de datos personales y el derecho a la vida privada*. Santiago, Editorial Jurídica, 2007.

ARÁNGUIZ, Matías. *Auditoría algorítmica para sistemas de toma o soporte de decisiones*. Washington DC, Banco Interamericano de Desarrollo, 2020.

ARAYA Paz, Carlos. *Desafíos legales de la inteligencia artificial en Chile*. Revista chilena de derecho y tecnología. 9 (2): 257-290, 2020.

ARAYA Paz, Carlos. 2021. *Transparencia algorítmica ¿un problema normativo o tecnológico?* [en línea] CUHSO (Temuco). 31(2): 306-334. <https://www.scielo.cl/scielo.php?pid=S2452-610X2021005000002&script=sci_abstract&tlng=en> [consulta: 19 octubre 2023].

ARELLANO LÓPEZ, Christian Alberto. 2020. *El derecho de protección de datos personal*es. [en línea] Biolex, 12(23): 163-174. <https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-55452020000200009> [consulta: 15 septiembre 2023].

ARGELICH-COMELLES, Cristina. 2023. *Deberes de transparencia del Reglamento 2019/1150 (P2B Regulation) para prevenir la discriminación algorítmica del consumidor en los sistemas de prelación de ofertas. (Ranking Transparency Guidelines in Platform-To-Business Regulation to Prevent Algorithmic Discrimination of Consumers).* [en línea] Cuadernos de Derecho Transnacional, 15(1): 129-135. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4434518> [consulta: 26 diciembre 2023].

AZUAJE, Michelle y FINOL, Daniel. *Transparencia algorítmica y la propiedad intelectual e industrial: tensiones y soluciones*. La Propiedad Inmaterial (30): pp. 111-146, 2020.

BARAONA, Jorge. *La regulación contenida en la Ley 19.496 sobre protección de los derechos de los consumidores y las reglas del Código Civil y Comercial sobre contratos: Un marco comparativo*. Revista chilena de derecho. 41(2): 2014, pp. 381-408.

BARRIENTOS Camus, Francisca. *Lecciones de derecho del consumidor.* Santiago, Thomson Reuters, 2019.

BARROS, Enrique. *Tratado de responsabilidad extracontractual*. Santiago, Editorial Jurídica, 2010.

BATHAEE, Yavar. *The Artificial Intelligence Black Box and the Failure of Intent and Causation*. Harvard Journal of Law & Technology (Harvard JOLT). 31 (2): 2018, pp. 890-938.

BELL, Andrew; STOYANOVICH, Julia; NOV, Oded. *Algorithmic Transparency Playbook.* [en línea] Center for Responsible AI. 2022 <https://dataresponsibly.github.io/algorithmic-transparency-playbook/resources/transparency_playbook_camera_ready.pdf> [consulta: 12 noviembre 2023].

BELLOSO, Nuria. *La problemática de los sesgos algorítmicos (con especial referencia a los de género). ¿Hacia un derecho a la protección contra los sesgos?*. En: LLANO, F(Coord.), GARRIDO, J y VALDIVIA, R (Eds.). *Inteligencia Artificial y Filosofía del Derecho*. Murcia, 2022, Ediciones Laborum, pp. 45-69.

BERGQVIST, Christian, Discrimination and self-favoring in the digital economy. Universidad de Copenhagen, 4 de febrero de 2020.

BERTELSEN REPETTO, Raúl. Datos personales: propiedad privada, libre iniciativa particular y respeto a la vida privada. En: "Tratamiento de datos personales y protección de la vida privada", BERTELSEN et al., 3ª edición, Cuadernos de extensión Jurídica, Ediciones Universidad de Los Andes, 2001.

BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. *Historia de la Ley N° 19.496*. [en línea] <https://www.bcn.cl/historiadelaley/nc/historia-de-la-ley/6746/> [consulta: 12 septiembre 2023].

BIBLIOTECA DEL CONGRESO NACIONAL DE CHILE. *Historia de la Ley N° 19.628. Sobre protección de la vida privada.* [en línea] <https://obtienearchivo.bcn.cl/obtienearchivo?id=recursoslegales/10221.3/71204/1/documento_3969_1693927810119.pdf> [consulta: 25 de octubre 2023].

BORJA, M. y PÉREZ, M. *Big data: un análisis documental de su uso y aplicación en el contexto de la era digital*. Rev. Prop. Inmaterial 28: p. 273, 2019.

BRANTT, M.G.; y, MEJÍAS, C. *El proveedor intermediario de servicios y su responsabilidad. Un estudio del artículo 43 de la Ley 19.496*. [en línea] Revista de Derecho, Vol. 34, n° 2, pp.29-50, Diciembre 2021, <https://www.scielo.cl/scielo.php?pid=S0718-09502021000200029&script=sci_arttext&tlng=pt> [consulta: 14 agosto 2023].

CÁMARA DE DIPUTADOS (CHILE). *Evaluación de la Ley N° 19.628. Protección de la Vida Privada*, agosto 2016.

CÁMARA DE DIPUTADOS (CHILE). *Oficio Nº 18.347 mediante el cual la Cámara de Diputados dio su aprobación al Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales*, de 08 de mayo de 2023.

CASADO, Eduardo. *El enfoque europeo de Inteligencia Artificial*. [en línea] Revista de Derecho Administrativo, 2021, n° 20, p. 268-289 <https://dialnet.unirioja.es/servlet/articulo?codigo=8510535> [consulta: 09 octubre 2023].

CASTELLÓ, José. Nuevo régimen de responsabilidad de los servicios digitales que actúan como intermediarios a la luz de la propuesta de Reglamento relativo a un mercado único de servicios digitales. 2021.

CERDA, Alberto. *Intimidad de los trabajadores y tratamiento de datos personales por los empleadores*. Revista Chilena de Derecho Informático, (2):35-59, 2003.

CHAMATROPULOS, Demetrio. *Inteligencia artificial, prevención de daños y acceso al consumo sustentable*. XXVI Jornadas Nacionales de Derecho Civil (La Plata, septiembre 2017). 26: 2017, pp. 1-8.

CHROMIK, Michael, et al. *Dark Patterns of Explainability, Transparency, and User Control for Intelligent Systems*. [en línea] IUI workshops, 2019 <https://www.medien.ifi.lmu.de/pubdb/publications/pub/chromik2019iuiworkshop/chromik2019iuiworkshop.pdf> [consulta: 28 noviembre 2023].

CITRON, Danielle Keats; WITTES, Benjamin. The internet will not break: Denying bad samaritans sec. 230 immunity. Fordham L. Rev. 86, pp. 406-408, 2017.

CLAUDETTE: an automated detector of potentially unfair clauses in online terms of service por Marco Lippi “et al”. Artificial Intelligence and Law, 27: pp. 128-130, feb. 2019.

COMISIÓN EUROPEA, 2020. *LIBRO BLANCO sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza.* [en línea], <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020DC0065> [consulta: 07 julio 2023].

COMISIÓN EUROPEA. Comunicación *"Directrices sobre la interpretación y la aplicación de la Directiva 2011/83/UE del Parlamento Europeo y del Consejo sobre los derechos de los consumidores"*.

COMISIÓN EUROPEA. Comunicación *"Directrices sobre la transparencia de la clasificación con arreglo al Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo".*

CONSEJO PARA LA TRANSPARENCIA. *Transparencia algorítmica. Buenas prácticas y estándares de transparencia en el proceso de toma de decisiones automatizadas* [en línea] Santiago, Chile, <https://www.consejotransparencia.cl/wp-content/uploads/estudios/2020/10/Transparencia-Algoritmica.pdf> [consulta: 17 de agosto de 2023].

CONTRERAS, Pablo. *El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena*. Estudios Constitucionales. 18(2): 2020, pp. 87-120.

CORRAL, Hernán. *La relación de causalidad en la responsabilidad por productos defectuosos*. Revista Chilena de Derecho Privado, (2):71-94, 2019.

CORTINA, Adela. *Por una ética del consumo*. Madrid, Taurus, 2002.

CRAIG, T. y LUDLOFF, M. E. *Privacy and Big Data: The Players, Regulators, and Stakeholders.* Newton, Massachusetts, O'Really Media, 2011.

DANESI, Cecilia. *El imperio de los algoritmos: IA inclusiva, ética y al servicio de la humanidad*. Buenos Aires, Galerna, 2022.

DARTMOUTH Artificial Intelligence Conference (1º, Hanover, New Hampshire, Estados Unidos, 1956). Inteligencia Artificial.

EGGERS, William D.; TURLEY, Mike; KISHNANI, PJDCFGI. The future of regulation: Principles for regulating emerging technologies. Deloitte Insights, 2018, vol. 19.

DE LA MAZA, Íñigo. *Contratos por adhesión y cláusulas abusivas: ¿Por qué el Estado y no solamente el mercado?* Revista chilena de derecho privado. (1): 2003, pp. 109-148.

DE LA MAZA, Íñigo. *El control de las cláusulas abusivas y la letra g*. Revista chilena de derecho privado. (3): 2004, pp. 35-68.

DE LA MAZA, Íñigo. *El suministro de información como técnica de protección de los consumidores: los deberes precontractuales de información*. Revista de derecho (Coquimbo). 17(2): 2010, pp. 21-52.

DE LA MAZA, Íñigo. y MOMBERG, Rodrigo., 2017. *Términos y condiciones: Acerca del supuesto carácter contractual de las autorizaciones para el tratamiento de datos personales en sitios web*. Revista chilena de derecho y tecnología 6(2): pp. 25-55, 2017.

DE LA MAZA, Íñigo y MOMBERG, Rodrigo. *La transparencia como mecanismo de tutela de la privacidad de los consumidores y usuarios en contratos electrónicos*. Revista chilena de derecho y tecnología 7(2): pp. 81-111, 2018.

DE MIGUEL ASENSIO, Pedro. *Obligaciones de diligencia y responsabilidad de los intermediarios: El Reglamento (UE) de Servicios Digitales*. La Ley Unión Europea. (109), pp. 1-47.

DE ZÁRATE, Luis. *Explicabilidad (de la Inteligencia artificial)*. Eunomía. Revista en Cultura de la Legalidad. (22):328-334, 2022.

DI PORTO, Fabiana., 2023. *Algorithmic disclosure rules*. Artificial Intelligence and Law, 31(1):13-51, Nov-2023.

DÍEZ-PICAZO, Luis. *Fundamentos del Derecho Civil Patrimonial.* 6ª Ed, Madrid, Editorial Civitas, 2007.

DOMÍNGUEZ, Ana Garriga. *Las exigencias de transparencia para los sistemas algorítmicos de recomendación, selección de contenidos y publicidad en línea en el nuevo*

Reglamento Europeo de Servicios Digitales. Revista española de la transparencia (17):137-164, Jul-2023.

ECHEVERRI, Verónica. *El control a las cláusulas abusivas en los contratos de adhesión con consumidores*. Opinión jurídica, 10(20): 2011, pp. 125-144.

EGUÍLUZ, Andoni. *Desafíos y retos que plantean las decisiones automatizadas y los perfilados para los derechos fundamentales.* [en línea] Estudios de Deusto: Revista de Derecho Público, 2020, Vol. 68, n° 2, p. 325-367 <https://dialnet.unirioja.es/servlet/articulo?codigo=7692059> [consulta: 25 noviembre 2023].

EUDENMÜLLER, *Horst. Whose fault? Firms products and liability in the age of artificial intelligence* [videograbación], Faculty of Law, Oxford University, disponible en <https://bit.ly/2BpwcsZ>.

EUROPEAN COMMISSION, 2019. *Ethics guidelines for trustworthy AI* [en línea], <https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai,> [consulta: 04 julio 2023].

EUROPEAN DATA PROTECTION BOARD. Directrices 8/2020 sobre la focalización de los usuarios de medios sociales, Versión 2.0, adoptadas el 13 de abril de 2021.

FENWICK, Mark; VERMEULEN, Erik PM; CORRALES, Marcelo. Business and regulatory responses to artificial intelligence: Dynamic regulation, innovation ecosystems and the strategic management of disruptive technology. En Robotics, AI and the Future of Law. Singapore: Springer Singapore, 2018. p. 81-103.

FERNÁNDEZ-ALLER, Celia y SERRANO, María. *¿Es posible una Inteligencia artificial respetuosa con la protección de datos?* Doxa. Cuadernos de Filosofía del Derecho (45): pp. 307-336, 2022.

FERNÁNDEZ, Ana. *Inteligencia artificial en los servicios financieros*. Boletín económico/Banco de España. 2: 2019, pp. 1-8.

FERNÁNDEZ, Berta. *Discriminación Algorítmica.* Tesis (Grado en Ingeniería de Tecnología y Servicios de Telecomunicación). Madrid, España. Universidad Autónoma de Madrid, Escuela Politécnica Superior, 2019.

FERNÁNDEZ Fredes, Francisco. *La regulación de la actividad económica y los derechos del consumidor. La experiencia chilena*.Temas de Derecho del Consumidor, 1997, pp. 13 y 14.

FERRANTE, Enzo. *Inteligencia artificial y sesgos algorítmicos: ¿Por qué deberían importarnos?*. Buenos Aires, Nueva sociedad, 2021, no 294, p. 27-36.

FLACH, Peter. *Machine learning: the art and science of algorithms that make sense of data*. Nueva York, Cambridge University Press, 2012.

FUENZALIDA, Eduardo. *El acto de consumo como hecho y la responsabilidad civil.* [en línea] Revista de derecho (Coquimbo), Jun. 2018, Vol. 25, n° 1, p. 121-152 <https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-97532018000100121> [consulta: 30 junio 2023].

FUNDACIÓN DATOS PROTEGIDOS*. Una propuesta a la ley de datos personales en Chile. Los datos más allá de la privacidad.* Santiago, Chile < https://datosprotegidos.org/wp-content/uploads/2017/11/InformeLeyDatos_FDP-3.pdf> [consulta: 02 septiembre 2023].

GARRIDO, Romina. *El Habeas data y la ley de protección de datos en Chile.* Serie Bibliotecología y Gestión de Información, (83):1-24, Jul-2013.

GARRO, Alejandro. *El Derecho Internacional Privado en los Estados Unidos: Balance y Perspectivas.* Revista Mexicana de Derecho Internacional Privado, Número especial, pp. 97-114, 2000.

GATICA, María Paz, MORALES, María Elisa. *El deber de profesionalidad como elemento determinante del estándar de diligencia en el derecho del consumo: un comentario a la*

sentencia de la Corte de Apelaciones de San Miguel de 15 de marzo de 2019 (Rol Nº 484-2018). Revista de derecho (Coquimbo) 29: pp. 1-16, 2022.

GAUTIER, Axel, ITTOO, Ashwin, VAN CLEYNENBREUGEL, Pieter. *AI algorithms, price discrimination and collusion: a technological, economic and legal perspective*. European Journal of Law and Economics, 50(3): pp. 405-435, jul. 2020.

GRAFANAKI, Sofía. *Autonomy challenges in the age of big data*. Fordham Intell. Prop. Media & Ent. LJ. 27(4): 2016, pp. 803-868.

GRETZEL, U., FESENMAIER, D, O'LEARY, J. *The transformation of consumer behaviour.* Tourism business frontiers: Consumers, products and industry, 9: pp. 7-16, 2006.

GUAÑA-MOYA, E., QUINATOA-AREQUIPA, E, PÉREZ-FABARA, M. T*endencias del uso de las tecnologías y conducta del consumidor tecnológico*. Ciencias Holguín, 23(2): pp. 15-30, 2017.

GURSOY, F., KENNEDY, R. y KAKADIARIS, I. *A critical assessment of the algorithmic accountability act of 2022*. [en línea] Available at SSRN 4193199 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4193199> [consulta: 14 noviembre 2023].

HARARI, Yuval Noah. *Homo Deus. Breve historia del mañana*. Buenos Aires, Ed. Debate, 2015.

HARGITTAI, Eszter y MARWICK, Alice. *"What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy.* International Journal of Communication 10(0): pp. 3737-3757, 2016.

HEISS, Stefan. *Towards Optimal Liability for Artificial Intelligence: Lessons from the European Union's Proposals of 2020*. [en línea] Hastings Sci. & Tech. LJ, 2021, vol. 12, p. 205. <https://heinonline.org/HOL/LandingPage?handle=hein.journals/hascietlj12&div=11&id=&page=> [consulta: 13 octubre 2023].

HELBERGER, N. y DIAKOPOULOS, N. *ChatGPT and the AI Act.* [en línea] Internet Policy Review, 16 Feb 2023, Vol. 12, n° 1 <https://policyreview.info/essay/chatgpt-and-ai-act> [consulta: 26 noviembre 2023].

HERNÁNDEZ Paulsen, Gabriel. *La obligación precontractual de la entidad de crédito de informar al cliente en los servicios bancarios y de inversión*. Madrid, Marcial Pons, 2014.

HERRERA, Diego; VADILLO, Sonia. *Sandbox* Regulatorio en América Latina y el Caribe para el ecosistema FinTech y el sistema financiero. Banco Interamericano de Desenvolvimento-BID, 2018.

HOFFMANN-RIEM, Wolfgang. Artificial intelligence as a challenge for law and regulation. Regulating artificial intelligence, 2020, p. 1-29.

HUESO, Lorenzo Cotino. Riesgos e impactos del Big Data, la inteligencia artificial y la robótica: enfoques, modelos y principios de la respuesta del derecho. Revista general de Derecho administrativo. (50): pp. 1-37, 2019.

HUESO, Lorenzo. *Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida*. [en línea] Revista española de la transparencia, n°. 16, p. 17-63 <https://dialnet.unirioja.es/servlet/articulo?codigo=8913030> [consulta: 23 noviembre 2023].

INSTITUTO DATA SCIENCE UDD y AMCHAM CHILE. *AI Readiness. 2° Diagnóstico de la adopción de la inteligencia artificial IA de empresas en Chile.* [en línea]. <https://ingenieria.udd.cl/files/2023/06/2023-05-10-ai-readiness-2023.pdf> [consulta: 30 agosto 2023].

ISLER Soto, Erika. *Aproximación al derecho a la no discriminación arbitraria en el régimen de la Ley 19.496.* Revista de Derecho Público (4): 2016, pp. 99-113.

ISLER, Erika. *Plataformas digitales y relación de consumo en Chile: un desafío actual.* En su: *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos.* 1ºed. Chile, Rubicón Editores, 2023. 189-199pp.

ISLER, Erika. *Derecho del consumo. Nociones fundamentales*. Valencia, Tirant lo Blanch, 2021.

JERVIS, Paula. La regulación del mercado de datos personales en Chile. Tesis (Magíster en Derecho). Santiago, Chile. Universidad de Chile, Facultad de Derecho, 2006.

JUÁREZ, Isabel Antón, et al. Marketplaces que personalizan precios a través del big data y de los algoritmos: ¿esta práctica es legal en atención al derecho de la competencia europeo?. Cuadernos de derecho transnacional, 2021, vol. 13, no 1, p. 42-69.

KASSIR, Sara. *Algorithmic Auditing: The Key to Making Machine Learning in the Public Interest*. [en línea] IBM Center for The Business of Government. Viewpoints. Winter 2019/2020. <https://www.businessofgovernment.org/sites/default/files/Algorithmic%20Auditing.pdf> [consulta: 10 septiembre 2023]

KINGSTON, John. *Using artificial intelligence to support compliance with the general data protection regulation*. Artificial Intelligence and Law. 25 (4): 2017, pp. 429-443.

KNIGHT, Will. *Microsoft is creating an oracle for catching biased AI algorithms*. [en línea] MIT Technology Review. 25 de mayo, 2018 <https://www.technologyreview.com/2018/05/25/66849/microsoft-is-creating-an-oracle-for-catching-biased-ai-algorithms/> [consulta: 10 septiembre 2023].

KÖCHLING, Alina y WEHNER, Marius. *Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development*. Business Research 13(3): p, 796. 2020.

LABBÉ Figueroa, María. 2020. *Big Data: Nuevos desafíos en materia de libre competencia*. Revista chilena de derecho y tecnología. 9(1): pp. 33-62.

LALALEO, F., BONILLA, D., ROBLES, R. 2021. *Tecnologías de la Información y Comunicación exclusivo para el comportamiento del consumidor desde una perspectiva teórica.* Retos: Revista de Ciencias de la Administración y Economía, 11(21): pp. 147-164.

LIGÜERRE, Carlos Gómez. La Propuesta de Directiva sobre responsabilidad por daños causados por productos defectuosos. InDret, 2022 <https://www.raco.cat/index.php/InDret/article/download/406110/500347> [consulta: 07 diciembre 2023].

LIPPI, Marco, et al. *CLAUDETTE: an automated detector of potentially unfair clauses in online terms of service*. [en línea] Artificial Intelligence and Law, Feb-2019, vol. 27, pp. 117-139 <https://link.springer.com/article/10.1007/s10506-019-09243-2> [consulta: 04 octubre 2023].

LLAMAS, Jersain, et al. 2022. Enfoques regulatorios para la Inteligencia Artificial (IA). Revista chilena de derecho, vol. 49, no 3, pp. 31-62.

LOGG, Jennifer. M., MINSON, Julia. A., MOORE, Don A., 2019. *Algorithm appreciation: People prefer algorithmic to human judgment.* Organizational Behavior and Human Decision Processes. 151: pp. 90-103, mar. 2019.

LÓPEZ, Patricia. *El consumidor hipervulnerable como débil jurídico en el derecho chileno: una taxonomía y alcance de la tutela aplicable*. Latin american legal studies, 10(2): 2022, pp. 340-415.

LOPEZ, David, et al. *Self-Regulation of electronic commerce: Issues in the context of Chilean Law.* Revista Chilena de Derecho, 2017, vol. 44, p. 347-369.

LOVELACE, Ada; DATAKIND, U. K. *Examining the black box: Tools for assessing algorithmic systems*. [en línea] Technical report, AdaLovelace Institute, 2020 <https://ico. org. uk/media/about-theico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf> [consulta: 02 diciembre 2023].

MANTILLA Gonzales de la Cotera, Eduardo Javier. *La paradoja de la privacidad de la información en los servicios de Internet*. Tesis (Maestría en Investigación en Ciencias de la Administración). Lima, Perú. Universidad ESAN, Graduate School of Business, 2019.

MARTÍN, Sara. *Cambio de horizontal a vertical: el dilema de la responsabilidad de los intermediarios de intercambio de contenidos protegidos en el derecho europeo*. En: CORNEJO, M. e ISLER, E. (Eds.). *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. Santiago, Rubicón Editores, 2023. pp. 171-173.

MARTORELL, Matías. *Análisis crítico del deber del proveedor de informar en forma veraz y oportuna impuesto por el Artículo 3 Letra B) de la Ley de Protección al Consumidor*. Tesis (Licenciatura en Ciencias Jurídicas y Sociales). Santiago, Chile. Universidad de Chile, Facultad de Derecho, 2015.

MENDOZA, Olivia. *El derecho de protección de datos personales en los sistemas de inteligencia artificial.* REVISTA IUS. 15(48): 2022.

MIK, Eliza. *The erosion of autonomy in online consumer transactions*. Law, Innovation and Technology. 8(1): 2016, pp. 1-38.

MÖKANDER, J., JUNEJA, P., WATSON, D.S. y FLORIDI, L., 2022. *The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other?* [en línea] Minds and Machines, Agosto-2022, Vol. 32, n°. 4 <https://link.springer.com/article/10.1007/s11023-022-09612-y> [consulta: 18 octubre 2023].

MOMBERG Uribe, Rodrigo. *Ámbito de Aplicación de la Ley No 19.496 Sobre Protección de los Derechos de los Consumidores*. Revista de Derecho (Valdivia). 17: 2004, pp. 41-62.

MOMBERG, Rodrigo. *El control de las cláusulas abusivas como instrumento de intervención judicial en el contrato*. Revista de derecho (Valdivia). 26(1): 2013, pp. 9-27.

MOMBERG URIBE, Rodrigo; MORALES ORTIZ, Maria Elisa. 2019. *Las cláusulas relativas al uso y tratamiento de datos personales y el artículo 16 letra g) de la Ley 19.496 sobre*

Protección de los Derechos de los Consumidores. [en línea] Revista chilena de derecho y tecnología 8(2): 157-180, <https://www.scielo.cl/scielo.php?pid=S0719-25842019000200157&script=sci_arttext> [consulta: 17 septiembre 2023].

MOMBERG, Rodrigo; DE LA MAZA GAZMURI, Iñigo; PIZARRO WILSON, Carlos. *La protección de los derechos de los consumidores: Comentario a la ley de protección a los derechos de los consumidores*. Santiago, Thomson Reuters, 2013.

MOTA, Eva y HERRERA, Esther. 2023. *Auditoría algorítmica en la inteligencia artificial en el sector público.* [en línea] Revista Digital Instituto de Investigaciones y Estudios Contables - FCE UNLP (17) <https://revistas.unlp.edu.ar/proyecciones/article/view/14782> [consulta: 09 septiembre 2023].

MURILLO DE LA CUEVA, Pablo. *La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*. En su: *La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad*. España, Fundación Coloquio Jurídico Europeo, 2009.

ORGANIZACIÓN DE NACIONES UNIDAS (ONU). 1979. *Convención sobre la eliminación de todas las formas de discriminación contra la mujer*. [en línea] <https://www.oas.org/dil/esp/convencion_sobre_todas_las_formas_de_discriminacion_contra_la_mujer.pf> [consulta: 12 de octubre de 2023].

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), 2021. *Principios Actualizados sobre la Privacidad y la Protección de Datos Personales* [en línea]. <https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf> [consulta: 09 julio 2023].

PALOMARES, Elena. *La intermediación en los contratos de consumo.* Tesis (Doctorado en Derecho con mención en Doctorado Europeo). Barcelona, España. Universidad de Barcelona, Facultad de Derecho, 2014.

PANTALEÓN Prieto, Ángel. *Causalidad e imputación objetiva: criterios de imputación.* Asociación de Profesores de Derecho Civil (coords.). Centenario del Código Civil (1889-1989). Tomo II. Madrid, Editorial Universitaria Ramón Areces, pp. 1561-1591, 1990.

PANTANO, Eleonora y SCARPI, Daniele. *I, robot, you, consumer: Measuring artificial intelligence types and their effect on consumers emotions in service*. Journal of Service Research 25(4): pp. 583-600, 2022.

PEÑA Lorenzo, José María. *Aplicación de técnicas de aprendizaje profundo (deep learning) para la detección de objetos en Industria 4.0.* Tesis (Máster en Ingeniería de Telecomunicación). Valladolid, España, Universidad de Valladolid, Escuela Técnica Superior de Ingenieros de Telecomunicación, 2022.

PERAULT, M., 2023. Section 230 Won't Protect ChatGPT. J. Free Speech L., vol. 3, p. 365.

PETRILLO, P. *Las violencias invisibles: sesgo algorítmico, discriminación y violencia algorítmica de género.* Diario La Ley, 2022, 86(94), 1-5.

PIZARRO, Carlos. *La eficacia del control de las cláusulas abusivas en el derecho chileno.* Estudios Socio-Jurídicos. 6(2): 2004, pp. 117-141.

POOLE, David, MACKWORTH, Alan, GOEBEL, Randy. *Computational intelligence: a logical approach*. Nueva York, Oxford University Press, 1998.

PORCELLI, Adriana y MARTÍNEZ, Adriana, 2021. *La Neurociencia aplicada a la Inteligencia Artificial: ¿un camino hacia la Inteligencia Artificial General?* [en línea], <https://www.researchgate.net/publication/351987016_La_Neurociencia_aplicada_a_la_Inteligencia_Artificial_un_camino_hacia_la_Inteligencia_Artificial_General> [consulta: 05 julio 2023].

PUNTONI, Stefano, et al. *Consumers and artificial intelligence: An experiential perspective.* Journal of Marketing, 2021, vol. 85, no 1, p. 131-151.

RADER, Emilee, COTTER, Kelley, CHO, Janghee. *Explanations as mechanisms for supporting algorithmic transparency*. Proceedings of the 2018 CHI conference on human factors in computing systems (103): pp. 1-13, abr. 2018.

ROCA, J., 2023. *¿Pueden los algoritmos ser evaluados con rigor?* Encuentros Multidisciplinares 25(73).

RODRÍGUEZ, N., VÁZQUEZ, J. y MARTÍNEZ, M. *El comercio electrónico y la asimetría de la información: una aproximación de los costes de transacción*. Revista galega de economía, 12(1): pp. 167-192, 2003.

ROMERO, Sebastián. El Desafío Regulatorio de las Nuevas Tecnologías: Análisis del Uso de Datos Personales e Inteligencia Artificial en el Contexto de Campañas Electorales. Una Mirada Nacional y Comparada. Tesis (Licenciatura en Ciencias Jurídicas y Sociales). Santiago, Chile. Universidad de Chile, Facultad de Derecho, 2023.

RUBÍ PUIG, Antoni. *Elaboración de perfiles y personalización de ofertas y precios en la contratación con consumidores*. Revista de educación y derecho= Education and law review,. 24: 2021, pp. 1-24.

SACRISTÁN, Estela. *Teoría de la regulación (en especial, acerca de los fundamentos de la regulación*. Derecho PUCP. (76): 2016, pp. 77-104.

SALESFORCE. Business Adopting AI Risk a 'Trust Gap' with Customers – Salesforce Report. [en línea] <https://www.salesforce.com/news/stories/customer-engagement-research-2023/> [consulta: 30 agosto 2023].

SÁNCHEZ VÁSQUEZ, Carolina; TORO-VALENCIA, José. *El derecho al control humano: Una respuesta jurídica a la inteligencia artificial.* [en línea] Revista chilena de derecho y tecnología. Dic-2021, Vol. 10, n° 2 <https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842021000200211> [consulta: 16 de agosto de 2023].

SANCHO CAPARRINI, Fernando. 2015. Redes neuronales: una visión superficial [en línea]. Dpto. deficiencias de la computación e inteligencia artificial - Universidad de Sevilla. <http://www.cs.us.es/~fsancho/?p=inteligencia-artificial-2022-23> [consulta: 13 septiembre 2023].

SANDVIG, Christian, et al. *Data and discrimination: Converting critical concerns into productive inquiry.* En Data and Discrimination: Converting Critical Concerns into Productive Inquiry at the Annual Meeting of the International Communication Association. 2014.

SANGÜESA, Ramón. *Inteligencia artificial y transparencia algorítmica: It's complicated.* BiD: textos universitaris de biblioteconomia i documentació. 41: 2018, pp. 1-4.

SANTOS Morón, M. *Derecho de daños e inteligencia artificial: hacia una posible regulación en la UE.* En: CORNEJO, M. e ISLER, E. (Eds.). *Temas actuales sobre consumo, inteligencia artificial, plataformas digitales y neuroderechos*. Santiago, Rubicón Editores, 2023.pp. 137-150.

SARTOR, Giovani, 2020. *New aspects and challenges in consumer protection*. [en línea], <https://policycommons.net/artifacts/1336949/new-aspects-and-challenges-in-consumer-protection/1944500/> [consulta: 01 julio 2023].

SCHUETT, Jonas. *Risk management in the artificial intelligence act.* [en línea] European Journal of Risk Regulation, 08 de febrero de 2023, <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/risk-management-in-the-artificial-intelligence-act/2E4D5707E65EFB3251A76E288BA74068> [consulta: 01 diciembre 2023].

Smart nudging: How cognitive technologies enable choice architectures for value co-creation por Cristina Mele "et al". Journal of Business Research, 129, pp. 949-960.

SMITH, Gary. *Artificial Intelligence and the privacy paradox of opportunity, Big Data and the Digital universe*. En: 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (2019).

SUNSTEIN, Cass y THALER, Richard. *Un pequeño empujón*. 1ª ed. Madrid, Taurus, 2017.

TAMAYO VELASCO, Jimena, et al. Big data, competencia y protección de datos: el rol del Reglamento General de Protección de Datos en los modelos de negocio basados en la publicidad personalizada. Revista de estudios europeos, 2021, N.78, pp.183-202.

THE EUROPEAN CONSUMER ORGANISATION (BEUC), 2019. *AI RIGHTS FOR CONSUMERS*. [en línea], <https://www.beuc.eu/sites/default/files/publications/beuc-x-2019-063_ai_rights_for_consumers.pdf> [consulta: 01 julio 2023].

TORROBA, Alejandra. *El impacto social de los algoritmos*. Tesis (Grado en Sistemas de Información). Madrid, España. Universidad Politécnica de Madrid, 2023.

FELZMANN, Heike, et al. *Towards transparency by design for artificial intelligence.* Science and Engineering Ethics, 26(6):3333-3361, 2020.

TREMBLE, Catherine. *Wild Westworld: Section 230 of the CDA and Social Networks' Use of Machine-Learning Algorithms*. Fordham L. Rev. 86: 2017, pp. 825-869.

TURNER, Jacob. *Robot rules: Regulating artificial intelligence*. New York, Springer, 2018.

UNESCO. 2021. *Recommendation on the ethics of artificial intelligence*. [en línea] <https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa> [consulta: 11 septiembre 2023].

VAROŠANEC, Ida. *On the path to the future: mapping the notion of transparency in the EU regulatory framework for AI.* [en línea] International Review of Law, Computers & Technology, 08 de abril de 2022, Vol. 36, n° 2 <https://www.tandfonline.com/doi/full/10.1080/13600869.2022.2060471> [consult: 17 noviembre 2023].

VIAL CLARO, Felipe. *La ley Nº 19.628 sobre protección de datos de carácter personal. Una visión general*. En: "Tratamiento de datos personales y protección de la vida privada",

BERTELSEN et al., 3ª edición, Cuadernos de extensión Jurídica, Ediciones Universidad de Los Andes, 2001.

VERDUGO, Francisco. *Los principios, derechos del titular de datos y deberes del responsable de datos, en la Ley Nº 19.628.* En "Derecho Informático", JIJENA, Renato. Santiago, El Jurista, 2022.

VERMA, Sahil y RUBIN, Julia. *Fairness definitions explained* [en línea]. Proceedings of the International Workshop on Software Fairness, FairWare'18, May 2018, pp. 1-7 < https://dl.acm.org/doi/10.1145/3194770.3194776> [consulta: 10 septiembre 2023].

WALDMAN, Ari. *Cognitive biases, dark patterns, and the 'privacy paradox*'. Current Opinion in Psychology. 31: 2020, pp. 105-109.

WEINMANN, Marcus, SCHNEIDER, Christoph, BROCKE, Jan Vom. *Digital nudging*. Business & Information Systems Engineering, 58, pp. 433-436, oct. 2016.

WERTENBROCH, Klaus, et al. 2020. *Autonomy in consumer choice.* [en línea] Marketing letters, 31: 429-439. <https://link.springer.com/article/10.1007/s11002-020-09521-z> [consulta: 17 octubre 2023].

YEOMANS, Michael, et al. *Making sense of recommendations*. [en línea] Journal of Behavioral Decision Making, Feb-2019, Vol. 32, n° 4, p. 403-414 <https://onlinelibrary.wiley.com/doi/abs/10.1002/bdm.2118> [consulta: 17 septiembre 2023].

ZAROR, Danielle. *¿Por qué resulta tan problemático regular la tecnología?* En: AZUAJE Pirela, M (coord.). *Introducción a la ética y el derecho de la inteligencia artificial*. Madrid, Wolters Kluwer-La Ley, 2023. pp. 238-248.

ZEIN, Dr Sarah. 2023. *The Civil Liability for Artificial Intelligence*. [en línea] BAU Journal-Journal of Legal Studies-مجلة الدراسات القانونية. Vol. 2022(1). <https://digitalcommons.bau.edu.lb/lsjournal/vol2022/iss1/14/> [consulta: 05 de diciembre de 2023].

ZUIDERVEEN, Frederik, 2018. *Discrimination, artificial intelligence, and algorithmic decision-making* [en lìnea], pp. 10-14. Council of Europe, Directorate General of Democracy, <https://pure.uva.nl/ws/files/42473478/32226549.pdf> [consulta: 08 julio 2023].

ZUMARÁN, M.G. y ALONZO, MEJÍAS. *El proveedor intermediario de servicios y su responsabilidad. Un estudio del artículo 43 de la Ley 19.496.* en línea] Revista de Derecho, 2021, Vol. 34, n° 2, pp. 29-50 <https://www.scielo.cl/scielo.php?pid=S0718-09502021000200029&script=sci_arttext&tlng=pt> [consulta: 03 noviembre 2023].

ZÚÑIGA Denegri, Martín. *Principio de préstamo responsable. Naturaleza y fuentes legales en el ordenamiento jurídico chileno.* Revista de Derecho Económico. 79(2): 2022, pp. 99-126.

Material normativo

CÁMARA DE DIPUTADOS (Chile). Proyecto de Ley que Regula los Sistemas de Inteligencia Artificial, la Robótica y las Tecnologías Conexas en sus Distintos Ámbitos de Aplicación. Boletín Nº 15.869-19, refundido con Boletín Nº 16.821-19. Valparaíso, Chile, 24 de abril de 2023.

CONGRESO de los Estados Unidos (Estados Unidos). *Communications Decency Act of 1996.* Washington D.C., Estados Unidos, 08 de febrero de 1996.

CONGRESO de los Estados Unidos (Estados Unidos). *H.R. 5628 - Algorithmic Accountability Act of 2023.* Washington D.C., Estados Unidos, 21 de septiembre de 2023.

CONGRESO de los Estados Unidos (Estados Unidos). *H.R.6216 - National Artificial Intelligence Initiative Act of 2020*. Washington D.C., Estados Unidos, 12 de marzo de 2020.

CONGRESO de los Estados Unidos (Estados Unidos). *H.R.6796 - Digital Services Oversight and Safety Act of 2022*. Washington D.C., Estados Unidos, 18 de febrero de 2022.

CONGRESO de los Estados Unidos (Estados Unidos). *H.R.8152 - American Data Privacy and Protection Act.* Washington D.C., Estados Unidos, 21 de junio de 2022.

CONGRESO de los Estados Unidos (Estados Unidos). *S.2325 - Algorithmic Justice and Online Platform Transparency Act*. Washington D.C., Estados Unidos, de 13 de julio de 2023.

CONGRESO de los Estados Unidos (Estados Unidos). *S.4201 - Digital Platform Commission Act of 2022*. Washington D.C., Estados Unidos, 12 de mayo de 2022.

Decreto 374. CHILE. Código de Derecho Internacional Privado. Ministerio de Relaciones Exteriores, Santiago, Chile, 25 de abril de 1934.

Decreto con Fuerza de Ley N° 1. CHILE. Fija Texto Refundido, Coordinado y Sistematizado del Código Civil; de la Ley Nº4.808, Sobre Registro Civil, de la Ley Nº17.344, que Autoriza Cambio de Nombres y Apellidos, de la Ley N°16.618, Ley de Menores, de la Ley N°14.908, sobre Abandono de Familia y Pago de Pensiones Alimenticias, y de la Ley N°16.271, de Impuesto a las Herencias, Asignaciones y Donaciones. Ministerio de Justicia, Santiago, Chile, 30 de mayo de 2000.

Decreto con Fuerza de Ley N° 3. CHILE. Fija Texto Refundido, Coordinado y Sistematización de la Ley N° 19.496, que Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 31 de mayo de 2021.

Decreto Ley N° 211. CHILE. Fija el Texto Refundido, Coordinado y Sistematizado del Decreto Ley N°211, de 1973. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 07 de marzo de 2005.

Ley Nº 19.496. CHILE. Establece Normas sobre Protección de los Derechos de los Consumidores. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 07 de febrero de 1997.

Ley N° 19.628. CHILE. Sobre Protección de la Vida Privada. Ministerio Secretaría General de la Presidencia, Santiago, Chile, 28 de agosto de 1999.

Ley Nº 20.575. CHILE. Establece el Principio de Finalidad en el Tratamiento de Datos Personales. Ministerio de Economía, Fomento y Turismo, Santiago, Chile, 17 de febrero de 2012.

MINISTERIO de Economía, Fomento y Turismo (Chile). Decreto 6 que Aprueba Reglamento de Comercio Electrónico. Santiago, Chile, 23 de septiembre de 2021.

MINISTERIO de Economía, Fomento y Turismo (Chile). Proyecto de ley que mejora la protección de los derechos de las personas consumidoras en el ámbito de sus intereses individuales fortaleciendo al Servicio Nacional del Consumidor, y establece otras modificaciones que indica. Boletín N° 16.271-03. Santiago, Chile, septiembre del 2023.

MINISTERIO Secretaría General de la Presidencia (Chile). Proyecto de ley sobre Protección de Datos Personales. Boletín N° 11.092-07. Santiago, Chile, enero del 2017.

MINISTERIO Secretaría General de la Presidencia (Chile). Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Boletín N° 11.144-07. Santiago, Chile, marzo del 2017.

PARLAMENTO Europeo (Unión Europea). Resolución del Parlamento Europeo con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas. Bruselas, Bélgica, 20 de octubre de 2020.

PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. Bruselas, Bélgica, 2000.

PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo relativa a la adaptación de las normas de responsabilidad civil extracontractual a la Inteligencia Artificial. Bruselas, Bélgica, 2022.

PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo sobre los derechos de los consumidores, por la que se modifican la Directiva 93/13/CEE del Consejo y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo. Bruselas, Bélgica, 2011.

PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por los daños causados por productos defectuosos. Bruselas, Bélgica, 2022.

PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (AI ACT) y se modifican determinados actos legislativos de la unión. Bruselas, Bélgica, 2021.

PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Bruselas, Bélgica, 2016.

PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2019/1150 sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea. Bruselas, Bélgica, 2019.

PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/1925 sobre mercados disputables y equitativos en el sector digital. Bruselas, Bélgica, 2022.

PARLAMENTO Europeo y Consejo de la Unión Europea (Unión Europea). Reglamento 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE. Bruselas, Bélgica, 2022.

PRESIDENTE de los Estados Unidos (Estados Unidos). *Executive Order N° 13.960, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, 03 de diciembre de 2020.

PRESIDENTE de los Estados Unidos (Estados Unidos). *Executive Order N° 14.110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 de octubre de 2023.

SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 33 que Aprueba Circular Interpretativa sobre Protección de los Consumidores frente al uso de sistemas de Inteligencia Artificial en las relaciones de consumo. Santiago, Chile, 18 de enero de 2022.

SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 174 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores. Santiago, Chile, 28 de febrero de 2022.

SERVICIO Nacional del Consumidor (Chile). Resolución Exenta Nº 931 que Aprueba Circular Interpretativa sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión de consumo. Santiago, Chile, 03 de diciembre de 2021.

SERVICIO Nacional del Consumidor (Chile). Resolución Exenta N° 1038 Aprueba Circular Interpretativa sobre noción de consumidor hipervulnerable, Santiago, Chile, 31 de diciembre de 2021.

TRIBUNAL de Defensa de la Libre Competencia (Chile). Auto Acordado N° 16 sobre reserva o confidencialidad de la información en los procesos. Santiago, Chile, 15 de mayo de 2017.

Jurisprudencia

Excma. Corte Suprema, Sentencia Rol Nº 1533-2015, de 07 de julio de 2016.

Excma. Corte Suprema, Sentencia Rol Nº 92134-2020, de 03 de julio de 2023.

Ilma. Corte de Apelaciones de Antofagasta, Sentencia Rol Nº 18-2017, de 04 de abril de 2017.

Ilma. Corte de Apelaciones de Santiago, Sentencia Rol Nº 792-2013, de 15 de abril de 2014.

Ilma. Corte de Apelaciones de Santiago, Sentencia Rol Nº 1253-2015, de 20 de enero de 2016.

Ilma. Corte de Apelaciones de Santiago, Sentencia Rol Nº 707-2021, de 07 de junio de 2021.

Ilma. Corte de Apelaciones de Talca, Sentencia Rol Nº 55-2020, de 29 de octubre de 2020.

Páginas web

CÁMARA DE DIPUTADAS Y DIPUTADOS. *Tratamiento de datos personales tendrá nuevo marco legal.* [en línea] 08 de mayo 2023, <https://www.camara.cl/cms/noticias/2023/05/08/tratamiento-de-datos-personales-tendra-nuevo-marco-legal/> [consulta: 15 de octubre 2023].

EUROPA. *Reglamento General de Protección de Datos.* [en línea] 06 de julio 2022 <https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm> [consulta: 22 de octubre 2023].

EY. *Proyecto de ley de datos personales: ¡Qué se viene para este año 2023?* [en línea] 18 de enero 2023 <https://www.ey.com/es_cl/tax/ey-tax-alert-chile/proyecto-de-ley-de-datos-personales-que-se-viene-para-este-anio-2023> [consulta: 18 de octubre 2023].

ZTZ. TECH GROUP. *5 beneficios clave de incorporar la Inteligencia Artificial en la gestión de reclamos.* [en línea] <https://ztz.ai/5-beneficios-clave-de-incorporar-la-inteligencia-artificial-en-la-gestion-de-reclamos/> [consulta: 10 septiembre 2023].