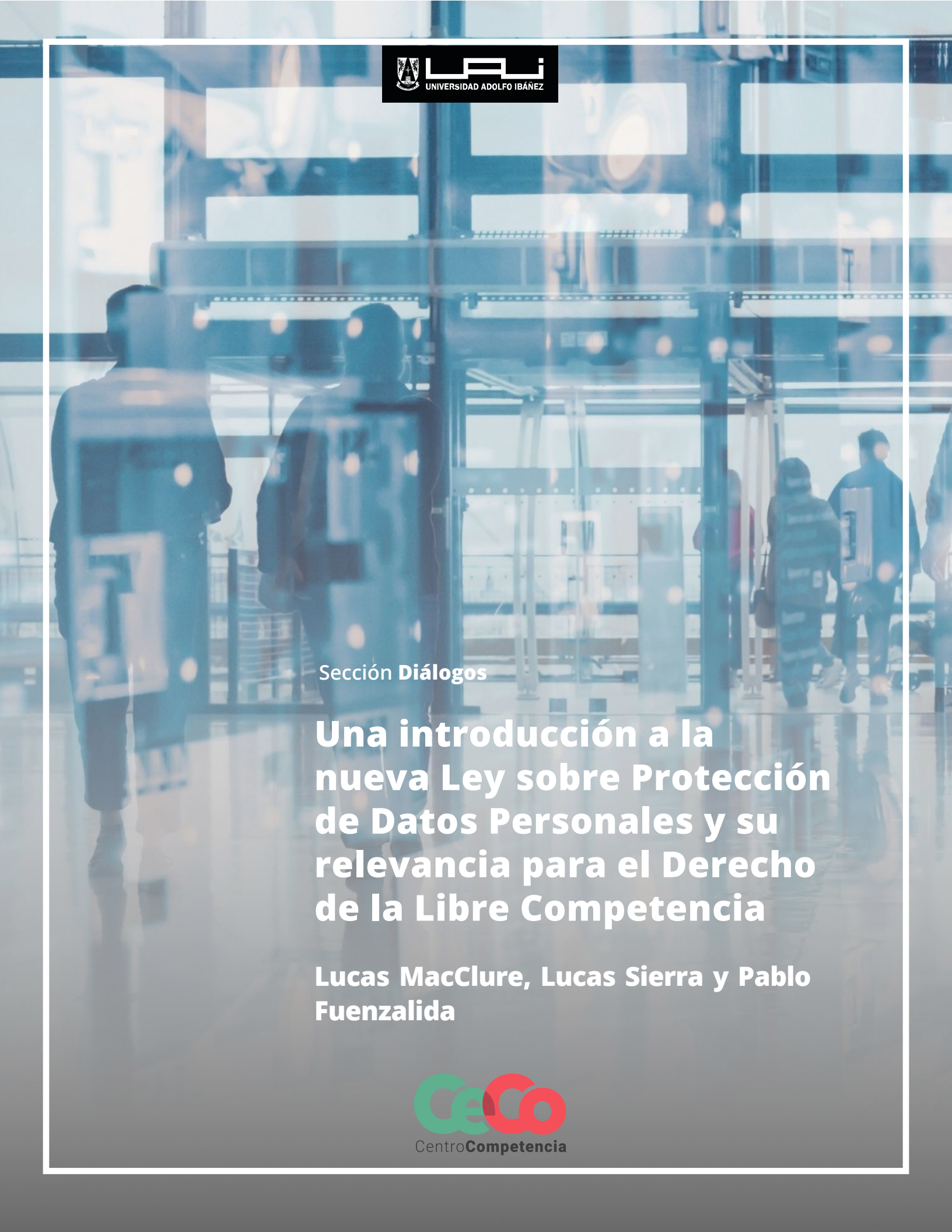

Sección **Diálogos**

Una introducción a la nueva Ley sobre Protección de Datos Personales y su relevancia para el Derecho de la Libre Competencia

Lucas MacClure, Lucas Sierra y Pablo Fuenzalida

Lucas MacClure B.

Abogado Universidad de Chile, LL.M. y J.S.D. Yale University. Socio de Lupa Legal.

Lucas Sierra I.

Abogado Universidad de Chile, LL.M. Yale University, Ph.D. Cambridge University. Profesor de Regulación de Telecomunicaciones y Profesión Jurídica en la Universidad de Chile. Socio de Lupa Legal.

Pablo Fuenzalida C.

Abogado Universidad de Chile. LL.M. UC Berkeley, MSc y Ph.D. University of Bristol. Profesor de Profesión Jurídica en la Universidad de Chile. Socio de Lupa Legal.

Noviembre 2024

Una introducción a la nueva Ley sobre Protección de Datos Personales y su relevancia para el Derecho de la Libre Competencia[1]

Abstract: Este artículo ofrece una introducción a la futura Ley sobre Protección de Datos Personales (LPDP) dirigida especialmente a profesionales del derecho de la libre competencia. Específicamente, el trabajo aborda el proyecto de ley que busca crear la LPDP mediante una reforma a la Ley Nº 19.628 sobre Protección de la Vida Privada (1999), según la versión aprobada por el Congreso y el Presidente en agosto y septiembre de 2024. Tras argumentar brevemente que la LPDP será relevante para el derecho de la libre competencia, la mayor parte del trabajo se dedica a describir el proyecto de ley. Resumimos los fines buscados por el legislador y sus implicancias para la interpretación de la LPDP, el ámbito de esta ley y sus varias reglas de conducta, su *enforcement* y otras instituciones de cumplimiento, el contexto regulatorio en el cual operará, y cómo la LPDP aborda la colaboración y los conflictos de competencia entre su agencia y otros órganos administrativos.

1 Este artículo fue encargado por el CentroCompetencia (CeCo) de la Universidad Adolfo Ibáñez. Agradecemos los excelentes comentarios y consejos de Ivonne Bueno, Pablo Contreras, Sebastián Dufeu, Juan Pablo Iglesias, Tamara Sandoval y Danielle Zaror.

Contenido

Una introducción a la nueva Ley Sobre Protección de Datos Personales y su relevancia para el Derecho de la Libre Competencia

INTRODUCCIÓN (RESUMEN EJECUTIVO)

El objeto de este artículo es ofrecer una introducción a la futura Ley Sobre Protección de Datos Personales ("LPDP" o la "Ley")[2], especialmente para profesionales del derecho de la libre competencia.[3] La LPDP es el resultado del proyecto de ley boletín Nº 11.144-07, que busca reformar la Ley Nº 19.628 Sobre Protección a la Vida Privada (1999).[4] El proyecto ya fue aprobado por el Congreso y el Presidente de la República en agosto y septiembre de 2024 (respectivamente); al cierre de este trabajo en octubre de 2024, solo falta que el Tribunal Constitucional termine de revisar el proyecto para que éste se convierta en ley.[5] Aquí asumimos que esta última etapa será sorteada, y nos referiremos al proyecto de ley como si ya fuera una ley de la República. Bajo esta premisa, la LPDP entrará en vigor a fines del año 2026 o a principios del 2027 (dependiendo de su fecha de publicación).[6]

La LPDP, como su antecesora la Ley Nº 19.628 Sobre Protección a la Vida Privada de 1999, regulará la manera como las empresas, órganos públicos, otras organizaciones y personas naturales –los "responsables" (o, en algunos casos, los "encargados")– recolectan y de otras maneras usan –realizan "tratamidento"– de información sobre personas naturales específicas –los "titulares"– con el fin de proteger sus intereses (art. 2). [7] Esta regulación busca garantizar el derecho fundamental de los titulares a la protección de sus datos personales, también conocido como el derecho a la "autodeterminación informativa". La protección de datos personales también está asociada a los conceptos jurídicos y morales de "vida privada" o "privacidad" (y *privacy* del derecho norteamericano), aunque la relación precisa entre estos conceptos es debatida.[8]

La LPDP es una cirugía mayor a la Ley Nº 19.628 y en general a la regulación chilena sobre datos personales. Tanto por la extensión de la LPDP –tiene 83 artículos permanentes; su antecesora tenía 24– como por las

2 Este trabajo utiliza varias abreviaturas. Junto a señalarlas en el texto principal la primera vez que son utilizadas, las compilamos en esta nota al pie: Agencia = Agencia de Protección de Datos Personales contemplada por la nueva Ley sobre Protección de Datos Personales; Fiscalía = Fiscalía Nacional Económica; GDPR = *General Data Protection Regulation* de la Unión Europea; LPDP = Ley sobre Protección de Datos Personales; LDE = Ley de Delitos Económicos. LDI = Ley sobre Delitos Informáticos; LMC = Ley Marco de Ciberseguridad; Subtel = Subsecretaría de Telecomunicaciones del Ministerio de Transportes y Telecomunicaciones; SERNAC = Servicio Nacional del Consumidor.

3 Este artículo también puede ser de utilidad para quienes se dedican a la protección de datos personales o están interesados en trabajar en este campo.

4 Ver proyecto de ley, aprobado por el Congreso, boletín Nº 11.144-07, Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (refundido con el boletín 11.092-07) (2017), 27 agosto 2024, http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07. Las modificaciones que introduce a la Ley Nº 19.628 se encuentran en sus artículo primero.

5 Ver TC, causa Rol Nº 15733-24-CPR, sobre Control de constitucionalidad del proyecto que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, correspondiente a los Boletines N°s 11.092-07 y 11.144-07, refundidos. El Tribunal Constitucional está revisando el proyecto en el marco de su control preventivo obligatorio respecto de leyes que contienen materias propias de ley orgánica constitucional. Si bien el TC siempre puede sorprender, en este artículo asumimos que el TC aprobará el proyecto y que éste se convertirá en ley de la República poco tiempo después de la publicación de este artículo. Con todo, la sentencia del TC podría eliminar algunas normas del proyecto que son descritas en este artículo.

6 Ver disposiciones transitorias, art. primero, del proyecto de ley, aprobado por el Congreso, boletín Nº 11.144-07, Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (refundido con el boletín 11.092-07) (2017), 27 agosto 2024, http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07.

7 A menos que se indique lo contrario, todas las referencias a disposiciones se refieren a las de la LPDP.

8 Para un argumento a favor de una separación conceptual entre la noción de protección de datos personales del derecho continental y chileno, y la noción de *privacy* del derecho norteamericano, ver Lorena Donoso Abarca y Carlos Reusser Monsálvez, *La protección de los datos personales en Chile* (Santiago: Der ediciones, 2022), 3-15. En la práctica, la literatura y las regulaciones sobre "data privacy", "information privacy" y en general "privacy" del derecho norteamericano abordan materias y persigue propósitos muy similares y a menudo equivalentes al derecho europeo y chileno sobre protección de datos personales. Los abogados chilenos y europeos de este campo frecuentemente prestan atención a los desarrollos del "privacy law" norteamericano, mientras los abogados norteamericanos hacen lo mismo en relación con el derecho europeo sobre protección de datos personales. Aquí no tomamos posición sobre este debate conceptual, aunque usamos las expresiones "protección de datos personales", "privacidad" y otras similares como sinónimos.

nuevas reglas de conducta que introduce en el sistema jurídico chileno.[9] Además, la LPDP crea la Agencia de Protección de Datos Personales (en adelante "la Agencia"), el primer órgano del Estado de Chile dedicado exclusivamente a la protección de datos personales.[10]

La dictación de la LPDP ocurre en el contexto de una creciente digitalización de la economía y la sociedad en general. Esta transformación social está marcada por la masificación del acceso de las personas a internet y a otras tecnologías digitales, por la vigilancia y el uso masivo de datos personales como un elemento central del modelo de negocios de un número creciente de empresas y también de las acciones del Estado, y por el auge de la inteligencia artificial, una tecnología cuyo desarrollo e implementación utiliza grandes bases de datos, incluyendo las de datos personales.[11]

Con el fin de facilitar el estudio de la LPDP, especialmente por parte de profesionales de libre competencia, abordaremos las siguientes preguntas:

Primero, ¿cuál es la potencial relevancia de la LPDP para el derecho de la libre competencia? En otras palabras, ¿en qué medida las autoridades de competencia y otros operadores utilizarán (o no) la LPDP en sus decisiones?[12]

Segundo, ¿en qué consiste LPDP? ¿Cuáles son los fines que el legislador intentó alcanzar mediante su dictación? ¿Cuáles son sus reglas de comportamiento? ¿Cómo la LPDP regula su *enforcement* y encaminadas el cumplimiento de esta ley, incluyendo su Agencia?

Tercero, ¿cómo se relaciona la LPDP con otras regulaciones sobre tratamiento de datos personales que afectan o pueden afectar a los responsables?

Para abordar estas preguntas, este trabajo se organiza en cinco partes.

La parte I –"Relevancia de la LPDP para el derecho de la libre competencia"– explica por qué es conveniente que los profesionales de competencia se familiaricen con esta ley y, en particular, por qué es probable que las autoridades de competencia invoquen la LPDP en sus decisiones. En primer lugar, este tipo de incorporación

9 La Ley Nº 19.628 de 1999 fue la primera ley chilena que buscó regular explícitamente el tratamiento de datos personales de manera general y comprehensiva. Se trataba de una ley relativamente breve –24 artículos– que establecía deberes de conducta para quienes trataban datos personales, derechos de los titulares, y acciones civiles para perseguir la responsabilidad de los infractores de la ley ante los tribunales de justicia. Al mismo tiempo, ella carecía de un órgano administrativo a cargo de fiscalizar su cumplimiento.

10 Con todo, esta dedicación exclusiva de la Agencia podría desaparecer si se aprueba un proyecto de ley sobre inteligencia artificial que la haría competente para regular tanto la protección de los datos personales como los sistemas de inteligencia artificial. Ver abajo sección IV.C.1.4.

11 Ver, entre otros, Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019); Laura DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch* (New Haven: Yale University Press, 2020); Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (New York: W. W. Norton & Company, 2022); Neil Richards, *Why Privacy Matters* (New York: Oxford University Press, 2022); Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (New York: Oxford University Press, 2019); Daniel J. Solove, "Artificial Intelligence and Privacy", *77 Florida Law Review (forthcoming)*, 2024; Nita A. Farahany, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (New York: St. Martin's Press, 2023).

12 Dejamos para otra ocasión el análisis de la pregunta inversa sobre la interacción entre libre competencia y protección de datos: en qué medida el derecho de la libre competencia es relevante para la LPDP y sus operadores. Para un análisis de esta pregunta en el derecho comparado, ver Carolina Abate, Giuseppe Bianco, y Francesca Casalini, "The Intersection between Competition and Data Privacy: A Joint Working Paper from the OECD Competition and Digital Economy Policy Secretariat", OECD Roundtables on Competition Policy Papers, 2024, 16–19, https://www.oecd-ilibrary.org/finance-and-investment/the-intersection-between-competition-and-data-privacy_0dd065a3-en.

de la regulación sobre datos personales en la libre competencia ya ha empezado a ocurrir en el derecho comparado y, en menor medida, en Chile. Identificaremos tres modos de incorporación de la regulación de datos personales en el derecho de la libre competencia: (a) la protección de los datos personales como un elemento de la calidad de productos y servicios que es afectada por las conductas anticompetitivas; (b) la desprotección de datos personales como un abuso de posición dominante; y, (c) la protección de datos personales como una exigencia jurídica en tensión o conflicto con el derecho de la libre competencia (y potencial defensa frente a acusaciones de ilícitos de libre competencia). Para ejemplificar estos tres modos haremos referencia a sentencias extranjeras y al informe de la Fiscalía Nacional Económica (en adelante "la Fiscalía" o "FNE") en el caso *Uber-Cornershop* del año 2020.

A continuación, sugeriremos que la utilización de uno o más modos de incorporación de la protección de datos personales en el derecho de la libre competencia sea catalizada, en Chile, por la dictación y entrada en vigencia de la LPDP. Esto puede suceder por varias razones. Primero, porque es probable que, motivados por la fiscalización de la Agencia y por consumidores concientizados sobre sus derechos, los responsables, mejoren sus estándares de protección de datos personales. Y, por lo tanto, que sea más frecuente que ellos compitan "en privacidad". Segundo, porque la LPDP puede clarificar el significado de la protección de datos, creando mayor certeza jurídica para los operadores del derecho de la libre competencia. Tercero, porque la misma LPDP y otras leyes contemplan procedimientos de colaboración entre los órganos públicos, procedimientos que pueden encausar y facilitar la colaboración entre la Agencia y las autoridades de competencia.

Por estas razones, la parte I concluye que es posible y tal vez probable que las autoridades de libre competencia chilenas invoquen la LPDP en algunas de sus decisiones; y, por lo tanto, que es importante que los profesionales de libre competencia se familiaricen con esta ley.

Para facilitar esa tarea, las partes II a IV de este trabajo resumen los contenidos de la LPDP. La parte II –"Fines de la LPDP e implicancias para su interpretación"– describe el "espíritu" de esta ley, es decir, los fines públicos articulados por los legisladores que lideraron la tramitación de esta ley, tal como consta en la historia fidedigna de su establecimiento. Estos fines se pueden resumir en dos. Primero, el legislador buscó promover y respetar el derecho constitucional a la protección de los datos personales consagrado en el artículo 19 Nº 4 de la Constitución. Segundo, el legislador intentó ajustar la regulación chilena a su par de la Unión Europea –la regulación del Reglamento General de Protección de Datos de la Unión Europea del 2016 (en adelante "GDPR", por sus siglas en inglés)– para que la Unión Europea declare que Chile es un "país adecuado" y, así, se facilite la transferencia internacional de datos personales.[13] Este último fin explica por qué la LPDP tiene muchas reglas que son similares al GDPR. Y tal como explicaremos, es probable que el GDPR y las interpretaciones que ha recibido de parte de autoridades europeas jueguen un rol muy importante en la interpretación de la ley chilena.

La parte III –"Reglas de conducta de la LPDP"– resume las reglas de comportamiento dispuestas en esta ley. Empieza por describir el ámbito de la LPDP. Éste es el tratamiento de datos personales relativo a personas naturales ("titulares") que residen en Chile, realizado por todo tipo de responsables, y el tratamiento de datos

13 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 (Reglamento general de protección de datos) (Texto pertinente a efectos del EEE), 119 OJ L § (2016), http://data.europa.eu/eli/reg/2016/679/oj/spa. Esta regulación entró en vigencia en el año 2018. Su título en inglés es *General Data Protection Regulation*. En tanto "reglamento" (*regulation*) de la UE, sus reglas son directamente aplicables en los estados miembros de la UE; estos tienen la obligación de aplicar el GDPR tal como si fuera una ley doméstica.

personales de titulares que residen en el extranjero realizado por responsables establecidos en Chile. En ambos casos, el concepto de "responsable" es aplicable a personas naturales y jurídicas, privadas o públicas, en la medida que decidan "acerca de los fines y medios del tratamiento de datos personales" (art. 2 letra n).

Por regla general, la LPDP solamente permite el tratamiento de datos cuando el responsable puede justificarlo apelando a alguna de las condiciones contempladas por la ley y conocidas como "fuentes de licitud". Por ejemplo, el consentimiento previo del titular. Pero eso no es todo. El responsable también debe realizar el tratamiento cumpliendo con condiciones adicionales, tal como la implementación de medidas de seguridad para evitar que terceros accedan a los datos. Asimismo, los responsables deben recibir y, cuando corresponda, acoger pretensiones de los titulares respecto de sus datos, las cuales están plasmadas en los llamados "derechos del titular", como los de acceso, rectificación, supresión y oposición (los así llamados "derechos ARCO") y otros derechos reconocidos por la LPDP (por ejemplo, el derecho a la portabilidad de datos).

La parte IV –"Enforcement y otras instituciones de cumplimiento de la LPDP"– resume los arreglos institucionales contemplados por esta ley para facilitar e incentivar el cumplimiento de sus reglas de conducta: (a) programas de *compliance*, (b) ejercicio de derechos por parte de los titulares y ante el responsable (y, eventualmente, ante la Agencia), (c) la fiscalización realizada por la Agencia y las sanciones que puede imponer, y (d) indemnizaciones civiles impuestas por tribunales en procesos judiciales.

La parte V –"Otras regulaciones sobre datos personales y su relación con la LPDP"– sitúa esta ley en el sistema chileno de protección de datos personales. La LPDP es parte de un cúmulo de regulaciones y órganos con competencias sobre los datos personales. Este cúmulo incluye disposiciones constitucionales y la jurisprudencia de los tribunales en el contexto de la acción constitucional de protección, varias regulaciones y órganos "sectoriales", y la regulación general de la seguridad informática, entre otras. Sin ánimo de exhaustividad, entregaremos ejemplos de estas regulaciones. También abordaremos cómo la LPDP regula, con alcance general, las interacciones entre la Agencia y los órganos sectoriales.

El alcance de este paper es limitado en al menos tres sentidos. Primero, porque ofrecemos una introducción a la LPDP y no un resumen comprehensivo de sus contenidos. La LPDP es una ley larga y compleja, que se relaciona con muchas otras regulaciones. No es posible hacer justicia a todo lo anterior en los confines de este artículo. Nuestro objetivo es más modesto: ofrecer una puerta de entrada a la LPDP.

Segundo, porque nos enfocaremos en las reglas generales de la LPDP que aplican a las empresas y organizaciones privadas, soslayando las reglas especiales de la LPDP sobre el tratamiento realizado por los órganos del Estado.[14] Estas reglas especiales tienen una relevancia limitada para el derecho de la libre competencia y su eventual intersección con la LPDP.[15] Por esta razón, y una de espacio, aquí no resumimos la regulación especial del Estado, pese a que hacerlo sería necesario si nuestro objetivo fuera explicar la LPDP de manera comprehensiva.

14 Los Títulos IV (arts. 20-26) y VIII (arts. 54-55) de la LPDP contienen reglas especiales sobre el tratamiento de datos personales realizado por el Estado. En breve, la LPDP establece que los órganos del Estado están autorizados para tratar datos personales si el tratamiento es necesario para el cumplimiento de sus funciones legales y se realiza dentro del ámbito de sus competencias, sin que se necesite en estos casos el consentimiento del titular (arts. 20 y 54). La LPDP también establece deberes adicionales para el tratamiento realizado por las las autoridades públicas, y procedimientos para hacer cumplir sus reglas de conducta (arts. 20-26, 44-46, y 54-55).

15 Para los profesionales de la libre competencia puede ser interesante consultar la regulación de los órganos de la Administración del Estado (arts. 20-26) y los tribunales especiales (arts. 54-55), en la medida que aplican a la Fiscalía Nacional Económica y el Tribunal de Defensa de la Libre Competencia, respectivamente.

Finalmente, como es obvio, este trabajo ha sido preparado antes de que la LPDP entre en vigencia y empiece a ser implementada –y, en estricto rigor, antes de que el proyecto de ley haya pasado el examen del TC y se haya convertido en ley–. Aquí es imposible considerar la práctica regulatoria e interpretativa de la Agencia que será creada por la LPDP (o de otros órganos o agentes que implementen esta ley). El foco de este trabajo, para bien o para mal, estará en el texto de la LPDP.

I. RELEVANCIA DE LA LPDP PARA EL DERECHO DE LA LIBRE COMPETENCIA

En esta parte sugerimos que la LPDP será relevante para el derecho de la libre competencia chileno porque es posible que sus definiciones, categorías, y el cumplimiento de sus reglas (o infracción de las mismas) sean tomadas en cuenta por algunas decisiones de las autoridades de competencia chilenas.

Defenderemos esta tesis sobre la relevancia de la LPDP para el derecho de la libre competencia en tres pasos. Primero, revisaremos varios modos de incorporación de la protección de datos que ya se observan en el derecho comparado de la libre competencia (sección I.A). Segundo, resumiremos un caso chileno en el cual la Fiscalía Nacional Económica invocó la regulación sobre protección de datos personales (sección I.B). Tercero, explicaremos porqué la LPDP, específicamente, tiene el potencial de catalizar en Chile la incorporación de la regulación sobre protección de datos personales en el derecho de la libre competencia (sección I.C).

A. Modos de incorporación de la regulación sobre protección de datos personales en el derecho comparado de la libre competencia

En los últimos años, autoridades de competencia extranjeras ya han invocado regulaciones sobre protección de datos personales con el objeto de determinar la eventual o real infracción de la libre competencia. Las autoridades de competencia han desarrollado una serie de modos de incorporación de la regulación sobre datos personales en el derecho de la libre competencia, tal como lo muestra una amplia literatura nacional[16] y e internacional[17]. A partir de esta literatura y el estudio de casos, a continuación resumimos cómo se ha justificado esa incorporación y tres modos específicos.[18]

16 Ver Javiera Sepúlveda A., "Convergencia de la protección de datos y la libre competencia en la economía digital", *Investigaciones CeCo*, agosto de 2023, https://centrocompetencia.com/wp-content/uploads/2023/08/Convergencia-de-la-proteccion-de-datos-y-la-libre-competencia-en-la-economia-digital.pdf; Sebastián Cañas, "Explotación de datos personales como precio excesivo: Una revisión del caso Bundeskartellamt c. Facebook", *Investigaciones CeCo*, octubre de 2023, https://centrocompetencia.com/wp-content/uploads/2023/10/Explotacion-de-datos-personales-como-precio-excesivo-una-revision-del-caso-Bundeskartellamt-c-Facebook-Canas-Sebastian.pdf; Sebastián Cañas, "El tortuoso romance entre datos y competencia: la mirada de la Corte Europea", *Centro Competencia (CeCo)* (blog), 12 de julio de 2023, https://centrocompetencia.com/el-tortuoso-romance-entre-datos-y-competencia-la-mirada-de-la-corte-europea/; Andrés Calderón, "Competencia y datos personales: Una innecesaria atadura en la reciente sentencia del TJUE en el caso 'Facebook'", *CentroCompetencia (CeCo)* (blog), 25 de julio de 2023, https://centrocompetencia.com/competencia-datos-personales-innecesaria-atadura-reciente-sentencia-tjue-caso-facebook/; Bruno Nocera Q., "Extracción de datos de usuarios como conducta exclusoria, según Calderón y Malca", *CentroCompetencia (CeCo)* (blog), 29 de noviembre de 2023, https://centrocompetencia.com/extraccion-de-datos-de-usuarios-como-conducta-exclusoria-segun-calderon-y-vilchez/. Para discusiones sobre la relación entre competencia y *big data* en general, ver María Francisca Labbé Labbé Figueroa, "Big Data: Nuevos desafíos en materia de libre competencia", *Revista Chilena de Derecho y Tecnología* 9, nº 1 (2020): 33–62; Catalina Frigerio, "Mecanismos de regulación de datos personales: una mirada desde el análisis económico del derecho", *Revista Chilena de Derecho y Tecnología* 7, nº 2 (31 de diciembre de 2018): 45–80; María Francisca Labbé Figueroa, "Soluciones para la colusión por algoritmos de fijación de precios", *Revista chilena de derecho y tecnología* 12 (2023).

17 Ver, entre otros, Erika Douglas, "Digital Crossroads: The Intersection of Competition Law and Data Privacy", *Temple University Legal Studies Research Paper No. 2021-40*, 2021; Erika M Douglas, "The New Antitrust/Data Privacy Law Interface", 2021; Maurice E. Stucke, "The Relationship Between Privacy and Antitrust", *Notre Dame L. Rev. Reflection* 97 (2022): 400; Andres Calderon y Piero Malca, "Maybe Excessive, Definitively Exclusionary: A Different Approach to the Anticompetitive Collection and Processing of Data.", *Virginia Journal of Law & Technology* 27, nº 3 (2023): 1–29; Abate, Bianco, y Casalini, "The Intersection between Competition and Data Privacy: A Joint Working Paper from the OECD Competition and Digital Economy Policy Secretariat".

18 Nuestra discusión se enfoca en la incorporación de la regulación de datos personales en el derecho de la libre competencia –es decir, por parte de las autoridades de la libre competencia y agentes que presentan posiciones jurídicas a estas–, y respecto de los sujetos pasivos a los cuales este derecho aplica. Distinguimos esta materia de la pregunta sobre los efectos de la regulación de datos personales sobre la competencia a secas. Respecto a esta otra pregunta, existe literatura que sugiere que la adopción de regulaciones robustas como el

1. La privacidad como calidad y el bienestar del consumidor

El argumento más frecuente a favor de la incorporación de la protección de datos personales en el derecho de la libre competencia es la idea de la "privacidad como calidad" ("*privacy-as-quality theory*").[19]

Esta teoría vincula los datos personales con la libre competencia por medio del concepto del "bienestar del consumidor" (*consumer welfare)*. Como ha explicado Ariel Ezrachi, la noción del bienestar del consumidor consiste en el objetivo de maximizar "los beneficios que los consumidores obtienen de consumir bienes y servicios en un ambiente competitivo. El derecho de la competencia nos garantiza que recibamos más de nuestros mercados: que recibamos mejores productos y servicios a precios más bajos".[20] El bienestar del consumidor es el objetivo principal de esta área del derecho según su paradigma predominante. [21]

En ese orden, la teoría que examinamos enfatiza que el objetivo del bienestar del consumidor se expresa tanto en precios de productos y servicios como la *calidad* de los mismos. Y, a continuación, agrega que la calidad es un concepto suficientemente amplio como para que incluya la protección de los datos personales o privacidad. Esta idea ha sido invocada repetidamente por las autoridades de competencia que han apelado a la regulación sobre protección de datos para examinar ilícitos anticompetitivos.

Desde la perspectiva de la teoría de la privacidad como calidad, resulta importante considerar si una operación de concentración podría disminuir la competencia en privacidad, causando así la degradación de servicios o productos en esta dimensión y, por lo tanto, del bienestar del consumidor. Si esto es así, las autoridades deberían imponer condiciones a estas operaciones de concentración o incluso rechazarlas. Esta relación entre competencia y privacidad como calidad ha sido explicada de la siguiente manera por la profesora Erika Douglas:

> Los consumidores pueden preferir un producto sobre otro en función de la competitividad de los diferentes atributos de privacidad que ofrece cada producto. Cuando los productos de

GDPR (y, posiblemente, nuestra LPDP) puede generar concentración en mercados digitales. Ver discusión y trabajos citados en Calderon y Malca, "Maybe Excessive, Definitively Exclusionary: A Different Approach to the Anticompetitive Collection and Processing of Data.", 11–12 y notas 46-52. Con todo, esta hipótesis es indirectamente relevante para nuestra discusión, en la medida que puede esgrimirse como una razón contra la incorporación de la protección de datos en la libre competencia (ver abajo nota 20 y su texto principal). También puede ser relevante para un modo de incorporación potencial que discutimos abajo en la nota 43. De manera similar, otra dimensión de la intersección entre protección de datos y libre competencia que omitimos abordar aquí se refiere a la FNE como potencial infractor de la LPDP. Esta última cuestión ha sido objeto de atención pública recientemente. Tres universidades interpusieron acciones constitucionales de protección en contra de la FNE por el requerimiento de información de datos personales de sus alumnos. Sobre este caso, ver Ignacio Peralta Fierro, "Tres piedras en el zapato de la FNE: la oposición de PUC, USACH y la Chile a entregar información en un Estudio de Mercado", *CeCo* (blog), 31 de julio de 2024, https://centrocompetencia.com/tres-piedras-en-el-zapato-de-la-fne-la-oposicion-de-puc-usach-y-la-chile-a-entregar-informacion-en-un-estudio-de-mercado/. Ver también normas mencionadas arriba en nota 15.

19 Ver Douglas, "Digital Crossroads", 62–67; Douglas, "The New Antitrust/Data Privacy Law Interface", 654; Stucke, "The Relationship Between Privacy and Antitrust", 7–11; Maureen K. Ohlhausen y Alexander P. Okuliar, "Competition, consumer protection, and the right [approach] to privacy", *Antitrust LJ* 80 (2015): 121.

20 Ariel Ezrachi, *Competition and Antitrust Law: A Very Short Introduction* (New York: Oxford University Press, 2021), 28–29. Traducción de los autores.

21 El estándar de bienestar del consumidor –y su contenido– ha sido ampliamente discutido en la literatura académica. A modo de ejemplo, ver las siguientes notas de CeCo: Bruno Nocera Q., "OCDE: Bienestar del consumidor y estándares distintos", CentroCompetencia, 2 de agosto de 2023, https://centrocompetencia.com/ocde-bienestar-del-consumidor-y-estandares-alternativos/; María Alejandra Ramos, "Una revisión al estándar de bienestar del consumidor (según Glick, Lozada y Bush)", CentroCompetencia, 13 de diciembre de 2023, https://centrocompetencia.com/una-revision-critica-e-historica-al-estandar-de-bienestar-del-consumidor-segun-glick-lozada-y-bush/; Tim Wu, "Después del bienestar del consumidor, ¿qué sigue? El estándar de la 'protección de la competencia' en la práctica", CentroCompetencia, 19 de junio de 2024, https://centrocompetencia.com/bienestar-consumidor-estandar-proteccion-competencia-competencia/. Para una influyente crítica a una noción restringida del estándar de bienestar del consumidor (reducido a precios más bajos y más producción), de autoría de la actual presidenta de la Federal Trade Commission de los Estados Unidos, ver Lina M. Khan, "Amazon's Antitrust Paradox", *Yale Law Journal* 126 (2017): 710-805 ("[t]he current framework in antitrust fails to register certain forms of anticompetitive harm (...) consumer interests include not only cost but also product quality, variety, and innovation", *ibid*. 737).

> las partes que se fusionan compiten en función de características de privacidad, las agencias antimonopolio considerarán los efectos de la fusión en dicha competencia basada en la privacidad. Si la fusión propuesta reduciría la competencia basada en la privacidad en un mercado relevante, ese impacto se considerará dentro del análisis antimonopolio general acerca de si es probable que la fusión reduzca sustancialmente la competencia.[22]

Por ejemplo, en el año 2017 la Comisión Europea examinó la adquisición por parte de Microsoft de la red social para profesionales LinkedIn. El órgano europeo afirmó que la adquisición le permitiría a Microsoft excluir a competidores en el mercado de redes sociales profesionales, y que ello limitaría las opciones de los consumidores en términos de las condiciones de privacidad. En consecuencia, la Comisión le impuso a Microsoft varias condiciones para aprobar la operación.[23]

La Comisión Europea no es el único órgano extranjero que ha adoptado la idea de privacidad como calidad. Como también ha explicado la profesora Douglas,

> Esta concepción de la privacidad como calidad ha recibido más reconocimiento de las agencias antimonopolio que cualquier otra teoría. Los discursos de las agencias, las presentaciones y las orientaciones propuestas en varias jurisdicciones han reconocido que la competencia puede basarse en la protección de datos o la privacidad como un elemento de la calidad de un producto o servicio. Algunas jurisdicciones han aplicado esta teoría en las revisiones de fusiones y, más recientemente, en casos de abuso de posición dominante. Esta visión es la más cercana al pensamiento de consenso, o al menos el paradigma más ampliamente referenciado, en esta intersección de la ley antimonopolio y la privacidad de datos.[24]

Sin embargo, el alcance y validez de la teoría no es claro. Una premisa general de esta modalidad de incorporación de la privacidad en el derecho de la libre competencia es que mientras menos concentrado esté el mercado (mientras más competitivo sea) mejores serán los estándares de privacidad ofrecidos por las empresas. Sin embargo, la validez de esta premisa es debatible. La premisa no opera bien si el estándar de protección de datos personales es un aspecto no reconocible para el consumidor, es decir, que no incide en su decisión de compra o demanda de un servicio. La literatura a menudo reconoce una "paradoja de la privacidad", según la cual si bien los consumidores dicen (por ejemplo, en encuestas) que valoran su privacidad, en los hechos demandan servicios que vulneran su privacidad. Si esto es así, se podría afirmar que la privacidad no puede ser protegida por el derecho de la libre competencia (sin perjuicio de que sí sea abordada por la regulación de la protección de datos y su autoridad de control).[25] Con todo, esta crítica pierde fuerza si la "paradoja de la privacidad" en realidad no existe o tiene un alcance muy limitado, un punto que ha sido defendido con fuerza por académicos de la protección de datos personales como Daniel Solove.[26]

---

22 Douglas, "Digital Crossroads", 83. Traducción de los autores. Ver también OECD, "The Intersection between Competition and Data Privacy", *OECD Roundtables on Competition Policy Papers* 310 (2024).

23 European Commission, Competition Merger Brief M.8124, Microsoft/LinkedIn: Big Data and Conglomerate Effects in Tech Markets 5 (May 2017), https://ec.europa.eu/competition/publications/cmb/2017/kdal17001enn.pdf, citado y resumido en Douglas, "Digital Crossroads", 85–88.

24 Douglas, "Digital Crossroads", 63-64. Traducción de los autores.

25 Ver Jörg Hoffmann y Omar Vásquez Duque, "Can Data Exploitation Be Properly Addressed by Competition Law? A Note of Caution", *Concurrences* 1–2021 (febrero de 2021): 75–82.

26 Ver Daniel J. Solove, "The Myth of the Privacy Paradox", *The George Washington Law Review* 89 (2020): 1–51.

Otra razón por la cual la teoría de la privacidad como calidad es discutible se relaciona con la premisa de que mayor competencia implica mayor protección de datos personales. Esta premisa puede tener excepciones, dependiendo de la dinámica de los mercados. Por ejemplo, algunos autores han planteado que la mayor concentración en mercados de plataformas online puede generar más privacidad. Esta concentración haría menos probable que esas plataformas compartan datos personales de sus usuarios con data brokers. Asimismo, la concentración de esas plataformas y de los data brokers estaría asociado a un menor riesgo de incidentes de seguridad que afecten a los datos personales.[27]

Desde otra perspectiva crítica, algunos autores han argumentado que la protección de los datos personales no necesariamente promueve el bienestar del consumidor. Por ejemplo, se ha dicho que la regulación sobre protección de datos personales no cumple con ese objetivo porque esta regulación reforzaría la posición de las grandes empresas como Google. Estas empresas podrían "absorber mejor que las pequeñas empresas los costos de implementación y lidiar [de mejor manera] con las restricciones legales relativas a la recopilación y el procesamiento de datos".[28] Parte de la resistencia a la teoría también se puede deber a desacuerdos más generales sobre la noción de "calidad" como un estándar del derecho de la libre competencia y, en particular, respecto de la metodología adecuada para cuantificarla.[29]

Con estas salvedades, la idea de privacidad como calidad está jugando un rol crucial en el derecho de comparado de libre competencia, y provee una modalidad atractiva para explorar si y cuándo este campo puede hacer uso de regulaciones como la LPDP.

2. Abuso de posición dominante de tipo explotativo y protección de datos personales

Un segundo modo de incorporación de la regulación sobre protección datos personales en el derecho de la libre competencia se refiere a empresas que tienen una posición dominante y que, a juicio de las autoridades de competencia, abusan de sus consumidores imponiendo políticas de privacidad de naturaleza explotativa. Este modo de incorporación fue desarrollado recientemente por la autoridad alemana de competencia (la *Bundeskartellamt*) y el Tribunal de Justicia de la Unión Europea ("TJUE") en un caso contra la empresa Facebook (hoy Meta).[30]

La autoridad de competencia alemana determinó que Meta había cometido un abuso de posición dominante de tipo explotativo en el tratamiento de los datos personales de sus consumidores. Como ha explicado el profesor Andrés Calderón, la autoridad alemana sancionó a la empresa por un abuso explotativo de su posición dominante, al recolectar –excesivamente– y combinar datos personales de los usuarios de las

27 Ver Arion Cheong, Tawei Wang, y D. Daniel Sokol, "Cookie Intermediaries: Does Competition Leads to More Privacy?"

28 Calderon y Malca, "Maybe Excessive, Definitively Exclusionary: A Different Approach to the Anticompetitive Collection and Processing of Data.", 12. Traducción de los autores. Ver también *ibid*. pp. 11-13.

29 Mientras el estándar de bienestar del consumidor (al menos en su noción tradicional) se mide en base a rebajas de precio (excedente del consumidor), no existe un consenso técnico sobre cómo medir cuantitativamente la variable calidad. Por ejemplo, alguna doctrina ha propuesto aplicar el test de elasticidad "SSNDQ" ('small but significant non-transitory decrease in product quality"), emulando el test SSNIP (precios), pero no se ha aplicado aún en un caso de competencia. Agradecemos a Juan Pablo Iglesias por esta observación.

30 Tribunal de Justicia de la Unión Europea (Gran Sala), Sentencia asunto C-252/21, Meta Platforms Inc., anteriormente Facebook Inc., Meta Platforms Ireland Ltd, anteriormente Facebook Ireland Ltd, Facebook Deutschland GmbH y Bundeskartellamt, con intervención de: Verbraucherzentrale Bundesverband eV, (4 de julio de 2023) (en adelante "Sentencia TJUE caso Bundeskartellamt con Meta").Meta Platforms Ireland Ltd, anteriormente Facebook Ireland Ltd, Facebook Deutschland GmbH y Bundeskartellamt, con intervenci\\uc0\\u243{}n de: Verbraucherzentrale Bundesverband eV, (4 de julio de 2023

plataformas y dispositivos del grupo Meta (Facebook, Instagram, Whatsapp, Oculus y Masquerade), así como de sitios web y aplicaciones de terceros con los que Facebook tenía una API (interfaz de programación de aplicaciones) que le permitía procesar sus datos. (...)

> Un factor trascendental para la autoridad alemana fue que la forma en que Facebook obtenía el consentimiento para recolectar y usar los datos personales resultaba violatoria del Reglamento General de Protección de Datos Personales de la Unión Europea ("GDPR").
>
> Así, el estándar para concluir que la conducta era explotativa (y un ilícito *antitrust)* fue el incumplimiento de la norma sectorial de protección de datos personales.[31]

Posteriormente, Meta desafió la decisión de la autoridad de competencia ante las cortes alemanas.[32] Una de estas cortes le pidió al TJUE que resolviera varias dudas interpretativas como cuestión previa o "prejudicial", y la TJUE se pronunció sobre ellas en el año 2023.

En su sentencia, el TJUE defendió dos tesis que son importantes para la cuestión de la interacción entre el derecho de la libre competencia y la regulación de la protección de datos personales. Ambas se refieren a la potestad que tienen las autoridades de libre competencia nacionales para aplicar el GDPR vis-à-vis la potestad de las agencias nacionales de protección de datos personales para aplicar, también, el GDPR. [33]

La primera tesis es que el GDPR no prohíbe que una autoridad de competencia interprete y aplique reglas de conducta establecidas por esa misma regulación para determinar si una empresa ha incurrido en un abuso explotativo. En principio, la ley alemana de competencia le permitía a su autoridad invocar otras leyes para determinar si había existido un abuso de posición dominante. La pregunta era si la naturaleza del GDPR –con sus propias agencias especializadas– impedía su aplicación por la autoridad de competencia.
Al respecto, el TJUE afirmó que las potestades establecidas por el GDPR a favor de las agencias de protección de datos personales no son excluyentes de otras potestades que pueda tener la autoridad de competencia para interpretar y aplicar el GDPR.

Para justificar esta tesis, el TJUE notó que el GDPR guarda silencio sobre las potestades de las autoridades de competencia, limitándose a reconocer potestades de las agencias de protección de datos y de otros órganos especializados en esta materia. En otras palabras, el silencio del GDPR respecto a las autoridades de competencia no puede leerse como una prohibición de estas autoridades interpreten y apliquen el GDPR.

Además, el TJUE señaló que la noción de abuso de posición dominante –propia del derecho de competencia– puede ser aplicable a comportamientos regulados y prohibidos por el GDPR. Más específicamente, la desprotección de los datos personales, al menos en la economía digital, puede ser un "indicio" de que una empresa ha cometido un abuso de posición dominante:

31 Calderón, "Competencia y datos personales: Una innecesaria atadura en la reciente sentencia del TJUE en el caso 'Facebook'".
32 Para un resumen del proceso ante las cortes de Alemania, ver Tribunal de Justicia de la Unión Europea (Gran Sala), Sentencia asunto C-252/21, Meta Platforms Inc., anteriormente Facebook Inc., Meta Platforms Ireland Ltd, anteriormente Facebook Ireland Ltd, Facebook Deutschland GmbH y Bundeskartellamt, con intervención de: Verbraucherzentrale Bundesverband eV, cc. 29-35.Meta Platforms Ireland Ltd, anteriormente Facebook Ireland Ltd, Facebook Deutschland GmbH y Bundeskartellamt, con intervenci\\uc0\\u243{}n de: Verbraucherzentrale Bundesverband eV, cc. 29-35.","plainCitation":"Tribunal de Justicia de la Unión Europea (Gran Sala
33 El TJUE también abordó preguntas sobre el significado de las reglas de conducta de la GDPR. Específicamente, sobre las "bases de licitud" del tratamiento de datos personales que se encuentran en sus arts. 6(1), 9(1) y 9(2). Ver *ibid*., c. 34 (dudas ii, iii y iv) y c. 35 (preguntas 2 a 6).

> el acceso a los datos personales y la posibilidad del tratamiento de estos se han convertido en un parámetro significativo de la competencia entre empresas de la economía digital. Por lo tanto, excluir las normas en materia de protección de datos personales del marco jurídico que las autoridades de defensa de la competencia deben tomar en consideración al examinar un abuso de posición dominante ignoraría la realidad de esta evolución económica y podría menoscabar la efectividad del Derecho de la competencia en el seno de la Unión.[34]
>
> [L]a conformidad o no conformidad de (...) [las] actividades [de las empresas con posición dominante] con las disposiciones del GDPR puede constituir, en su caso, un indicio relevante, entre las circunstancias pertinentes del caso concreto, para determinar si dichas actividades constituyen medios que rigen una competencia normal y para evaluar las consecuencias de una determinada práctica en el mercado o para los consumidores. [35]

Por lo tanto, las autoridades de competencia podían aplicar la GDPR para determinar si una conducta atentaba el derecho de la libre competencia.

A continuación el TJUE evaluó qué grados de deferencia le debía la autoridad de competencia alemana a las autoridades de protección de datos personales cuando la primera aplicaba la GDPR. Respecto a esta pregunta, el TJUE invocó, interpretó y aplicó el "principio de cooperación leal" del Tratado de la Unión Europea.[36] Según la interpretación del TJUE, el principio establece que las autoridades administrativas de los Estados miembros "deben respetarse y asistirse mutuamente en el cumplimiento de las misiones derivadas de los Tratados".[37] El TJUE afirmó que en casos como el de *Bundeskartellamt* v. Facebook –en los cuales la autoridad de competencia evalúa la legalidad de la conducta de una empresa desde la perspectiva de la regulación de datos personales– el principio de cooperación leal tenía dos implicancias.

Primero, la autoridad de competencia debía adoptar el criterio de una autoridad de protección de datos si ésta ya se había pronunciado sobre la legalidad del tratamiento de datos personales en cuestión.[38]

Segundo, la autoridad de competencia debía "consultar" y "solicitar la cooperación" de la autoridad de protección de datos (a) cuando la autoridad de competencia tiene dudas sobre el alcance de una decisión tomada por la autoridad de protección de datos respecto del tratamiento en cuestión o de uno similar, o (b) cuando la autoridad de datos no ha tomado una decisión o no ha investigado la conducta y según la autoridad de competencia ésta infringe la regulación de protección de datos personales.[39] En estos casos, la autoridad de competencia debe consultar, y la consulta buscará resolver dudas, o determinar si es necesario una decisión previa de la autoridad de protección de datos. Si la autoridad de protección de datos personales no pone objeción a la posición de la autoridad de competencia, u omite responder "en un plazo razonable", la de competencia puede continuar con su investigación. [40]

34 *Ibid.*, c.51.
35 *Ibid.*, c.47.
36 Ver art. 4(3) Tratado de la Unión Europea, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A12016ME%2FTXT.
37 Tribunal de Justicia de la Unión Europea (Gran Sala), Sentencia asunto C-252/21, Meta Platforms Inc., anteriormente Facebook Inc., Meta Platforms Ireland Ltd, anteriormente Facebook Ireland Ltd, Facebook Deutschland GmbH y Bundeskartellamt, con intervención de: Verbraucherzentrale Bundesverband eV, c.53.
38 *Ibid.*, c.63
39 *Ibid*.
40 *Ibid.* El TJUE no explicó porqué el principio de coordinación justifica esa deferencia y no, a la inversa, que la autoridad de datos personales le deba deferencia a los juicios de la autoridad de competencia. Pero es probable que el tribunal haya considerado que las autoridades de datos personales tienden a tener mayor experticia en materia de protección de datos personales. Tal como lo dijo el mismo TJUE, bajo el GDPR "la función principal de la autoridad de control es (...) controlar la aplicación" de dicha regulación. *Ibid.*, c.45.

En resumen, tras la sentencia del TJUE, el derecho de la Unión Europea reconoce que las autoridades de competencia tienen potestad para aplicar el GDPR con el fin de evaluar si una empresa ha cometido un ilícito de competencia de abuso de posición dominante. Pero con una condición: las autoridades de competencia le deben una cierta deferencia a las de protección de datos.[41] Y, en ese contexto, la infracción a la regulación sobre protección de datos personales –determinada por la autoridad de competencia con ayuda de la de agencia de datos personales– puede ser un indicio de un abuso de posición dominante.

3. Protección de datos personales como justificación de conductas anticompetitivas

Los modos de incorporación de la regulación sobre protección de datos personales en el derecho de libre competencia que hemos revisado asumen una complementariedad entre la protección de datos personales y la competencia. La competencia tiende a aumentar la protección de datos personales, y cuando se reduce la primera, se reduce también la segunda. Pero la regulación sobre protección de datos también puede ser relevante como una forma de justificar conductas a primera vista contrarias a la libre competencia. Como ha explicado la profesora Erika Douglas,

> [l]as plataformas digitales están invocando la privacidad de los datos para justificar su conducta anticompetitiva. Ante las supuestas violaciones del derecho antimonopolio, los gigantes de las redes sociales, las búsquedas y las aplicaciones móviles están argumentando que se debe sacrificar la competencia en línea para proteger la privacidad de los datos de sus usuarios.[42]

La protección como justificación de conductas anti-competitivas fue aceptada recientemente por tribunales de los EE.UU. en *Epic Games, Inc. v. Apple Inc*.[43] En la sentencia de primera instancia—que fue confirmada en la apelación—una corte de distrito del estado de California determinó

> que las reglas de Apple para su tienda de aplicaciones móviles [la *App Store*] estaban justificadas, porque esas reglas mejoraban la privacidad y seguridad de los datos respecto de los usuarios finales. Esta mejora de la privacidad, a su vez, mejoró la competencia entre Apple y otros sistemas operativos de dispositivos móviles. Habiendo sido establecida esta justificación de privacidad, Apple evitó responsabilidad por infracciones al derecho federal antimonopolio. Esto fue a pesar de que la jueza (…) también concluyó que las reglas de Apple eran prima facie anticompetitivas según la Parte 1 de la Ley Sherman. (…) [E]l caso es significativo: es la primera decisión de los Estados Unidos que acepta la privacidad y seguridad de los datos como justificación pro-competitiva de la conducta de un gigante digital.[44]

41 La sentencia del TJUE ha sido criticada por expertos del derecho de la libre competencia. Como explica Calderon, críticos como Thibault Schrepel "han criticado al Tribunal por no tomar en cuenta la relación causal entre la condición dominante de la empresa y la práctica abusiva imputada". Calderón, "Competencia y datos personales: Una innecesaria atadura en la reciente sentencia del TJUE en el caso 'Facebook'". A su vez, Calderón ha sostenido que "el estándar de la legislación de protección de datos personales es distinto al estándar de bienestar del consumidor que tradicionalmente se aplica en el Derecho de la Competencia". *Ibid*. Ver también Calderon y Malca, "Maybe Excessive, Definitively Exclusionary: A Different Approach to the Anticompetitive Collection and Processing of Data."; Nocera Q., "Extracción de datos de usuarios como conducta exclusoria, según Calderón y Malca". Algunos críticos, explica Sebastián Cañas, "han sostenido que el caso podría haberse resuelto acudiendo a la figura de 'precios excesivos'". Cañas, "Explotación de datos personales como precio excesivo: Una revisión del caso Bundeskartellamt c. Facebook", 5.

42 Erika M. Douglas, "Data Privacy as a Procompetitive Justification: Antitrust Law and Economic Analysis", *Notre Dame L. Rev. Reflection* 97 (2022): 430. Traducción de los autores.

43 Citado en *ibid*., 451.

44 *Ibid*., 431. Traducción de los autores. La sentencia fue confirmada en sede de apelación por la Corte de Apelaciones del Noveno Circuito; más tarde, la Corte Suprema rechazó conocer del caso. Ver Adi Robertson, "Supreme Court Rejects Epic v. Apple Antitrust Case", The Verge, 16 de enero de 2024, https://www.theverge.com/2024/1/16/24039983/supreme-court-epic-apple-antitrust-case-rejected.

El alcance de la privacidad como justificación de conductas a primera vista anti-competitivas no es claro en el derecho de la libre competencia.[45] Pero muestra, una vez más, que en este campo la regulación sobre protección de datos puede jugar un rol importante.[46]

B. La incorporación de la protección de datos personales en el derecho de la libre competencia chileno: la Fiscalía Nacional Económica y la fusión Uber-Cornershop

Chile también ha empezado a incorporar la protección de datos en el derecho de la libre competencia, al menos de manera incipiente. Este criterio fue considerado en la resolución de la Fiscalía que rechazó la adquisición de la plataforma *Cornershop* por parte de Uber en el año 2020.[47] Este es el único caso que conocemos en el cual una autoridad de competencia chilena ha considerado la protección de los datos personales.[48] Por ello, conviene detenerse en *Uber-Cornershop*.

La Fiscalía evaluó una propuesta de operación de adquisición de Cornershop por parte de Uber. Al momento de la propuesta de operación en el año 2020, Uber se podía describir como una empresa norteamericana que "ofrece el servicio de intermediación para el transporte de personas ('Uber Rides')" y "servicios de compra y entrega a domicilio o delivery de comida preparada" ('Uber Eats'). A su vez, Cornershop era una empresa norteamericana, pero de origen chileno, cuya "plataforma digital provee los servicios de compra en línea y entrega a domicilio de bienes, principalmente de supermercados".[49] Uber buscó adquirir Cornershop.

La Fiscalía examinó varios aspectos de la operación. Uno de ellos fue si ésta podía afectar la protección de datos personales de los consumidores finales de Uber y Cornershop, específicamente, a través de una degradación de las políticas de privacidad de sus servicios. Como explicó la autoridad,

> el riesgo analizado se desprendería de la capacidad que tendría la entidad fusionada de condicionar una mayor cantidad de servicios a la aceptación por parte de los usuarios de sus plataformas de una política de privacidad común. En efecto, ante dicho escenario, se

45 Según Douglas, el derecho norteamericano de la libre competencia acepta que las empresas demandadas justifiquen conductas que son *prima facie* anticompetitivas –i.e. que han sido demostradas como tales por el demandante– si y sólo si demuestran que esa protección de la privacidad tiene, a su vez, un efecto pro-competitivo. Ver Douglas, "Data Privacy as a Procompetitive Justification".

46 Más allá de las tres modalidades que hemos explorado, es posible imaginar una adicional, en la cual la autoridad de competencia evalúa los efectos de una operación de concentración teniendo en consideración que el cambio regulatorio en el ámbito de la protección –el paso desde una regulación "leve" a una más robusta– le puede dar una ventaja competitiva a la empresa en cuestión que puede ser difícil de replicar por un competidor, operando como una barrera de entrada artificial. Por ejemplo, imagine que un retailer que también recolectó una significativa base de datos personales bajo la vigencia de la versión original de la Ley 19.628, quiere adquirir otro retailer que recolectó una base de datos personales en ese periodo, y que esta operación ocurre cuando la LPDP ya ha entrado en vigencia. La autoridad de competencia que analiza la operación probablemente tendrá a la vista que será muy difícil para un competidor actual o potencial replicar esa ventaja de datos (nuevos), dado los límites a la recolección impuestos por la LPDP, pudiendo considerar remedios estructurales o conductuales como condición para aprobar la operación. Agradecemos a Juan Pablo Iglesias por esta observación.

47 Ver Fiscalía Nacional Económica, "Informe de Aprobación Adquisición de Cornershop por parte de Uber Technologies, Inc. Rol FNE F217-2019", 29 de mayo de 2020, https://www.fne.gob.cl/wp-content/uploads/2020/06/inap2_F217_2020.pdf.

48 Anteriormente, cuando las autoridades chilenas consideraban el tratamiento de estos datos, lo hacían sin prestar atención a la dimensión de protección o privacidad. Por ejemplo, ver Tribunal de Defensa de la Libre Competencia, "Resolucion Nº 24/2008", 31 de enero de 2008, https://www.fne.gob.cl/wp-content/uploads/2011/03/reso_0024_2008.pdf. En esta resolución el TDLC rechazó una propuesta de fusión de Falabella y D&S. La sentencia sostuvo que la fusión permitiría que la empresa fusionada desarrollara bases de datos sobre los patrones de consumo y endeudamiento de los consumidores finales, y sobre los ingresos de los arrendatarios de los centros comerciales de la empresa (ver cc. 48, 58, 209), y que esta información podría ser usada en modos que perjudicaran la libre competencia y, en definitiva, el bienestar de los consumidores (c. 264). Sin embargo, el tribunal no se refirió expresamente a las bases de datos como bases de "datos personales" (pese a que muy probablemente incluían información de ese tipo), ni consideró si la empresa afectaría la privacidad de datos.

49 Fiscalía Nacional Económica, "Informe de Aprobación Adquisición de Cornershop por parte de Uber Technologies, Inc. Rol FNE F217-2019" cc. 13-14.

> verían reducidas las posibilidades de los consumidores finales de rechazar condiciones que menoscaben su privacidad, lo que no sucedería si se solicitasen autorizaciones independientes para cada uno de ellos.[50]

Este riesgo fue conceptualizado como un "riesgo explotativo" derivado "del aumento de poder de mercado respecto a consumidores finales (en lo que respecta a la política de protección de datos personales)".[51] La Fiscalía justificó esta calificación de la desprotección de datos personales apelando a la idea de *calidad* de productos y servicios: "en este tipo de mercado [(de plataformas digitales)] las políticas de privacidad podrían considerarse atributos relativos a la calidad de los servicios ofrecidos".[52] En esta materia, la Fiscalía seguía "lineamientos de agencias de competencia comparadas en la materia", específicamente de las de Francia y Alemania, así como de la OCDE.[53] Así, citó la decisión de su par alemana en el caso *Bundeskartellamt con Facebook*,[54] que ya hemos discutido arriba.[55]

En consecuencia, la Fiscalía intentó predecir si, tras la operación de compra, se materializaría el riesgo explotativo de degradación de la protección de datos de los consumidores de Uber Eats, Cornershop o ambas empresas. Este análisis predictivo concluyó que era improbable que ello ocurriera.

Primero, la Fiscalía afirmó que Uber Eats y Cornershop, o ambas empresas agrupadas en una, continuarían enfrentando una competencia robusta en los mercados de intermediación y entrega de productos de supermercados y de restaurantes. Esta competencia lograría disciplinar la conducta de la empresa fusionada, haciendo poco atractivo degradar la protección de datos, desde una perspectiva costo-beneficio.

Respecto a los beneficios, la recolección de más datos personales no produciría una ventaja comparativa. Si la entidad fusionada, cambiando sus políticas de privacidad, obtuviera más datos personales de sus usuarios para competir mejor con otras empresas –ofreciendo propuestas más atractivas– estas empresas competidoras también tendrían acceso a los mismos tipos de datos.[56] Respecto a los costos, si la empresa fusionada ofreciera menos protección de datos a sus usuarios se expondría a perderlos, pues éstos podrían contratar los servicios de competidores que ofrecen mejores términos.[57] En conclusión, la competencia disciplinaría la conducta de la entidad fusionada.

Segundo, la Fiscalía argumentó que el riesgo de un abuso explotativo de los consumidores –en la forma de desprotección de datos– era improbable porque la evidencia mostraría que "las políticas de privacidad que aplican las plataformas digitales en los mercados afectados no serían, a la fecha, variables que dependan estrechamente del tamaño de las mismas ni de la cantidad de servicios que provean".[58] En este nivel de análisis, la Fiscalía examinó las políticas de privacidad de los distintos oferentes en el mercado y su relación con las regulaciones chilena y europea de protección de datos.

A la luz de dicho análisis, la Fiscalía observó que dos competidores –Rappi y PedidosYa– "no exhibirían

50 *Ibid.*, c. 275.
51 *Ibid.*, c. 180
52 *Ibid.*, c. 274.
53 *Ibid.*, c. 274. Ver también nota al pie 364.
54 Ver *ibid.*, c. 136 y nota al pie 202.
55 Ver arriba sección I.A.2.
56 *Ibid.*, cc. 276-277.
57 *Ibid.*, c. 278.
58 *Ibid.*, c. 279. Sin embargo, la Fiscalía moderó esta afirmación agregando que "[e]sta situación, no obstante, puede modificarse a futuro y habría que tomarla con precaución". *Ibid.*, nota al pie 373.

diferencias significativas respecto al tratamiento de datos y en general ambas señalan que la información de los usuarios no puede ser comercializada por la plataforma, salvo aceptación expresa de los usuarios, y las transferencias se realizan a empresas vinculadas"[59]. Por otra parte, señaló que Uber "se encuentra regulada por una política de tratamiento de datos que, sin perjuicio de ajustarse a la legislación local, incorpora criterios más estrictos alineados con la legislación europea sobre protección de datos" (es decir, el GDPR).[60] Y, por último, observó que Cornershop "se rige por la legislación chilena que permite un uso más amplio de los datos que obtiene".[61] Aunque sin decirlo expresamente, la Fiscalía pareció sugerir que la adquisición de Cornershop por parte de Uber podría producir que la primera incorpore los criterios "más estrictos" de protección de datos ya adoptados por Uber. Es decir, se produciría una suerte de *overcompliance* desde la perspectiva de la regulación nacional existente al momento de la operación.

Finalmente, la Fiscalía predijo que Cornershop adoptaría criterios más restrictivos porque, en tanto empresa sometida a la legislación chilena, implementaría la futura nueva ley de protección de datos personales que estaba siendo tramitada en el Congreso.[62]

En base a estas razones, la Fiscalía concluyó que "es posible descartar que la presente Operación genere una restricción relevante que signifique un empeoramiento de las políticas de privacidad de los consumidores finales".[63]

Como se puede observar, la Fiscalía implementó la idea de la desprotección de datos personales como un abuso explotativo examinando y comparando políticas de privacidad y, también, las regulaciones de protección de datos que servían de base a esas políticas (el GDPR y la Ley 19.628 en su versión anterior a la LPDP). Es más, esta aproximación fue reconocida abiertamente por la Fiscalía:

> en mercados digitales, existen asimetrías de información y sesgos de comportamiento que podrían ser relevantes y que eventualmente podrían hacer que *las empresas incurrieran en prácticas abusivas respecto a la obtención, tratamiento o uso de los datos personales*. En este sentido, l*as autoridades de protección de datos, de protección de derechos de los consumidores, así como las de libre competencia pueden intervenir ante posibles prácticas que den cuenta de un incumplimiento de las normas recaídas en estas materias* y que las afecten dentro de la esfera de sus correspondientes competencias (énfasis agregado).[64]

Ante ello, cabe preguntarse: ¿cómo este rol de la Fiscalía (o uno similar del TDLC) será afectado por la LPDP? ¿La dictación e implementación de la LPDP hace más o menos probable que las autoridades de competencia chilenas tomen decisiones que tengan en cuenta la regulación sobre protección de datos personales? Sugerimos respuestas a estas preguntas en la próxima parte.

59 *Ibid.*, nota al pie 374.
60 Ibid.
61 Ibid.
62 *Ibid.*, nota al pie 375. Sin embargo, la LPDP recién sería aprobada más de cuatro años después de la decisión de la Fiscalía.
63 *Ibid.*, c. 281.
64 *Ibid.*, nota al pie 375.

C. La LPDP como regulación catalizadora de la incorporación de la protección de datos personales en el derecho de la libre competencia

Las secciones anteriores de esta parte I del artículo han mostrado que el derecho de la libre competencia extranjero y el derecho nacional han empezado a invocar la regulación de protección de datos en sus decisiones. Aquí sostenemos que es probable que esta tendencia sea catalizada por la implementación de la LPDP.

1. La LPDP y el cambio en la cultura de *compliance* y las ofertas de las empresas

La primera razón por la cual la LPDP puede catalizar la incorporación de la protección de datos en el derecho de la libre competencia se relaciona con los cambios que esta ley puede producir en el comportamiento de las empresas y otros responsables.

Con la entrada en vigencia de la LPDP los responsables tendrán nuevos incentivos para mejorar sus prácticas de protección de datos personales. El más obvio es la existencia de la Agencia –un órgano encargado de guiar y fiscalizar el cumplimiento de la ley– y las sanciones que podrá imponer a los infractores. Además, la LPDP contempla varios otros incentivos al cumplimiento de sus reglas de conducta.[65]

Por otra parte, y desde la perspectiva de la demanda, es posible que las creencias y expectativas de los consumidores sean reconfiguradas como consecuencia de la entrada en vigencia de la LPDP[66] y de la actividad fiscalizadora de la Agencia en casos emblemáticos.[67] Por lo tanto, es posible que los consumidores demanden de los responsables una mayor protección de sus datos personales.

Estos efectos de la LPDP pueden contribuir a que más responsables mejoren la protección de datos personales y enfaticen estas prácticas en sus ofertas. Empresas como Apple ya tratan a la privacidad como un aspecto muy importante de los productos y servicios que ofrecen a sus clientes.[68] Otras empresas seguirán este camino, motivadas por los incentivos al cumplimiento de la LPDP y las nuevas expectativas sociales.

Este escenario hace más probable, a su vez, que las autoridades de competencia entiendan a la privacidad como un elemento de la calidad de los productos y servicios, y a su desprotección como una consecuencia negativa de la concentración de mercados y de conductas anti-competitivas. Y si es así, es posible imaginar que la Fiscalía y el TDLC muestren mayor disposición a analizar infracciones potenciales o reales al derecho de la libre competencia considerando las normas de la LPDP y las interpretaciones de las mismas desarrolladas por la Agencia.

65 Ver abajo parte IV de este trabajo.

66 Sobre el efecto "expresivo" de la legislación (o la relación entre ésta y las normas sociales), ver Richard H. McAdams, *The Expressive Powers of Law: Theories and Limits* (Cambridge: Harvard University Press, 2015); Lawrence Lessig, "Social Meaning and Social norms", *University of Pennsylvania Law Review* 144, nº 5 (1996): 2181–89; Lawrence Lessig, "The Regulation of Social Meaning", *The University of Chicago Law Review* 62, nº 3 (1995): 943–1045.

67 Además, el art. 30 bis letra g LPDP le entrega a la Agencia la facultad de "[d]esarrollar programas, proyectos y acciones de difusión, promoción e información a la ciudadanía, en relación al respeto a la protección de sus datos personales".

68 Ver, por ejemplo, Apple, "Acerca de la privacidad y la seguridad de los productos Apple para la educación" (2024), https://support.apple.com/es-cl/102123 ("En Apple, creemos que la privacidad es un derecho humano fundamental. Por ese motivo, todos los productos Apple están diseñados desde cero con el objetivo de proteger la información personal y de darle a cada cliente el poder de elegir qué comparte y con quién").

2. La LPDP y sus instituciones concretizan y aclaran el significado de la protección de datos personales

La LPDP facilitará el trabajo de las autoridades de competencia porque tanto el texto de la Ley, así como la Agencia que crea, clarificarán el significado de la protección de datos, contribuyendo a crear certeza jurídica en este campo.

A diferencia de su antecesora, la LPDP a menudo regula los deberes de los responsables de manera pormenorizada o específica. También entrega definiciones relativamente claras sobre conceptos clave del tratamiento de datos personales. Es más, estas reglas y definiciones han sido actualizadas para que sean coherentes con las características del fenómeno del tratamiento de datos tal como ocurre en la economía digital.

Por supuesto, y como señalamos en otras partes de este artículo, la LPDP también cuenta con varias reglas notoriamente indeterminadas. Pero, y también a diferencia de su antecesora, la LPDP cuenta con la Agencia, un órgano especializado en clarificar el contenido de esas reglas mediante normas generales y resoluciones sobre casos concretos. La actividad reguladora y la casuística de la Agencia contribuirá a aumentar la certeza jurídica en el ámbito de la protección de los datos personales, lo cual debería facilitar, a su vez, la actividad de las autoridades de competencia en esta materia.

Así, el texto de la LPDP y su desarrollo por la Agencia facilitarán el análisis de la Fiscalía y del TDLC cuando necesiten evaluar si las empresas cumplen con un estándar adecuado de protección de datos y, en general, cuando necesiten desarrollar un lenguaje técnico-jurídico sobre esta materia. Por supuesto, es posible que las autoridades de competencia deseen desarrollar criterios propios –distintos a los criterios de la Agencia– sobre la protección de datos personales. Pero incluso cuando lo hagan, es probable que las autoridades competencia trabajen utilizando la categorías o lenguaje de la LPDP, al menos como un punto de partida de su análisis.

3. Mecanismos institucionales para la cooperación entre las autoridades de competencia y la Agencia de Protección de Datos

Las autoridades de competencia chilenas no solamente tendrán acceso al texto de la LPDP y la experticia de la Agencia al igual que cualquier otra persona. También podrán acceder directamente a la opinión de la Agencia respecto de casos particulares, haciendo uso de mecanismos de cooperación y atribuciones contemplados en nuestra legislación.

En efecto, el Decreto Ley 211 contempla mecanismos de colaboración, por cuanto el artículo 39, letra f) establece la atribución del Fiscal Nacional Económico de:

> Solicitar la colaboración de cualquier funcionario de los organismos y servicios públicos, de las municipalidades o de las empresas, entidades o sociedades en que el Estado o sus empresas, entidades o sociedades, o las municipalidades, tengan aporte, representación o participación, *quienes estarán obligados* a prestarla, como asimismo, a proporcionar los antecedentes que obren en sus archivos y que el Fiscal Nacional Económico les requiera, aun cuando dichos antecedentes se encuentren calificados como secretos o reservados, de conformidad a la legislación vigente,

caso este último en que se requerirá la autorización previa del Tribunal (énfasis agregado).[69]

Además, la Fiscalía tiene atribuciones para requerir informes de organismos públicos técnicos, celebrar convenios de cooperación con otros servicios públicos y convenios para la transferencia electrónica de información y la interconexión electrónica.[70]

Por su parte, la LPDP también contempla mecanismos de colaboración. Esta ley dispone que la Agencia tiene la atribución de "[s]uscribir convenios de cooperación y colaboración con entidades públicas o privadas, nacionales, extranjeras o internacionales, que tengan competencia o estén relacionadas al ámbito de los datos personales" (art. 30 bis. inc. 1 letra k). Abordaremos en mayor detalle estos y otros mecanismos de colaboración en la parte V de este trabajo.[71]

En esta parte del trabajo, es posible concluir que la LPDP es relevante para los profesionales de la competencia chilenos porque es posible, e incluso probable, que su implementación motive a las autoridades de competencia a incorporar la regulación sobre protección de datos personales en sus decisiones. Esta incorporación ya se observa en el derecho comparado y en Chile, y esta tendencia puede ser catalizada en nuestro país por la LPDP. Si esto es así, conviene que los profesionales de la libre competencia se familiaricen con la LPDP.

Para facilitar este fin, el resto de este artículo ofrece un resumen de la LPDP, sus antecedentes, y su contexto regulatorio. Específicamente, abordamos sus fines según sus redactores (parte II), sus reglas de conducta (parte III), los incentivos al cumplimiento de estas reglas contemplados en esta ley, incluyendo la Agencia de Protección de Datos Personales y las sanciones que puede imponer (parte IV), y la relación entre la LPDP y otras leyes que regulan el tratamiento de datos personales (parte V).

II. FINES DE LA LPDP E IMPLICANCIAS PARA SU INTERPRETACIÓN

En esta parte nos referiremos a los fines o el "espíritu" de la LPDP en su conjunto, tal como consta en la historia fidedigna de su establecimiento.

Los fines buscados por el legislador mediante la LPDP se pueden resumir en dos. Primero, el legislador pretendió mejorar el estándar de protección de datos personales. En particular, aumentar el "control" que tienen los titulares sobre el tratamiento de sus datos, con el fin de promover el derecho constitucional a la protección de los datos personales o "autodeterminación informativa" (sección II.A).

69 Decreto Ley 211 art. 39 inc. 2° letra f.

70 Ver, respectivamente, DL 211 art. 39 inc. 2° letras k, l, y m. Además, la Ley 19.880 sobre Procedimientos Administrativos tiene reglas específicas de cooperación "forzada" entre agencias y servicios. Sin embargo, una limitación importante del mecanismo es que solo alcanza los actos administrativos "de carácter general" (art. 37 bis inc. 1). Por ejemplo, sería aplicable a los informes que la Fiscalía elabora para el TDLC en relación con uso de sus facultades para proponer proyectos de ley pro-libre competencia (ver el art. 18 N 4 y el 39 inc. 2° letra e del DL 211). Pero no se podría utilizar respecto de investigaciones de ilícitos contrarios a la libre competencia. Con estas precisiones, el art. 37 bis inc. 1 de la Ley 19.880 ley dice: "Cuando un órgano de la Administración del Estado deba evacuar un acto administrativo de carácter general que tenga claros efectos en los ámbitos de competencia de otro órgano, le remitirá todos los antecedentes y requerirá de éste un informe para efectos de evitar o precaver conflictos de normas, con el objeto de resguardar la coordinación, cooperación y colaboración entre los órganos involucrados en su dictación". Según el mismo artículo, el órgano requerido tiene 30 días corridos para elaborar un informe; órgano que lo solicitó está obligado a considerar el informe y referirse al mismo en su decisión, aunque el informe es no vinculante. Con todo, en casos de urgencia se puede omitir la petición del informe. Ver también abajo sección V.B.2.

71 Ver abajo sección V.B.2.

Segundo, el legislador intentó ajustar la legislación chilena a los estándares del GDPR de la Unión Europea. En parte para alcanzar el primer objetivo, pero también (y tal vez principalmente) para obtener de la Unión Europea una declaración de que Chile es "país adecuado" en esta materia y, de esa manera, facilitar la transferencia internacional de datos personales, por razones que explicaremos aquí (sección II.B). Este fin se relaciona con el concepto del "efecto Bruselas" del GDPR –las dinámicas sociales que explican el alcance global de esta regulación europea– el cual será abordado brevemente en un excurso (sección II.C).

Tras describir estos fines y ese breve excurso, reflexionaremos sobre la relación entre el segundo fin –obtener la declaración de adecuación de la UE– y los métodos que guiarán la interpretación de la LPDP. Argumentaremos que es probable que el derecho europeo sea una fuente utilizada frecuentemente por la Agencia y otros actores para dilucidar el significado de las disposiciones de la LPDP (sección II.C).

A. Mejorar el estándar de protección del derecho constitucional a la protección de los datos personales

Los fines de la LPDP fueron articulados en dos proyectos de ley que dieron lugar a esta ley tras ser acumulados. Estos proyectos son una moción parlamentaria de los senadores Harboe, Araya, De Urresti, Espina y Larraín del año 2017, y un mensaje presidencial de la Presidenta Michele Bachelet del mismo año.[72]
En ambos proyectos se afirmó que el fin de la futura ley sería mejorar la protección de datos personales, específicamente aumentando el "control" que tienen las personas sobre el tratamiento de datos personales realizado por empresas y otras personas. Esta justificación de la ley fue desarrollada en la moción parlamentaria de la siguiente manera:

> Es un hecho que no contamos con una legislación adecuada, esto es una ley que exprese adecuadamente el principio rector en materia de protección de datos: el control. Este control significa poner a las personas en el centro, se traduce en la entrega de herramientas efectivas para el control de la información personal. Estas herramientas de control presentan una doble faz, un conjunto de derechos y una autoridad con facultades competentes a efectos

72 Aquí nos enfocamos en el mensaje y la moción, y el texto de la misma ley, dada la importancia que tienen estos documentos para dilucidar los fines generales de las leyes. Para quienes estén interesados en explorar otros aspectos de la historia legislativa de la LPDP, esta nota al pie resume sus principales hitos. En el año 2017, el Congreso empezó a tramitar dos proyectos de ley que buscaban reformar la Ley 19.628 de 1999. Uno había sido presentado mediante una moción de senadores en enero del 2017, y otro por mensaje de la Presidenta Bachelet en marzo del mismo año. Ver Moción de los Honorables Senadores señores Harboe, Araya, De Urresti, Espina y Larraín, sobre protección de datos personales, Boletín N° 11.092-07, 17 de enero de 2017, http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11092-07 (en adelante, "Moción LPDP"); Mensaje de la Presidenta de la República, Boletín N° 11.144-04, 15 de marzo de 2017, http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07 (en adelante, "Mensaje LPDP"). El Congreso acumuló estos proyectos en el proyecto Boletín N° 11.144-07. La tramitación del proyecto de ley duró más de siete años. El Senado aprobó el proyecto en primer trámite constitucional el 25 de enero del 2022, cinco años después de la presentación del primer proyecto. La Cámara de Diputados, en segundo trámite constitucional, revisó el proyecto por casi un año y medio, y aprobó una nueva versión el 8 de mayo del 2023. El Senado, en tercer trámite constitucional, aprobó y rechazó varias de las modificaciones de la Cámara, produciendo una tercera versión del proyecto el 3 de enero del 2024. En ese momento, las dos cámaras crearon una comisión mixta para resolver sus diferencias y mejorar el proyecto. La Comisión Mixta trabajó a partir de enero 2024, y presentó su versión del proyecto en un informe del 12 de agosto del mismo año. Ambas cámaras del Congreso aprobaron la propuesta de la Comisión Mixta el 26 de agosto de 2024. El 29 de agosto del mismo año, el Presidente de la República le comunicó al Congreso que no observaría el proyecto. El 3 de septiembre, el Senado envió el proyecto al Tribunal Constitucional, para que este órgano revisara la constitucionalidad de las normas de la LPDP que tienen rango orgánico constitucional. Ver "Tramitación", Boletín N° 11.144-04, 15 de marzo de 2017, http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07. Al momento del cierre de nuestra investigación (fines de octubre de 2024), el Tribunal Constitucional está revisando el proyecto de ley haciendo ejercicio del control obligatorio de constitucionalidad en la causa Rol N° 15733-24-CPR, sobre Control de constitucionalidad del proyecto que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, correspondiente a los Boletines N°s 11.092-07 y 11.144-07, refundidos.

> de la [sic] prevenir, difundir, investigar, fiscalizar, detectar y sancionar las infracciones a las leyes de protección de datos.[73]

El mensaje presidencial, a su vez, explicó su objetivo así:

> 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.[74]

Tanto la moción como el mensaje vincularon el control del titular y otras formas de protección con los derechos humanos, específicamente, el derecho a la vida privada. Por ejemplo, la Presidenta Bachelet dijo que la ley buscaba asegurar "el respeto y protección de los derechos y libertades fundamentales de los titulares de datos, en particular el derecho a la vida privada".[75]

Este fundamento de tipo constitucional fue reforzado mediante una reforma constitucional del 2018, cuya tramitación había comenzado el 2014, antes del proyecto de nueva ley de datos personales. El Congreso modificó la Constitución para agregar en su art. 19 Nº 4 una referencia expresa a la protección de datos personales:

> El respeto y protección a la vida privada y a la honra de la persona y su familia, *y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley*.[76]

El significado de la reforma constitucional ha sido resumido así por el profesor Pablo Contreras:

> Antes de este reconocimiento expreso, el derecho a la protección de datos personales se había entendido como parte del contenido iusfundamentalmente protegido del derecho al respeto y protección de la vida privada, establecido en el artículo 19 N° 4 de la Constitución. Así lo había argumentado la doctrina y la jurisprudencia mayoritaria. Pero hoy eso debe ser repensado a partir del reconocimiento explícito del derecho a la autodeterminación informativa como un derecho independiente del derecho a la vida privada, consagrado a partir de la reforma constitucional del 2018.[77]

---

73 Moción LPDP, p. 4.
74 Mensaje LPDP, p. 4.
75 Ibid.
76 Art. 19 Nº 4 Constitución, énfasis agregado. El texto en cursivas fue agregado por la ley N°21.096, Consagra el derecho a protección de los datos personales, publicada en el Diario Oficial el 16 de junio de 2018. La reforma se originó en la Moción de los Honorables Senadores señores Harboe, Araya, Lagos, Larraín y Tuma, que consagra el derecho a la protección de los datos personales, Boletín N° 9.384-07, 11 de junio de 2024, http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=9384-07. Como se puede observar, algunos de los senadores que presentaron esta moción también presentaron la moción que originó la LPDP (Harboe y Araya). Sobre la tramitación de esta reforma constitucional, ver Pablo Contreras, "El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena", *Estudios constitucionales* 18, nº 2 (2020): 87–120.{\\i{}Estudios constitucionales} 18, n\\super o\\nosupersub{} 2 (2020

La creación del derecho constitucional a la protección de los datos personales (o "autodeterminación informativa") también tuvo un fin político-estratégico:

> Estratégicamente, la reforma persiguió un objetivo de forzar al legislador en la regulación y reforma del tratamiento y protección de los datos personales en nuestro país. En efecto, el debate legislativo advirtió la necesidad de continuar el esfuerzo de la reforma constitucional con una modificación integral de Ley No. 19.628.[78]

Sin embargo, tomaría más de seis años tras la reforma constitucional para que su propósito político se expresara en una nueva ley de datos personales.

La LPDP hace explícita su relación con el derecho constitucional a la protección de los datos personales en su art. 1 inc. 1:

> Objeto y ámbito de aplicación. La presente ley tiene por objeto regular la forma y condiciones en la cual se efectúa el tratamiento y protección de los datos personales de las personas naturales, *en conformidad al artículo 19 N° 4 de la Constitución Política* (énfasis agregado).

En definitiva, un objetivo buscado por el legislador con la LPDP fue mejorar la situación jurídica del derecho constitucional a la protección de los datos personales.

B. Adecuar la legislación chilena a la regulación de la Unión Europea

Otro fin buscado por los legisladores con la LPDP fue adecuar la legislación nacional a los estándares de regulaciones comparadas, específicamente el GDPR de la Unión Europea; y, a su vez, alcanzar fines ulteriores, incluyendo no solo la mejor protección de los titulares (a la cual ya nos hemos referido en la parte anterior) sino también facilitar la transparencia internacional de datos personales.
Según el mensaje presidencial, uno de los objetivos del proyecto de ley fue

> [d]otar al país de *una legislación moderna y flexible en materia de tratamiento de datos personales*, que sea consistente con los compromisos internacionales adquiridos luego de su incorporación a la OCDE y ajustada a las normas y estándares internacionales.[79]

De manera similar, la moción parlamentaria dijo que se necesitaba "[e]stablecer un nuevo esquema normativo que se ajuste los estándares exigidos por las legislaciones más modernas".[80] También aludió

77 *Ibid*., 89.Contreras, 89.it reviews the legislative history of the constitutional amendment and the main debates that took place. In particular, three dilemmas are reviewed: first, the need to constitutionalize or not informational self-determination as a fundamental right; second, the normative density required to constitutionalize the right; and, third, the legal relationship of entitlement or ownership over personal data. The text concludes by anticipating two challenges for the legal regulation of the right: first, regarding the type of constitutional referral to the legislator to protect personal data and, second, the jurisdictional protection of informational self-determination and, in particular, the protection of the right through the recurso de protección, through habeas data and through a specialized agency as control authority.","container-title":"Estudios constitucionales","ISSN":"0718-5200","issue":"2","journalAbbreviation":"Estudios constitucionales","language":"es","page":"87-120","source":"DOI.org (Crossref

78 *Ibid*., 115.

79 Mensaje LPDP, 5.

80 Moción LPDP, 5.

a la OCDE: "el ingreso de Chile a OCDE en 2010 significó el compromiso de adecuaciones normativas y modificación de marcos legales, entre ellos el de protección de datos".[81]

Por supuesto, existen varias regulaciones comparadas sobre protección de datos personales. Entonces, ¿cuál es la que se buscó emular? La respuesta es clara: el derecho europeo, específicamente, el GDPR.[82] Si bien el mensaje presidencial guardó silencio al respecto, la moción parlamentaria fue explícita:

> son varios los estándares que es posible adoptar, optándose en la presente moción parlamentaria por el más alto de ellos, el Reglamento Europeo de Protección de Datos N° 679 del 27 de abril de 2016, 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 que deroga la Directiva 95/46/CE, como referente.[83]

Los legisladores también citaron al GDPR como referente durante las siguientes etapas de la tramitación del proyecto.[84] También invitaron a representantes de la Unión Europea a participar de la deliberación y ofrecer sugerencias al proyecto.[85]
¿Por qué los órganos colegisladores utilizaron el GDPR como referente para redactar la LPDP?

La moción parlamentaria sostuvo que "[l]os países que muestran un mayor desarrollo normativo en la materia, han basado sus normas en el modelo europeo".[86] Efectivamente, el GDPR se ha transformado en el "estándar de oro" de la regulación de datos personales a nivel global, inspirando la adopción de leyes similares en muchos países.[87] Como ha afirmado la profesora Anu Bradford, hoy "[l]a UE marca la pauta a nivel mundial en materia de regulación de la privacidad y la protección de datos".[88] En este ámbito la UE

81 *Ibid*., 1. Sobre las recomendaciones de la OCDE y su influencia en la reforma constitucional que fue tramitada en paralelo a la LPDP, ver Contreras, "El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena", 92.92.","plainCitation":"Contreras, "El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena", 92.","noteIndex":76},"citationItems":[{"id":41116,"uris":["http://zotero.org/users/1504437/items/FQ34NDAR"],"itemData":{"id":41116,"type":"article-journal","abstract":"The paper examines the recognition of the right to the protection of personal data as a fundamental right in the Chilean Constitution. To this end, it reviews the legislative history of the constitutional amendment and the main debates that took place. In particular, three dilemmas are reviewed: first, the need to constitutionalize or not informational self-determination as a fundamental right; second, the normative density required to constitutionalize the right; and, third, the legal relationship of entitlement or ownership over personal data. The text concludes by anticipating two challenges for the legal regulation of the right: first, regarding the type of constitutional referral to the legislator to protect personal data and, second, the jurisdictional protection of informational self-determination and, in particular, the protection of the right through the recurso de protección, through habeas data and through a specialized agency as control authority.","container-title":"Estudios constitucionales","ISSN":"0718-5200","issue":"2","journalAbbreviation":"Estudios constitucionales","language":"es","page":"87-120","source":"DOI.org (Crossref Ver también OECD, "Roadmap for the Accession of Chile to the OECD Convention. C(2007)100/FINAL", 3 de diciembre de 2007, http://www.oecd.org/legal/41463062.pdf, p. 29.

82 Sobre el GDPR, ver nota 13.

83 Moción LPDP, 5.

84 Ver, por ejemplo, Boletín N° 11.144-07, Primer informe de la Comisión de Constitución del Senado, p. 7; Segundo informe Comisión Constitución del Senado, pp. 42-43; Informe Comisión de Hacienda, p. 3, disponibles en http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07.

85 Ver, por ejemplo, Senado, "Proyecto de datos personales: estudian normas que irían a Comisión Mixta - Senado - República de Chile", Senado, accedido 28 de noviembre de 2023, https://www.senado.cl/proyecto-de-datos-personales-estudian-normas-que-irian-a-comision-mixta ("en el paso por la Cámara de Diputados se constituyó una comisión en paralelo con expertos de la Unión Europea, académicos y asesores legislativos, entre otros, para ir consensuando aspectos"). Ver también Marcelo Drago y Romina Garrido, "No todo es perfecto en la reforma a la ley de protección de datos personales", *La Tercera*, 14 de noviembre de 2023, https://www.latercera.com/opinion/noticia/columna-de-romina-garrido-y-marcelo-drago-no-todo-es-perfecto-en-la-reforma-a-la-ley-de-proteccion-de-datos-personales/PIWLIKL7T5EXHHQUGOIXZAXXBQ/ ("[L]a reforma a la ley de protección de datos personales chilena está decididamente inspirada en el reglamento europeo sobre la materia").

86 Moción LPDP, p. 3.

87 Ver Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, (New York: Oxford University Press, 2020), p. 147-155.

88 *Ibid*., 132. Traducción de los autores.

ha mostrado una notable capacidad para ser una fuente de estándares globales, lo que se conoce como el "efecto Bruselas",[89] concepto al cual volveremos al final de esta sección.

En este contexto regulatorio global, si el legislador chileno quería alcanzar un "mayor desarrollo normativo en la materia"–mejorar la protección de datos personales, como hemos explicado en la sección anterior– era razonable que mirara al GDPR como modelo.[90] Sin embargo, este fin no es la única razón que explica la adopción del GDPR como modelo o referente de la LPDP.

Como ha explicado la profesora Michelle Bordachar, el legislador también buscó "conseguir que la Unión Europea declare que Chile garantiza un nivel de protección adecuado y, por tanto, autorice la transferencia internacional de datos personales sin requerir ninguna autorización específica".[91] Facilitar la transferencia internacional de datos, para lo cual es útil una declaración de país adecuado de la UE, fue un objetivo mencionado por el legislador chileno. Tanto la moción parlamentaria como el mensaje presidencial enfatizaron que la nueva ley facilitaría la "libre circulación" de los datos personales.[92] Ambos proyectos conectaron esta libre circulación con una decisión de adecuación de la Unión Europea.[93] En su mensaje, la Presidenta Bachelet declaró:

> *Para que Chile mantenga e incremente su trayectoria de desarrollo y crecimiento económico*, es necesario, tal como lo ha venido planteando la OCDE en sus recomendaciones, emprender cambios y transformaciones que permitan avanzar hacia una economía más innovadora, basada en el conocimiento e *integrada por más empresas que sean capaces de competir a nivel mundial y participar en las cadenas globales de valor, especialmente en el ámbito de los servicios globales*.
>
> Una de las mayores deudas en materia regulatoria es la falta de una legislación moderna y flexible que permita cumplir las normas y estándares internacionales en materia de protección y tratamiento de los datos personales.[94]

Para entender este fin del legislador chileno –obtener una declaración de adecuación de la UE para facilitar la transferencia internacional de datos personales– es útil tener en cuenta qué dice el GDPR sobre esta materia y sus implicancias económicas y jurídicas. La regulación europea establece que los responsables que tratan datos personales de titulares que están en la UE no pueden transferir estos datos a otro territorio –a Chile, por ejemplo– a menos que garanticen niveles "adecuados" de protección de datos personales.[95]

Estas restricciones establecidas por el GDPR a la transferencia internacional de datos pueden tener un alto impacto económico. Así lo ha explicado el profesor Lothar Detterman:

89 Ver abajo notas 97, 98 y 99, y el texto principal que acompañan.
90 EE.UU., otro país que tiende a influenciar a los legisladores chilenos, hasta ahora ha sido incapaz de crear una regulación robusta y comprehensiva en materia de protección de datos personales, más allá de esfuerzos de estados como California.
91 Michelle Bordachar Benoit, "Comentarios al proyecto de ley chileno sobre protección de datos personales: Deficiencias e inconsistencias en los derechos ARCO", *Revista chilena de derecho y tecnología* 11, nº 1 (junio de 2022): 398.
92 Ver Mensaje LPDP, 4, y Moción LPDP, 4.
93 Ver Moción, 3 ("en este momento Chile, al ser considerado como un país con un nivel no adecuado de protección en materia de datos personales ha debido someterse al mecanismo de las cláusulas tipo en los respectivos contratos que se suscriben con empresas extranjeras"). La moción, tras afirmar que Chile tenía una regulación "insuficiente y actualmente inferior al de sus países vecinos", inmediatamente notó que Argentina y Uruguay eran países que habían obtenido la declaración de la Unión Europea de país adecuado. *Íbid*., 3.
94 Mensaje, 2, énfasis agregado.
95 Ver arts. 44 a 49 del GDPR.

> La mayoría de las empresas del mundo se ven más o menos afectadas, ya sea porque ellas o sus filiales están directamente sujetas a estas leyes [el GDPR y las leyes domésticas europeas basadas en el GDPR] o porque los socios comerciales directos o indirectos están traspasando sus propias obligaciones de cumplimiento. Ellas se enfrentan a la cuestión de cómo transferir legalmente datos personales de Europa a otros continentes. Las empresas del Espacio Económico Europeo (EEE) generalmente tienen prohibido enviar datos personales a países fuera del EEE, a menos que se garanticen niveles adecuados de protección de datos. Esto afecta directamente a los grupos multinacionales de empresas con sede fuera de Europa porque sus propias filiales en el EEE tienen prohibido compartir datos personales sobre empleados, contratistas y clientes. Se ven afectadas indirectamente todas las empresas que tienen clientes, proveedores y otros socios comerciales en Europa porque sus socios comerciales europeos tienen prohibido compartir datos personales. También se ven afectadas indirectamente las empresas que prestan servicios a empresas con datos europeos. Muy pocas empresas grandes están completamente aisladas del problema, dadas las estrechas conexiones globales de las empresas actuales.[96]

Así, para los responsables y los estados que, como Chile, quieren fomentar sus actividades económicas, es importante cumplir con las garantías de protección de datos personales exigidas por le UE.

Para ello una regulación como la LPDP es clave. Una garantía de protección adecuada reconocida por el GDPR es que, a juicio de la Comisión Europea, el país al cual se transfieren los datos personales garantice "un nivel de protección adecuado".[97] En esta evaluación la Comisión debe considerar, entre otros factores, "la legislación pertinente" y "la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes".[98] Es decir, debe examinar si el país en cuestión tiene leyes similares al GDPR y autoridades de control de protección similares a las europeas. El legislador chileno intentó cumplir con estos requisitos mediante las reglas de conducta de la LPDP y su Agencia.

En resumen, el legislador dictó la LPDP para lograr que la UE (su Comisión) declarara que nuestro país tiene un nivel de protección de datos adecuado y, por esa vía, permitiera la transferencia internacional de datos personales de titulares dentro de la UE a nuestro país[99]

C. Excurso: la LPDP y el "efecto Bruselas" del GDPR

Las consideraciones anteriores permiten entender a la LPDP como una expresión del así llamado "efecto Bruselas", un concepto que es a menudo mencionado en discusiones nacionales e internacionales sobre la regulación de protección de datos personales.

Como ha explicado Anu Bradford, quien acuñó la expresión, el concepto de efecto Bruselas se refiere al "poder

96 Lothar Determann, *Determann's Field Guide to Data Privacy Law: International Corporate Compliance*, 5th ed. (Cheltemham, UK: Edward Elgar, 2022), 31. Traducción de los autores. Sobre las transferencias internacionales, ver también arriba sección III.D.

97 Ver art. 45 del GDPR. Con todo, mecanismos de transferencia internacional alternativos se encuentran en los arts. 46, 47 y 49.

98 Art. 45.2 letras a y b (respectivamente).

99 Es posible que haya una tensión entre el fin de mejorar la protección de datos personales y facilitar la transferencia internacional de los datos personales. Un mayor volumen de transferencias crea nuevas oportunidades para los incidentes de seguridad y otras afectaciones a los intereses de los titulares. Con todo, los nuevos deberes del responsable establecidos por la LPDP y la actividad fiscalizadora de la Agencia pueden contribuir a minimizar ese riesgo.

unilateral de la UE para regular los mercados globales".[100] ¿En qué consiste este poder? Según Bradford, el efecto Bruselas puede ser de dos tipos, y ambos han contribuido a que el GDPR tenga una influencia global.

El primer tipo es el efecto Bruselas *de facto*. Incluso antes de que países no europeos adoptaran leyes como el GDPR, varios responsables que operaban en ellos –especialmente las empresas transnacionales– empezaron a adoptar los estándares del GDPR en sus operaciones en esos países. Lo hicieron para mantener su acceso al mercado de la UE (para lo cual debían cumplir con el GDPR) y para abaratar costos mediante la estandarización de la manera como tratan datos personales.

El segundo tipo de efecto Bruselas es el *de jure* o formal. El GDPR ha servido como modelo o referente de nuevas leyes extranjeras de protección de datos personales, especialmente como consecuencia del mecanismo de "adecuación" que hemos discutido en esta sección y de la colaboración e influencia de autoridades europeas.[101]

Así, el efecto Bruselas *de jure* parece dar cuenta de la creación de la LPDP. Pero también es posible que la LPDP también se relacione con el efecto Bruselas *de facto*. En la medida que, como también ha explicado Bradford, una vez que las empresas trasnacionales adoptan regulaciones europeas como el GDPR fuera de la UE, ellas tienen incentivos para hacer lobby a nivel local y lograr que otros países adopten regulaciones similares.[102]

A su vez, es posible que la LPDP también contribuya al efecto Bruselas del GDPR en el futuro. La ley chilena tiene reglas sobre transferencia internacional de datos que reproducen el requisito de adecuación del GDPR (aunque esta vez utilizando la LPDP como referente directo).[103] Por esa vía, la ley chilena puede incentivar a otros países –tal vez especialmente en Latinoamérica– a adoptar regulaciones similares al GDPR.

D. Implicancias para la interpretación de la LPDP: el rol del derecho europeo

Hasta aquí hemos observado que los fines generales de la LPDP, según los órganos colegisladores que la crearon, fueron mejorar el estándar de protección de los datos personales y lograr que la Comisión Europea declare que Chile es un "país adecuado" para facilitar la transferencia internacional de datos personales. Este segundo fin y, en general, la importante similitud entre el GDPR y la LPDP, pueden tener implicancias para la interpretación de nuestra ley.

La Agencia y otros operadores de la protección de datos personales se enfrentarán a la tarea de dilucidar el significado de términos vagos de la LPDP y resolver conflictos de reglas, para resolver casos particulares y al crear normas generales que concreticen las de la LPDP. ¿Cómo llevarán a cabo esta tarea interpretativa?

La interpretación de la LPDP probablemente acudirá al derecho europeo: al GDPR y a decisiones sobre esta regulación de las autoridades de protección de datos europeas nacionales y comunitarias.

100 Anu Bradford, The Brussels Effect, xvi. Traducción de los autores.
101 Sobre el efecto Bruselas y su relevancia global para la protección de datos personales, ver Anu Bradford, The Brussels Effect, especialmente pp. 25-65 y 132-155. Ver también Paul M. Schwartz, "Global Data Privacy: The EU Way", New York University Law Review 94 (2019): 771–818.
102 Ver Anu Bradford, The Brussels Effect, p. 119 ("Esas empresas prefieren normas uniformes y enfrentan menos costos de ajuste si sus gobiernos de origen adoptan una ley que, de facto, ya rige su conducta empresarial"). Traducción de los autores.
103 Ver abajo sección III.E.3.

Esta utilización del derecho europeo como fuente para interpretar las LPDP se puede justificar en nuestras reglas sobre interpretación de la ley. Estas reglas mandan dilucidar los términos vagos o indeterminados de la ley considerando su "intención o espíritu" –sus fines– tal como han sido expresados en su mismo texto o en "la historia fidedigna de su establecimiento".[104] Un aspecto del "espíritu" de la LPDP, tal como consta en la historia legislativa que revisamos en las secciones anteriores, es que la LPDP adopte el estándar de la UE para que la UE declare que Chile es un "país adecuado". Este fin son honrado si la LPDP es interpretada según el derecho europeo.

Más allá del criterio teleológico de interpretación, hay una razón pragmática a favor de una interpretación de la LPDP en base al derecho europeo. Este derecho ya cuenta con fuentes que desarrollan reglas del GDPR que son muy similares a las reglas de la LPDP. A saber, las decisiones de las autoridades europeas y la literatura académica sobre el GDPR. Por ejemplo, cuando la Agencia desarrolle guías sobre el uso de cookies –materia que carece de una regulación específica en la LPDP– es probable que considere las guías al respecto del Comité Europeo de Protección de Datos (*European Data Protection Board*) y especialmente de la Agencia Española de Protección de Datos (por razones de lenguaje y de tradición jurídica). [105] Es más, esta utilización de fuentes europeas ya es una práctica habitual de los profesionales de protección de datos chilenos.[106]

III. REGLAS DE CONDUCTA DE LA LPDP

La parte anterior introdujo la LPDP mediante el análisis de sus fines generales y sus implicancias para la interpretación de esta ley. El resto de este trabajo aborda el contenido de las disposiciones de la LPDP, empezando por sus reglas de comportamiento.

Nuestro resumen de las reglas de conducta de la LPDP comienza por su ámbito de aplicación. La LPDP regula el tratamiento de datos personales de personas naturales ubicadas en el territorio chileno, realizado por responsables establecidos en Chile o el extranjero, y el tratamiento de datos personales de personas naturales ubicadas en el extranjero, cuando es realizado por responsables establecidos en Chile. El ámbito de aplicación de la LPDP es limitado por excepciones expresas reconocidas por esta ley (sección III.A).

Por regla general, la LPDP solamente permite el tratamiento de datos personales cuando los responsables cumplen con alguna de las condiciones que la LPDP denomina "fuentes de licitud del tratamiento" (también

104 El texto completo del art. 19 inc. 2 del Código Civil dice: "Pero bien se puede, para interpretar una expresión obscura de la ley, recurrir a su intención o espíritu, claramente manifestados en ella misma, o en la historia fidedigna de su establecimiento". Sobre el origen y significado de esta regla y su relación con otros cánones de interpretación de la leyes, ver Alejandro Guzmán Brito, "La historia dogmática de las normas sobre interpretación recibidas por el Código Civil de Chile", en Interpretación, integración y razonamiento jurídicos: Conferencias y ponencias presentadas en el Congreso realizado en Santiago y Viña del Mar entre el 23 y 25 de mayo de 1991 (Santiago: Editorial Jurídica de Chile, 1992), 41–87; Alejandro Guzmán Brito, Las reglas del "Código Civil" de Chile sobre interpretación de las leyes, 2da edición revisada (Santiago: LegalPublishing Chile, 2011); Alejandro Guzmán Brito, Codificación del Derecho Civil e Interpretación de las Leyes (Madrid: Iustel, 2011), 456–70; Antonio Bascuñán Rodríguez, "Savigny Revisitado", en Estudios de Derecho Civil XV – XVII. Jornadas Nacionales de Derecho Civil. Viña del Mar (2019), ed. Fabián Elorriaga (Santiago: Thompson Reuters, s. f.), 3–30.

105 European Data Protection Board, "Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive", 14 de noviembre de 2023, https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en; Agencia Española de Protección de Datos, "Guía sobre el uso de las cookies", Enero de 2024, https://www.aepd.es/guias/guia-cookies.pdf.

106 En un documento del SERNAC que revisa experiencia comparada sobre la regulación de cookies, el órgano chileno se refiere repetidamente a la guía de cookies de la Agencia Española de Protección de Datos. Ver Servicio Nacional del Consumidor, "Consentimiento en el uso de Cookies: Evidencia experimental sobre el impacto de la privacidad por defecto y los patrones oscuros en las decisiones de los consumidores.", marzo de 2022, https://www.sernac.cl/portal/619/articles-64969_archivo_01.pdf.

conocidas como "bases de legitimidad"). Estas fuentes de licitud incluyen el consentimiento del titular, leyes que exigen el tratamiento, y otras fuentes (sección III.B).

Además, los responsables deben cumplir con varios deberes adicionales, por ejemplo, el deber de velar por la seguridad de los datos personales frente a riesgos de diverso tipo, desde ataques de hackers hasta la publicación por error de los datos (sección III.C).

Los responsables también deben establecer procedimientos para responder a reclamos de los titulares y satisfacer sus pretensiones, cuando ellas corresponden a uno de los "derechos del titular de datos personales" reconocidos por la LPDP (sección III.D).

Finalmente, esta parte resume las reglas especiales de la LPDP sobre cesión de datos personales, mandatarios (o "encargados"), y transferencia internacional de datos (sección III.E). También menciona los deberes relacionados con las instituciones de cumplimiento de la LPDP (sección III.F), aunque estos últimos serán objeto de una descripción más detallada en la parte IV del trabajo.

A. Ámbito de las reglas de conducta de la LPDP

1. Ámbito personal y material: tratamiento de datos sobre personas naturales realizado por todo tipo de personas

La LPDP regula "todo tratamiento de datos personales que realice una persona natural o jurídica, incluidos los órganos públicos" (art. 1 inc. 2). Esta disposición hace alusión a algunos conceptos claves que conviene explicitar.

1.1. Dato personal

La LPDP define el concepto de dato personal de la siguiente manera:

> cualquier información vinculada o referida a una persona natural identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante uno o más identificadores, tales como el nombre, el número de cédula de identidad, el análisis de elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona (art. 2 letra f).

1.2. Titular de datos personales

El titular es la persona natural a quien se refiere la información que tiene el estatus de dato personal (art. 2 letra ñ).

1.3. Tratamiento de datos personales

La LPDP define el "tratamiento de datos" así:

> cualquier operación o conjunto de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan de cualquier forma recolectar, procesar, almacenar, comunicar, transmitir o utilizar datos personales o conjuntos de datos personales (art. 2 letra o).[107]

Este concepto de "tratamiento" es similar al concepto asociado al término "uso" en el lenguaje común. Así, se podría decir que la LPDP regula a quienes usan datos personales de terceros.

1.4. Sujetos regulados: todo tipo de personas

La LPDP regula el tratamiento de datos personales realizado por todo tipo de personas, ya sea naturales y jurídicas, privadas o públicas. Así, esta ley es aplicable a empresas, organizaciones de la sociedad civil, órganos del Estado e individuos.

Para efectos de determinar las obligaciones que pesan sobre los sujetos regulados, la LPDP distingue entre el "responsable" y el "encargado". La distinción depende del grado de control que ejercen sobre el tratamiento.

> Responsable de datos o responsable: toda persona natural o jurídica, pública o privada, que decide acerca de los fines y medios del tratamiento de datos personales, con independencia de si los datos son tratados directamente por ella o a través de un tercero mandatario o encargado (art. 2 letra n).
>
> Tercero mandatario o encargado: la persona natural o jurídica que trate datos personales, por cuenta del responsable de datos (art. 2 letra x).

Tanto el responsable como el encargado son sujetos de obligaciones establecidas por la LPDP. Sin embargo, en general el primero tiene una carga regulatoria más pesada que el segundo.[108] Este trabajo se concentra en los deberes del responsable.[109]

2. Ámbito territorial

La LPDP aplica a:

(a) Responsables o encargados establecidos en Chile (art. 1 bis inc. 1, letra a);

(b) Encargados establecidos en el extranjero que tratan datos por cuenta de responsables establecidos en

107 Existe una incongruencia entre la expresión "tratamiento de datos", que es comprehensivo del tratamiento de todos los tipos de datos (personales y no personales) y la definición, que se refiere solo al tratamiento de datos *personales*. Esta incongruencia puede obedecer a un error de técnica legislativa.

108 La LPDP también distingue entre responsables o encargados que son personas públicas (autoridades y órganos del Estado) y las personas que no tienen esa calidad. Ver arriba nota 11.

109 Sobre los deberes del encargado, ver abajo sección III.E.2.

Chile (art. 1 bis inc. 1, letra b);

(c) Responsables o encargados establecidos en el extranjero cuyo tratamiento tiene una conexión importante con titulares ubicados en Chile. Específicamente, cuando el tratamiento esté destinado a (1) "ofrecer bienes o servicios a titulares que se encuentren en Chile", o (2) "monitorear el comportamiento de titulares que se encuentran en el territorio nacional, incluyendo su análisis, rastreo, perfilamiento o predicción de comportamiento" (art. 1 bis inc. 1, letra c).

(d) Responsables establecidos en el extranjero a quienes se les aplique LPDP "a causa de un contrato o del derecho internacional" (art. 1 bis inc. 2).

Por ejemplo, por aplicación del art. 1 bis inc. 1, letra c, la empresa Meta, que está establecida en los EE.UU., debe cumplir con la LPDP cuando recopila datos personales de usuarios que residen en Chile con el fin de ofrecer el servicio de red social Facebook o Instagram.

3. Límites al ámbito de aplicación de la LPDP

La LPDP excluye de su ámbito de aplicación a los siguientes tratamientos de datos personales:

3.1. Excepción "doméstica"

La LPDP excluye de su ámbito de aplicación "al tratamiento de datos que efectúen las personas naturales en relación con sus actividades personales" (art. 1 inc. 4). La GDPR se refiere a este tipo de actividad como actividad "exclusivamente personal o doméstica", y también la exceptúa de su alcance.[110]

A partir de este tipo de excepción "doméstica", en la Unión Europea se ha entendido que la regulación sobre protección de datos personales no aplica a "la correspondencia y los registros de direcciones incluso si se pueden referir a la vida privada de otros, en la medida que su uso sea para fines meramente personales y no para fines profesionales o comerciales".[111]

3.2. Excepción de la libertad de expresión

La LPDP también excluye de su ámbito de aplicación "al tratamiento de datos que se realice en el ejercicio de las libertades de emitir opinión y de informar reguladas por las leyes a que se refiere el artículo 19, N° 12, de la Constitución Política de la República" (art. 1 inc. 3 LPDP).

¿A qué personas aplica esta excepción de libertad de expresión? Una interpretación posible es que ella aplica solamente a los "medios de comunicación social" tradicionales, tales como los diarios, canales de televisión o estaciones de radio.[112] Una interpretación alternativa es que la excepción aplica a todo tipo de persona en la

110 GDPR, art. 2(2)(c).

111 Eduardo Ustaran, ed., European Data Protection Law and Practice, 3rd ed. (Portsmouth, NH: International Association of Privacy Professionals, 2023), 115. Traducción de los autores. Para una discusión de diversas interpretaciones de la regla, ver ibid., 115-116.

112 Ello porque inmediatamente después de esta excepción (y como indicamos más abajo en el texto principal), la LPDP agrega que "[l]os medios de comunicación social quedarán sujetos a las disposiciones de esta ley en lo relativo al tratamiento de datos que efectúen con una finalidad distinta a la de opinar e informar" (art. 1 inc. 3 LPDP). Una interpretación sistemática sugeriría que toda esta disposición

medida que difundan contenidos, lo cual puede ocurrir tanto en medios tradicionales como también en redes sociales.[113] No es claro cuál interpretación es correcta. Preguntas similares han sido debatidas en el derecho europeo, a partir de una disposición similar del GDPR, sin que se hayan alcanzado respuestas concluyentes.[114] La Agencia y los tribunales chilenos tendrán la tarea de determinar el significado de la excepción.[115]

En cualquier caso, tras introducir la excepción de libertad de expresión la LPDP limita su alcance, al menos respecto de los "medios de comunicación social". Así, señala que "[l]os medios de comunicación social quedarán sujetos a las disposiciones de esta ley en lo relativo al tratamiento de datos que efectúen con una finalidad distinta a la de opinar e informar" (art. 1 inc. 3 LPDP). Una de las consecuencias posibles de esta regla es que clarifica que medios como las estaciones de televisión y de radio deben cumplir con la LPDP cuando realizan tratamiento de datos personales de sus trabajadores para fines de pago de sueldos, monitoreo, etc.

B. Fuentes de licitud del tratamiento de datos personales

Los responsables solo pueden tratar datos si cumplen con ciertas condiciones que reciben el nombre de "fuentes de licitud del tratamiento de datos" (art. 13). Estas fuentes de licitud (también conocidas como "bases de legitimación") incluyen el consentimiento del titular y el cumplimiento de una ley, entre otras. El responsable tiene la carga de acreditar que su tratamiento encuentra justificación en una fuente de licitud (arts. 12 inc. 8 y 13 inc. 2).

1. Consentimiento del titular

1.1. Consentimiento del titular en general

El responsable puede tratar datos personales si el titular ha declarado que acepta el tratamiento. La ley dice que el consentimiento es la "regla general" del tratamiento de datos (art. 12). En este sentido, la LPDP continúa el modelo regulatorio de la versión original de la Ley 19.628, que también configuraba al consentimiento como la regla general. Sin embargo, la LPDP intensificó los requisitos del consentimiento. Estos requisitos, al menos

se refiere exclusivamente a los medios de comunicación social. Además, entre las leyes comúnmente asociadas con el art. 19 N° 12 –a las que se remite la LPDP– se encuentran la Ley 19.733 Sobre las Libertades de Opinión e Información y Ejercicio del Periodismo del año 2001 (también conocida como la "Ley de Prensa", disponible en https://www.bcn.cl/leychile/navegar?idNorma=186049), la cual regula los "medios de comunicación social". Con todo, la definición legal de "medios de comunicación social" de la Ley de Prensa es bastante indeterminada: "aquellos [medios] aptos para transmitir, divulgar, difundir o propagar, en forma estable y periódica, textos, sonidos o imágenes destinados al público, cualesquiera sea el soporte o instrumento utilizado" (art. 2 inc. 1). A primera vista incluye los contenidos difundidos en redes sociales por sus usuarios, e incluso a estas plataformas.

113 Una interpretación menos restrictiva –que no limita la excepción a los medios de comunicación– es posible por al menos dos razones. Primero, porque la primera parte del art. 1 inc. 3 LPDP no especifica las personas a las cuales aplica la excepción. Un significado posible de este texto, según el lenguaje ordinario o común, es que se limita a crear una contraexcepción para un tipo de actor (los medios de comunicación social), sin que ello afecte el alcance de la excepción a otros actores. Segundo, porque si bien artículo 19 N° 12 de la Constitución se refiere a leyes sobre "medios de comunicación social" (incs. 1 y 2), "diarios, revistas y periódicos" (inc. 4), "estaciones de televisión" (incs. 5 y 6), y "la producción cinematográfica" (inc. 7), también contempla leyes que atribuyan responsabilidades por contenidos difundidos "en cualquier forma y por cualquier medio" (inc. 1).

114 Ver art. 85 GDPR. Sobre el debate interpretativo europeo, ver Natalija Bitiukova, "The GDPR's Journalistic Exemption and Its Side Effects", Verfassungsblog (blog) (Verfassungsblog, 16 de junio de 2023), https://verfassungsblog.de/the-gdprs-journalistic-exemption-and-its-side-effects/; Melinda Rucz, "SLAPPed by the GDPR: Protecting Public Interest Journalism in the Face of GDPR-Based Strategic Litigation against Public Participation", Journal of Media Law 14, nº 2 (3 de julio de 2022): 378–405.

115 Otra dimensión del problema es que la Ley de Prensa contiene un tipo penal pro-libertad de expresión que a primera vista es aplicable a los funcionarios de la Agencia, aunque al mismo tiempo la disposición hace posible que estos se defiendan invocando la propia LPDP. El art. 36 de la Ley de Prensa dice: "El que, fuera de los casos previstos por la Constitución o la ley, y en el ejercicio de funciones públicas, obstaculizare o impidiere la libre difusión de opiniones o informaciones a través de cualquier medio de comunicación social, sufrirá la pena de reclusión menor en su grado mínimo o multa de cuarenta a cien unidades tributarias mensuales" (énfasis agregado).

en teoría, buscan hacer probable que el titular ejerza control sobre el tratamiento de sus datos personales.[116]

Específicamente, para que el consentimiento al tratamiento cuente como tal la declaración del titular debe reunir los siguientes requisitos de oportunidad, forma y fondo (art. 12):

(a) Oportunidad: La declaración deber ser previa al tratamiento (art. 12 inc. 2).

(b) Fondo: El consentimiento debe ser "libre, informado y específico en cuanto a su finalidad o finalidades" (art. 12 inc. 2).

(c) Forma: La declaración debe ser verbal, escrita, o expresada a través de un medio electrónico equivalente, o mediante "un acto afirmativo que dé cuenta con claridad de la voluntad del titular" (art. 12 inc. 2). Además, el medio debe ser expedito, fidedigno, gratuito y estar permanentemente disponible para el titular (art. 12 inc. 5).

Los responsables que operan sitios web y aplicaciones suelen cumplir con esta fuente de licitud mediante páginas web o ventanas que presentan sus políticas de privacidad, y un formulario mediante el cual los usuarios las aceptan o rechazan. Como ya indicamos, el responsable debe "probar que contó con el consentimiento del titular" cuando así lo requiera la Agencia o un tribunal (art. 12 inc. 8). Esta regla procesal, junto a la obligación de obtener el consentimiento, incentiva a los responsables a obtener el consentimiento dejando un registro escrito del mismo.

Es posible que los requisitos del consentimiento sean desarrollados por la Agencia, en normativas o decisiones en casos concretos, con el fin de expandir la libertad de las personas. Así, la Agencia podría invocar el requisito del consentimiento "libre" para prohibir que los responsables extraigan el consentimiento del titular de manera manipulativa, mediante "elementos de la interfaz del usuario *(UI)* que pueden influir en el comportamiento de una persona en contra de sus intenciones o mejores intereses".[117]

1.2. consentimiento del tratamiento de datos sensibles y datos sobre menores de edad

La LPDP tiene reglas especiales para el consentimiento relativo al tratamiento de "datos sensibles" y a los datos sobre menores de edad. Los datos sensibles son

> aquellos datos personales que se refieren a las características físicas o morales de las personas o hechos o circunstancias de su vida privada o intimidad, tales como aquellos que revelen el origen étnico o racial, la afiliación política, sindical o gremial, situación socioeconómica, las convicciones ideológicas o filosóficas, las creencias religiosas, los datos relativos a la salud, al perfil biológico humano, los datos biométricos, y la información relativa a la vida sexual, a la orientación sexual y a la identidad de género de una persona natural (art. 2 letra g).

116 Para un análisis crítico de esta fuente de licitud, ver abajo sección III.B.4.

117 Johanna Gunawan et al., "A Comparative Study of Dark Patterns Across Web and Mobile Modalities", Proceedings of the ACM on Human-Computer Interaction 5, nº CSCW2 (18 de octubre de 2021): 1.n\\super o\\nosupersub{} CSCW2 (18 de octubre de 2021 Este tipo de elementos se conocen como "patrones oscuros" (dark patterns). Ver también M. R. Leiser, "Dark Patterns: The Case for Regulatory Pluralism between the European Unions Consumer and Data Protection Regimes", en Research Handbook on EU Data Protection Law, ed. Eleni Kosta, Ronald Leenes, y Irene Kamara (Cheltemham, UK: Edward Elgar Publishing, 2022), 240–69, https://doi.org/10.4337/9781800371682; Marcelo Drago, "Un antes y un después para los patrones oscuros", Idealex, 19 de junio de 2024, https://idealex.press/un-antes-y-un-despues-para-los-patrones-oscuros/.

La LPDP también tiene reglas especiales para los datos sensibles "relativos a la salud y el perfil biológico humano" (art. 16 bis) y los sensibles "de carácter biométrico" (art. 16 ter). Estos últimos son los datos "relativos a las características físicas, fisiológicas o conductuales de una persona que permitan o confirmen la identificación única de ella, tales como la huella digital, el iris, los rasgos de la mano o faciales y la voz" (art. 16 ter).

Respecto a todos estos datos sensibles, la LPDP establece que el consentimiento debe ser siempre "expreso" (arts. 16, 16 bis, 16 ter). Esta ley también agrega requisitos adicionales de información para los datos de carácter biométrico (art. 16 ter).

Por otra parte, la LPDP también regula de manera especial el consentimiento respecto del tratamiento de datos personales de niñas, niños y adolescentes (art. 16 quáter). Así, en el caso de los niños o niñas menores de 14 años el consentimiento debe ser otorgado por los padres o representantes legales. En cambio, en el caso de los adolescentes –personas naturales entre los 14 y 18 años– ellos mismos otorgan el consentimiento, con una excepción: si el adolescente es menor de 16 años y el tratamiento se refiere a datos personales sensibles, el consentimiento debe ser otorgado por sus padres o representantes legales.

1.3. Revocación consentimiento como fuente de licitud "débil"

Desde la perspectiva de los responsables, el consentimiento como fuente de licitud puede presentar ciertas dificultades. Una es que puede ser retirado por el titular:

> El titular puede revocar el consentimiento otorgado en cualquier momento y sin expresión de causa, utilizando medios similares o equivalentes a los empleados para su otorgamiento. La revocación del consentimiento no tendrá efectos retroactivos (art. 12 inc. 4).

Dado este carácter "débil" del consentimiento como fuente de licitud, los responsables tienen un interés en fundar el tratamiento de datos en otras fuentes de licitud.

2. Otras fuentes de licitud del tratamiento de datos (distintas al consentimiento)

Más allá del consentimiento del titular, la LPDP establece "otras fuentes de licitud del tratamiento de datos" en su art. 13. Cinco fuentes, específicamente, que revisaremos a continuación.

2.1. Obligaciones financieras, económicas, bancarias o comerciales

La LPDP permite el tratamiento de datos personales relativos a las obligaciones financieras, económicas, bancarias o comerciales, "incluidos los datos referidos a la situación socioeconómica del titular" (art. 13 inc. 1 letra a), en la medida que se someta a las reglas especiales que se encuentran en el Título III de la LPDP (arts. 17-19).

El Título III regula principalmente la comunicación de información sobre esas obligaciones que realiza un responsable de una base de datos a un tercero, junto a otros aspectos del tratamiento. La LPDP permite que se comuniquen las deudas bajo ciertas condiciones, por ejemplo, cuando constan en cheques protestados por falta de fondos (art. 17 inc. 1). Al mismo tiempo, la ley prohíbe la comunicación bajo ciertas condiciones,

por ejemplo, cuando se trata de información sobre deudas contraídas con responsables que prestan servicios de electricidad, agua, teléfono y gas (art. 17 inc. 2).

2.2. Ley

Se permite el tratamiento cuando éste es ordenado por la ley o resulta necesario para cumplir una obligación legal (art. 13 inc. letra b).

2.3. Contratos y negociaciones pre-contractuales

Se permite el tratamiento cuando es necesario para la celebración o ejecución de un contrato entre el titular y el responsable, o para la ejecución de medidas pre-contractuales (art. 13 inc. letra c).

2.4. Intereses legítimos del responsable o de un tercero

El responsable puede realizar tratamiento de datos personales para satisfacer "intereses legítimos del responsable o de un tercero, siempre que con ello no se afecten los derechos y libertades del titular" (art. 13 letra d). Esta regla permite que los responsables invoquen sus propios intereses para justificar el tratamiento no consentido. Al mismo tiempo, la regla exige que el responsable balancee sus intereses con los del titular.

Cuando la LPDP todavía era tramitada en el Congreso, los profesores Pablo Contreras y Pablo Trigo advirtieron que la expresión "intereses legítimos" presentaba una "alta indeterminación jurídica".[118] También indicaron que esta fuente presentaba el riesgo de una "merma significativa en la protección de los datos personales de un titular".[119]

El concepto de interés legítimo, lamentablemente, no fue definido en la LPDP. Esta ley se limita a mencionarlo como fuente de licitud, y a declarar que un tipo específico de tratamiento cumple con esta fuente (art. 16 quinquies inc. 1):

> Se entiende que existe un interés legítimo en el tratamiento de datos personales que realicen las personas naturales o jurídicas, públicas o privadas, incluidos los organismos públicos, cuando el tratamiento se realiza exclusivamente con fines históricos, estadísticos, científicos y para estudios o investigaciones, todos los cuales deben atender fines de interés público.

Clarificar el significado del interés legítimo será una importante tarea de la Agencia y los tribunales. En el derecho europeo, un ejemplo de tratamiento basado en el interés legítimo es "transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados".[120]

---

118 Ver Pablo Contreras y Pablo Trigo, "Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile", Revista Chilena de Derecho y Tecnología 8, nº 1 (2019): 74.
119 Ibid., 104. Ver también Pablo Contreras y Pablo Trigo, "¿Abriendo la caja de Pandora? El interés legítimo en la reforma a la Ley 19.628, sobre protección de la vida privada", Revista Chilena de Derecho y Tecnología 9, nº 1 (30 de junio de 2020): 185–206.
120 GDPR, considerando 48.

2.5. Defensa legal

Se permite el tratamiento cuando éste es necesario para la formulación, ejercicio o defensa de derechos ante los tribunales de justicia u otros órganos públicos (art. 13 inc. letra e).[121]

2.6. Fin de las "fuentes accesibles al público" como fuente de licitud

Una modificación importante introducida por la LDPD se refiere a lo que ésta llamaba "fuentes accesibles al público", es decir, "los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes".[122] La Ley 19.628 de 1999 establecía que algunos tipos de datos personales obtenidos de estas fuentes –por ejemplo, los "de carácter económico, financiero, bancario o comercial"– podían ser tratados sin la autorización del titular.[123] Es decir, la ley consideraba que el tratamiento a partir de estas bases de datos constituían una fuente de licitud alternativa al consentimiento. La amplitud de las fuentes accesibles al público como fuente de licitud –y su tensión con la autodeterminación informativa del titular– fue "uno de los aspectos más criticados de nuestra ley sobre protección de datos personales".[124]

En la LPDP las fuentes accesibles al público ya no son una fuente de licitud. En principio, esta ley las reconoce mediante la expresión "fuentes de acceso público" y la siguiente definición: "todas aquellas bases de datos o conjuntos de datos personales, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, tales como el Diario Oficial, medios de comunicación o los registros públicos que disponga la ley" (art. 2 letra i). Pero la LPDP agrega que "[e]l tratamiento de datos personales provenientes de fuentes de acceso público se someterá a las disposiciones de esta ley" (art. 2 letra i). Es decir, este tratamiento debe justificarse en las fuentes de licitud descritas en las secciones anteriores, y debe respetar los deberes del responsable que analizaremos en las próximas secciones.[125] Así, por ejemplo, el responsable que ha obtenido datos personales mediante el consentimiento del titular para agregarlos a una fuente de acceso público deberá limitarse a realizar tratamiento según la finalidad consentida por el titular.

Este cambio regulatorio puede tener implicancias importantes para el *web scrapping* y otras prácticas comunes en nuestra economía digital.[126]

121 Aunque los arts. 12 y 13 distinguen seis fuentes, se podría pensar que en realidad la LPDP simplemente contempla dos fuentes de licitud –el consentimiento y la ley– y que varias de las disposiciones que hemos resumido simplemente establecen reglas específicas que clarifican que una determinada hipótesis cuenta como una de esas dos fuentes. Por ejemplo, la regla sobre contratos y negociaciones pre-contractuales (art. 13 inc. 1 letra c) sería reconducible al consentimiento como fuente de licitud (art. 12). Esta discusión no es meramente conceptual. Puede tener consecuancias jurídicas. Por ejemplo, la interpretación recién planteada pordría permitir que el titular exija el fin del tratamiento de datos personales que el responsable ha justificado invocando la fuente de licitud sobre contratos, pese a que ella no menciona la revocación; en este caso, el titular podría apelar a la regla según la cual el consentimiento es revocable. Agradecemos a Danielle Zaror por esta observación.

122 Art. 2 letra i de la Ley 19.628 de 1999.

123 Ver art. 4 inc. 5 de la Ley 19.628 de 1999.

124 Francisco Alvarado Ávalos. "Las fuentes de acceso público a datos personales". Revista Chilena de Derecho y Tecnología 3, nº 2 (2014): 205–26, 219.

125 Además, la LPDP regula de manera específica algunos aspectos del tratamiento de datos personales contenidos en fuentes de acceso público a propósito del deber de secreto o confidencialidad de su art. 14 bis inc. 1, y las obligaciones del responsable de datos reguladas en su art. 14 inc. 1 letra b.

126 Ver Jaime Urzúa, "Las fuentes accesibles al público en el proyecto de ley de datos personales", Alessandri Abogados (blog), 19 de enero de 2024, https://alessandri.legal/las-fuentes-accesibles-al-publico-en-el-proyecto-de-ley-de-datos-personales/ ("Una de las áreas que con seguridad se verá afectada con el PDL [el proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (boletín 11.144-07)] es el web scrapping. Este se refiere a un proceso que permite la extracción de datos a gran escala desde páginas web por medio del uso de herramientas automatizadas. Obviamente el cambio normativo significará una gran transformación del modelo de negocios de muchas empresas que actualmente operan en base a esta técnica (pensemos en fintech, burós, suscriptores digitales, entre otros), ya que se les restringirá legalmente la forma en que podrán tratar los datos que extraen continuamente").

3. Fuentes de licitud del tratamiento de otras categorías de datos personales: sensibles, relativos a menores de edad, con fines históricos, estadísticos, científicos y de estudios o investigaciones, y de geolocalización

La LPDP contempla reglas especiales sobre fuentes de licitud del tratamiento (y otras aspectos del mismo) respecto de cuatro categorías adicionales de datos personales, alguno de los cuales tienen subcategorías: los datos personales sensibles (art. 16), los datos personales sensibles relativos a la salud del titular y su perfil biológico (art. 16 bis), los datos personales sensibles biométricos (art. 16 ter), los "datos personales relativos a los niños, niñas y adolescentes" (art. 16 quáter), los "datos personales con fines históricos, estadísticos, científicos y de estudios o investigaciones" (art. 16 quinquies), y los "datos de geolocalización" (art. 16 sexies).[127] Ya nos hemos referido a algunos de estos datos más arriba. [128]

4. Límites del modelo regulatorio del consentimiento y la autogestión

Si bien la LPDP reconoce fuentes de licitud distintas al consentimiento, ellas tienen un alcance limitado. En la práctica, el consentimiento es y será utilizado frecuentemente para justificar el tratamiento de datos personales. Este énfasis de la regulación en el consentimiento del titular –también presente en el GDPR y la regulación norteamericana– se conoce como el modelo del "*notice-and-choice*" (notificación y elección) o "modelo del control". Esta regulación busca aumentar el control de los usuarios sobre el tratamiento de sus datos personales. Como hemos visto, ese fue uno de los fines buscados por el legislador chileno.[129]

Sin embargo, en la práctica el modelo del control tiene un efecto pro-libertad limitado. El modelo descansa en la autogestión del titular: decisiones individuales, hechas posibles por la regulación, respecto de tratamientos individuales de datos personales. Pero es un hecho notorio que en el contexto de servicios digitales, como el acceso a páginas web y uso aplicaciones descargadas en *smart phones*, los usuarios tendemos a aceptar las políticas de privacidad sin detenernos a leerlas. Así, en la práctica, el consentimiento no es informado, o al menos no en el sentido fuerte de *información efectivamente conocida* por el usuario. La consecuencia de lo anterior es que, a menudo, los usuarios desconocen las consecuencias específicas y potencialmente negativas que puede tener el tratamiento de sus datos. Por ésta y otras razones, el consentimiento como fuente de licitud es a menudo una ficción legal.[130]

Con todo, esta observación no es una crítica a los usuarios. El problema no se resuelve llamando a la población a ser más celosos de sus datos, pues es imposible que los usuarios lean la multitud de políticas de privacidad a las que se enfrentan día a día.[131] Más bien, es una crítica al modelo regulatorio.

127 Además de estas categorías, la LPDP regula de manera especial los datos relativos a infracciones penales, civiles, administrativas y disciplinaria (art. 25), así como otros datos recolectados y tratados por el Estado (ver Título IV y Título VIII de la LPDP). Tal como señalamos en la Introducción, nuestro artículo no aborda las regulación del tratamiento realizado por órganos públicos.

128 Respecto al consentimiento y estas cuatro Ver arriba sección III.B.1.2.

129 Ver arriba sección II.A.

130 Para importantes críticas al paradigma del control en el derecho de la privacidad de datos, ver Daniel J. Solove, "Privacy Self-Management and the Consent Dilemma", Harvard Law Review 126 (2012): 1880–1903, traducido al español como Daniel J. Solove, "Autogestión de la privacidad y el dilema del consentimiento", Revista chilena de derecho y tecnología 2, nº 2 (2013): 11–47; Neil Richards, Why Privacy Matters (New York: Oxford University Press, 2022).

131 Ver Geoffrey A. Fowler, "I Tried to Read All My App Privacy Policies. It Was 1 Million Words.", Washington Post, 31 de mayo de 2022, https://www.washingtonpost.com/technology/2022/05/31/abolish-privacy-policies/; Brooke Auxier Turner Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica, "Americans' Attitudes and Experiences with Privacy Policies and Laws", Pew Research Center

La implicancia de la crítica es que una regulación de protección de datos robusta necesita ir más allá de la autogestión de intereses realizada por el titular. Necesita establecer deberes adicionales de los responsables. Afortunadamente, la LPDP va en esa dirección al establecer deberes como el de proteger los datos "desde el diseño y por defecto" (art. 14 quáter).[132] Es posible, y tal vez deseable, que la Agencia y reformas legales futuras profundicen esta tendencia.[133]

Sin perjuicio de lo anterior, en algunos casos las reglas sobre consentimiento de la LPDP pueden tener efectos positivos para la libertad de las personas. Como mínimo, ellas entregan a los consumidores la oportunidad de ejercer control en aquellos casos que consideran particularmente relevantes como para justificar la inversión de su tiempo y esfuerzo, y obligan al responsable a dejar un registro escrito del tratamiento que pretenden realizar y sus fines, lo cual puede ser más tarde utilizado por el titular y la Agencia para poner límites al tratamiento indiscriminado de datos personales.

C. Deberes adicionales de quienes tratan datos personales

La LPDP establece deberes adicionales a la exigencia de una fuente de licitud. La ley se refiere a estos deberes adicionales con diversas expresiones: "principios" (art. 3), "obligaciones del responsable de datos" (arts. 14), y "deber" (incluyendo cinco deberes en los arts. 14 bis a 14 sexies).

La utilización de esta diversidad de términos es cuestionable, pues todas las disposiciones mencionadas crean deberes del responsable. Pese a que la doctrina ha distinguido entre "reglas" y "principios" en algunos contextos (como el derecho constitucional),[134] no hay razones para pensar que la distinción haya sido adoptada por la LPDP; tampoco se observa en esta ley una distinción conceptual clara entre lo que llama "obligaciones" y "deberes", más allá del hecho de que aparecen en artículos distintos. Por lo tanto, nos referiremos a todas estas reglas bajo la etiqueta de "deberes adicionales del responsable". Ellas serán analizadas en esta sección.

Lo anterior no agota los deberes del responsable. En la sección siguiente (III.D) revisaremos lo que la LPDP llama "derechos del titular de datos personales";[135] estos derechos generan, a su vez, deberes correlativos del responsable de datos. Luego, en la sección subsiguiente (III.E) daremos cuenta de los deberes especiales del responsable en relación a la transferencia internacional de datos, junto a otras reglas especiales de comportamiento.[136] Y en la última sección de esta parte (III.F) menciona los deberes del responsable de

(blog), 15 de noviembre de 2019, https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/; Alexis C. Madrigal, "Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days", The Atlantic, 1 de marzo de 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/; Aleecia M. McDonald y Lorrie Faith Cranor, "The cost of reading privacy policies", I/S: A Journal of Law and Policy for the Information Society 4 (2008): 540–65.

132 Ver abajo sección III.C.

133 Para esfuerzos doctrinarios recientes en los EE.UU. que buscan articular un modelo regulatorio alternativo que enfatiza los deberes de los responsables más allá del consentimiento como fuente de licitud, ver Neil M. Richards y Woodrow Hartzog, "A Duty of Loyalty for Privacy Law", Washington University Law Review 99 (2022): 961–1021; Woodrow Hartzog y Neil M. Richards, "Legislating Data Loyalty", Notre Dame Law Review Reflection 97 (2022): 356–84; Daniel J. Solove, "The Myth of the Privacy Paradox", The George Washington Law Review 89 (2020): 1–51 ("La mejor manera de fortalecer la regulación de la privacidad es regularla de maneras que no dependan de que los individuos gestionen su propia privacidad, sino que se centren en regular la arquitectura que estructura la forma en que se utiliza, mantiene y transfiere la información"; íbid. 6, traducción de los autores).

134 Ver abajo nota 136.

135 Ver abajo sección III.D.

136 Ver abajo sección III.E.

evaluar riesgos y prevenir de infracciones, los cuales serán desarrollados en la parte IV.[137]

Finalmente, y como ya hemos observado, la LPDP contempla reglas especiales para el tratamiento de datos personales relacionados con obligaciones financieras, económicas, bancarias o comerciales,[138] datos sensibles, datos relativos a menores de edad, datos personales utilizados con fines históricos, estadísticos, científicos y de estudios o investigaciones, y datos personales de geolocalización.[139] Estas reglas contienen deberes del responsable, pero no las abordaremos aquí por razones de espacio.

1. Los "principios" del tratamiento de datos personales

La LPDP establece ocho "principios": (a) "de licitud y lealtad", (b) "de finalidad", (c) "de proporcionalidad", (d) "de calidad", (e) "de responsabilidad", (f) "de seguridad", (g) "de transparencia e información", y h) "de confidencialidad" (art. 3).

Por ejemplo, según el "principio de proporcionalidad", el responsable no debe tratar más datos que los "necesarios, adecuados y pertinentes en relación con los fines del tratamiento" (art. 3 letra c). Una vez que los datos han sido utilizados para ese fin, ellos deben ser "suprimidos o anonimizados" (art. 3 letra c). Así, los responsables deben minimizar la cantidad de datos personales que tratan; no pueden extraer y almacenar datos de sus consumidores de manera indiscriminada, sino sólo aquellos necesarios para alcanzar la finalidad del tratamiento que ha sido comunicada al momento de extraer los datos y que ha sido consentida por el titular. Este principio recibe el nombre de "minimización de datos" en el GDPR. [140]

¿Cuál es la naturaleza de los "principios" de la LPDP? Como ya adelantamos, pese a la terminología utilizada las disposiciones de "principios" no son principios en el sentido de mandatos de optimización que puedan ser balanceados con otros mandatos de optimización; tampoco son una mera lista de objetivos de política pública.[141] Al contrario, estos principios son reglas de comportamiento, es decir, mandatos definitivos que solamente admiten una aplicación binaria del tipo todo o nada, conforme a una operación lógica de subsunción. Específicamente, reglas de comportamiento que imponen deberes a los responsables.

Así lo sugiere el hecho de que cumplir los principios es, según la misma LPDP, una "obligación" del responsable (art. 14 inc. 1 letra e), que su incumplimiento constituye una "infracción" que genera responsabilidad (art. 34 inc. 1), y que la LPDP omite mencionar la posibilidad de que la autoridad de protección pondere los principios con otros intereses.

Con todo, varias de las reglas conducta contenidas en las disposiciones de "principios" de la LPDP tienen una relación género-especie con otras reglas conducta de la misma LPDP. Es decir, los contenidos de las primeras son concretizados en las segundas. Así, se podría pensar que los principios no solamente establecen deberes

137 Ver abajo secciones III.F. y IV.A.
138 Ver arriba sección III.B.2.
139 Ver arriba secciói III.B.3.
140 El art. 5.1(c) del GDPR dice: "Principios relativos al tratamiento 1. Los datos personales serán: (...) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)".
141 Para el concepto de principios como mandato de optimización, ver Robert Alexy, Teoría de los derechos fundamentales (Madrid: Centro de Estudios Constitucionales, 1993), 86–87; Robert Alexy, "On the Structure of Legal Principles", Ratio Juris 13, nº 3 (septiembre de 2000): 294–304.

del responsable: también pueden tener un rol pedagógico y tal vez orientar la interpretación de reglas más específicas que parecen desarrollarlos.

Por ejemplo, según el "principio de transparencia e información" el responsable "debe entregar al titular toda la información que sea necesaria para el ejercicio de los derechos que establece esta ley, incluyendo las políticas y las prácticas sobre el tratamiento de los datos personales" (art. 3 letra g). Más adelante el art. 14 de la LPDP –titulado "obligaciones del responsable"–[142] establece, entre otros, el deber del responsable de "informar" al titular sobre los "antecedentes que acrediten la licitud del tratamiento de datos que realiza" (art. 14 letra a). Y el art. 14 ter –titulado "deber de información y transparencia"– contiene más deberes específicos sobre información y transparencia, entre ellos los de mantener la política de privacidad en el sitio web del responsable (art. 14 letra a).[143]

2. "Obligaciones" del responsable

El art. 14 de la LPDP, titulado "obligaciones del responsable de datos", establece deberes del responsable en cinco letras. La disposición aclara que estos deberes existen "sin perjuicio de las demás disposiciones previstas en esta ley" (art. 14 inc. 1). Estos deberes son:

> a) Informar y poner a disposición del titular los antecedentes que acrediten la licitud del tratamiento de datos que realiza. Asimismo, deberá entregar de manera expedita dicha información cuando le sea requerida.
>
> b) Asegurar que los datos personales se recojan de fuentes de acceso lícitas con fines específicos, explícitos y lícitos, y que su tratamiento se limite al cumplimiento de estos fines.
>
> c) Comunicar o ceder, en conformidad a las disposiciones de esta ley, información exacta, completa y actual.
>
> d) Suprimir o anonimizar los datos personales del titular cuando fueron obtenidos para la ejecución de medidas precontractuales.
>
> e) Cumplir con los demás deberes, principios y obligaciones que rigen el tratamiento de los datos personales previstos en esta ley (art. 19 inc. 1).

Además, la misma disposición establece un deber especial del responsable que carece de domicilio en Chile y al mismo tiempo trata datos de residentes en territorio chileno: el deber de "señalar y mantener actualizado y operativo, un correo electrónico u otro medio de contacto idóneo para recibir comunicaciones de los titulares de datos y de la Agencia" (art. 14 inc. 2).

3. "Deberes" del responsable

Junto a los deberes del responsable que se encuentran en las disposiciones de los "principios" (art. 3) y de las "obligaciones del responsable" (art. 14), cinco artículos de la LPDP establecen, respectivamente, cinco deberes del responsable (o conjuntos de deberes) utilizando en su encabezado la expresión "deber". En

142 Ver también abajo sección III.C.2.
143 Ver también abajo sección III.C.3.

general, estas disposiciones desarrollan deberes de manera más detallada o específica que las dedicadas a los "principios" y las "obligaciones del responsable", tal como ya adelantábamos más arriba.

Específicamente, ellas establecen el "deber de secreto o confidencialidad" (art. 14 bis), el "deber de información y transparencia" (art. 14 ter, al cual ya hemos hecho referencia),[144] el "deber de protección desde el diseño y por defecto" (art. 14 quáter), el "deber de adoptar medidas de seguridad" (14 quinquies), y el "deber de reportar las vulneraciones a las medidas de seguridad" (14 sexies).

Por ejemplo, según el deber de adoptar medidas de seguridad (art. 14 quinquies), que concretiza el principio (deber) de seguridad (art. 3 letra f),[145] los responsables deben considerar varios factores al establecer estas medidas: "el estado actual de la técnica", "los costos de aplicación", "la naturaleza, alcance, contexto y fines del tratamiento", "la probabilidad de los riesgos", y "la gravedad de sus efectos en relación con el tipo de datos tratados" (art. 14 quinquies). La LPDP menciona algunas de las medidas técnicas y organizativas que constituyen medidas de seguridad apropiadas, por ejemplo, la "seudonimización y el cifrado de datos personales" (art. 14 quinquies letra a).[146]

Finalmente, la LPDP confía en la Agencia la tarea de regular, mediante instrucción general, las condiciones mínimas de cumplimiento de los deberes de información y de seguridad (art. 14 septies inc. 2). Al mismo tiempo, le ordena hacerlo considerando varios factores, incluyendo el tamaño de la organización del responsable.

D. Derechos de los titulares y deberes correlativos del responsable

Más allá de los deberes del responsable que hemos resumido –los asociados a las fuentes de licitud, los "principios", las "obligaciones", y los "deberes"–, el responsable está obligado a satisfacer los deberes correlativos a siete "derechos del titular de datos personales" (art. 4).

Estos son los derechos (a) de "acceso", (b) de "rectificación", (c) de "supresión", (d) de "oposición",[147] (e) a "oponerse y no ser objeto" de "[d]ecisiones individuales automatizadas, incluida la elaboración de perfiles", (f) de "bloqueo", y (g) a la "portabilidad de los datos personales" (arts. 5-9). Todos los derechos del titular se ejercen ante el responsable y, en caso de denegación, mediante una reclamación ante la Agencia; abordaremos estos procedimientos en otra sección de este trabajo.[148] A continuación resumimos los derechos del titular y sus deberes correlativos.

1. Derecho al acceso a datos personales

El responsable debe aclarar si está tratando datos personales del titular, además de darle acceso a esos datos, y explicar la naturaleza del tratamiento (art. 5).

144 Ver arriba sección III.C.1.
145 Art. 3 letra f LPDP: Principio de seguridad. En el tratamiento de los datos personales, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la naturaleza de los datos.
146 A su vez, el art. 14 sexies establece el "deber de reportar las vulneraciones a las medidas de seguridad".
147 Tradicionalmente la doctrina se ha referido a los primeros cuatro derechos del titular como los "derechos ARCO": acceso, rectificación, cancelación (que en la LPDP se llama supresión) y oposición.
148 Ver abajo sección IV.B.

2. Derecho a la rectificación de datos personales

El responsable debe rectificar datos inexactos, desactualizados o incompletos relativos al titular, y comunicar esta rectificación a otras personas a quienes haya comunicado o cedido los datos (art. 6).

3. Derecho a la supresión de datos personales

El responsable debe eliminar datos personales que están en su poder. Este derecho aplica sólo en algunos casos, por ejemplo, cuando el titular revoca su consentimiento y el responsable carece de otra fuente de licitud para tratar los datos (art. 7).

En la UE, una de las posiciones jurídicas que ha sido derivada del derecho supresión es el "derecho al olvido" digital. Es decir, un derecho a pedir la desindexación de datos de una persona en motores de búsqueda como Google.[149] Está por verse cómo esta experiencia comparada influenciará la interpretación de la regla chilena. La LPDP, a diferencia del GDPR, no menciona la palabra "olvido".[150]

4. Derecho a oponerse al tratamiento de datos personales

El responsable debe poner fin al tratamiento de datos personales en tres tipos de casos: (a) si el responsable trata los datos invocando como fuente de licitud la satisfacción de sus "intereses legítimos"; (b) si el tratamiento se realiza con el único fin de realizar marketing directo de bienes; (c) si los datos han sido obtenidos de una fuente de acceso público, sin que exista otra fuente de licitud del tratamiento (art. 8).

5. Derecho a oponerse a las decisiones individuales automatizadas

Este derecho es, como el anterior, un derecho de oposición al tratamiento de datos personales. El responsable debe poner fin a "decisiones basadas en el tratamiento automatizado de sus datos personales, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente" (art. 8 bis inc. 1). La LPDP define excepciones a este derecho (art. 8 inc. 2); por ejemplo, no aplica cuando existe consentimiento previo y expreso del titular (art. 8 bis inc. 2 letra b).

6. Derecho al bloqueo temporal del tratamiento de datos personales

Se refiere al deber del responsable de suspender temporalmente el tratamiento de los datos personales del titular. Este derecho sólo procede cuando la "exactitud" de los datos "no pueda ser establecida" o su "vigencia sea dudosa", y no sea aplicable el derecho de supresión (art. 8 ter).

149 Uno de los casos europeos sobre protección de datos personales más famosos se refiere precisamente al derecho al olvido digital. Ver Tribunal de Justicia de la Unión Europea (Gran Sala), Sentencia asunto C131/12, Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, 13 de mayo de 2014, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0131.

150 El GDPR establece una vinculación entre el derecho de supresión y la idea de "olvido" en el encabezado de su art. 17: "Derecho de supresión ('el derecho al olvido'). Sobre el derecho al olvido digital en Chile, ver Carlos Reusser, Derecho al olvido. La protección de datos personales como límite a las libertades informativas, 2da ed. (Santiago: Ediciones Der, 2021).

7. Derecho a la portabilidad de los datos personales

El responsable debe entregar una copia de los datos personales del titular que almacena, en un formato que permita que esos datos sean transferidos y utilizados por otro responsable (art. 9). El "derecho a la portabilidad de los datos personales" sólo aplica a datos personales cuyo tratamiento "esté basado en el consentimiento del titular" y "se realice en forma automatizada" (art. 9 letras b y a).

Aunque es probable que el legislador haya establecido este derecho de portabilidad de datos personales para contribuir a la autodeterminación informativa de los titulares, se trata de una institución que podría tener consecuencias para el derecho de la libre competencia. Según una interpretación, es posible que este derecho tenga un efecto positivo en este ámbito. Como ha explicado el profesor Maurice E. Stucke, "[l]a esperanza es que regulaciones de portabilidad de datos más estrictas reduzcan nuestros costos de cambio y nos proporcionen una mayor libertad".[151] En consecuencia, las grandes empresas de plataformas online que han acumulado grandes bases de datos personales "[t]endrán menos capacidad para encerrarnos y acaparar nuestros datos. Otras empresas, con estos datos, pueden ofrecer servicios personalizados. Los mercados pueden volverse más disputables. La innovación podría florecer a medida que otras empresas descubran el valor de nuestros datos".[152] Al mismo tiempo, hay razones para el escepticismo, como ha explicado el mismo profesor Stucke.[153]

Está por verse cuál será el impacto en nuestros mercados de la portabilidad de datos personales de la LPDP. La evaluación de este potencial impacto tendrá que considerar cómo esta regulación interactuará con otras que establecen portabilidad de datos personales (y otros datos), tal como la que establece la portabilidad financiera.[154]

E. Reglas especiales sobre cesión de datos personales, mandato de tratamiento, y transferencia internacional de datos personales

La LPDP contiene reglas especiales sobre la transferencia de datos personales desde un responsable a un tercero, así como el tratamiento realizado por éste. Hay reglas diferenciadas para la transferencia a otro responsable (la "cesión de datos personales"), la transferencia a un mandatario (o "encargado") y el tratamiento realizado por éste, y la transferencia internacional de datos personales.

1. Cesión de datos personales

La LPDP define la "cesión de datos personales" como la "transferencia de datos personales por parte del responsable de datos a otro responsable de datos" (art. 2 letra v). A su vez, establece deberes específicos asociados a esa cesión art. 15). Por ejemplo, la fuente de licitud de la cesión es el consentimiento, el cumplimiento y ejecución de un contrato del cual es parte el titular, y el "interés legítimo" del cedente o cesionario, o la ley (art. 15 inc. 1). Además, la cesión debe "constar por escrito o a través de cualquier medio electrónico idóneo" (art. 15 inc. 3).

151 Maurice E. Stucke, Breaking Away: How to Regain Control Over Our Data, Privacy, and Autonomy (New York: Oxford University Press, 2022), 158.
152 Ibid.
153 Ver ibid., 159-161.
154 Ver Ley N° 21.236 que Regula la Portabilidad Financiera, D.O. 9 junio 2020, https://www.bcn.cl/leychile/navegar?idNorma=1146340.

2. Tratamiento de datos a través de un mandatario

La LPDP define el "tercero mandatario o encargado" como "la persona natural o jurídica que trate datos personales, por cuenta del responsable de datos" (art. 2 letra x). La ley regula esta relación y los deberes del responsable y el encargado (art. 15 bis). Por ejemplo, el encargado debe realizar el tratamiento según las órdenes y para el objeto convenido con el responsable. Si el encargado no respeta este mandato, la ley lo considera responsable y queda sujeto a todas las obligaciones legales aplicables a estos sujetos, debiendo responder personalmente por las infracciones en que incurra, y solidariamente con el responsable respecto a los daños que cause (art. 15 bis inc. 2).

3. Reglas especiales sobre transferencia internacional de datos personales

Como ya hemos observado, en la economía digital es muy frecuente que los responsables realicen tratamiento de datos personales a territorios distintos a aquellos donde se encuentran sus titulares.[155] A menudo "las empresas tienen empleados, clientes, proveedores u otros socios comerciales en otras jurisdicciones", o "sus clientes, proveedores u otros socios comerciales los tienen".[156] Es más, según el significado técnico del concepto, basta con que una persona, utilizando un computador y una conexión a internet, acceda a datos personales que se encuentran en un servidor ubicado en un país extranjero para que exista "transferencia internacional de datos personales".[157]

La transferencia internacional de datos personales es objeto de un marco regulatorio especial en la LPDP, el cual complementa los deberes del responsable (o encargado) del tratamiento que ya hemos revisado en este trabajo, incluyendo las fuentes de licitud. Específicamente, la ley establece varias condiciones que permiten la transferencia internacional de datos (art. 27). El responsable solamente necesita cumplir con una de esas condiciones para que la transferencia se entienda autorizada por la ley.

Por ejemplo, el responsable puede transferir los datos si ha pactado, con la persona que recibe los datos en el extranjero, cláusulas contractuales en las cuales "se establezcan los derechos y garantías de los titulares, las obligaciones de los responsables y terceros mandatarios y los medios de control" (art. 27 letra b).
Otro ejemplo: la transferencia internacional está permitida si ella se realiza "a una persona, entidad u organización pública o privada, sujeta al ordenamiento de un país que proporcione niveles adecuados de protección de datos personales" (art. 27 letra a). Una regulación "adecuada" es aquella que, según la Agencia, cuenta con "estándares similares o superiores a los fijados en esta ley [la LPDP]" (art. 28).

Esta última disposición es similar a la regla del GDPR que motivó al legislador chileno a adoptar esta regulación europea como modelo. Ésta incentiva a otros países a adoptar regulaciones similares a la LPDP y, por lo tanto, similares también al GDPR. Por esta vía, el derecho chileno ha dado nueva fuerza al efecto Bruselas de la regulación europea sobre protección de datos personales, tal como ya explicamos.[158]

155 Ver arriba sección II.B.
156 Determann, Determann's Field Guide to Data Privacy Law: International Corporate Compliance, 30.
157 Ibid.
158 Sobre el impacto del requisito de adecuación del GDPR en la LPDP, y el efecto Bruselas, ver arriba secciones II.B y II.C.

F. Deberes relacionados con las instituciones de cumplimiento de la LPDP

La LPDP también incluye deberes de evaluación de impacto del tratamiento y de prevenir infracciones (arts. 15 ter y 48). Los abordaremos en la siguiente parte de este trabajo,[159] en la cual revisaremos el *enforcement* y otras instituciones de la LPDP que incentivan el cumplimiento de sus reglas de conducta.

IV. ENFORCEMENT Y OTRAS INSTITUCIONES DE CUMPLIMIENTO DE LA LPDP

Esta parte del trabajo resume cómo la LPDP regula el *enforcement* y otras instituciones de cumplimiento de sus reglas de conducta. Entre estos mecanismos institucionales se incluyen, por supuesto, la Agencia y las sanciones que puede imponer a los infractores de la ley.

La omisión de incentivos adecuados al cumplimiento fue una de las principales críticas que recibió la versión anterior de la Ley 19.628. Esta ley confió su implementación a la voluntad de los responsables y la iniciativa de los titulares, ejercida ante los mismos responsables y los tribunales. En efecto, la ley consagraba derechos ARCO a favor de los titulares, para que estos los ejercieran ante los responsables y los tribunales de justicia mediante una acción judicial conocida como "habeas data".[160] Además, la ley les reconocía una acción civil contra el responsable para obtener la indemnización de perjuicios por "el daño patrimonial y moral que causare [el responsable] por el tratamiento indebido de los datos", y la eliminación, modificación o bloqueo de datos.[161] Sin embargo, esta versión de la Ley 19.628 omitió consagrar una autoridad de control, es decir, una agencia administrativa especializada en la protección de datos personales. Esta omisión fue una de las críticas más frecuentes que recibió la ley de parte de la academia, la sociedad civil, y los legisladores de la LPDP. [162]

En contraste, la LPDP contempla y regula pormenorizadamente una amplia batería de instituciones que incentivan el cumplimiento de sus reglas de conducta. Estas instituciones incluyen varias formas de *compliance* (sección IV.A), las solicitudes de los titulares ante los responsables para ejercer sus derechos (sección IV.B), la fiscalización de la Agencia y la imposición de sanciones administrativas (sección IV.C), y las acciones civiles que buscan obtener indemnización de perjuicios ante los tribunales ordinarios (sección IV.D).

159 Ver abajo sección IV.A.
160 Ver arts. 12 a 16 Ley 19.628, versión pre-LPDP.
161 Art. 23 Ley 19.628, versión pre-LPDP.
162 Ver Mensaje LPDP, 3 ("La obsolescencia de algunos de sus criterios u orientaciones y la ausencia de una autoridad de control que den eficacia a la ley, son parte de un diagnóstico en el que existe un amplio consenso entre los actores políticos e institucionales, agentes económicos, medios de comunicación social y la ciudadanía en general"); Moción LPDP, 5-6. Remediar este déficit fue uno de los fines principales buscados por el legislador (ver ibid.). A su vez, la configuración de la autoridad de control y sus sanciones fue uno de los focos principales de la discusión legislativa. Por ejemplo, ahí se discutió latamente si la función debía ser entregada al Consejo Para la Transparencia o a un nuevo órgano. Ver María Paz Canales, "Chile necesita una regulación de protección de datos con dientes", Derechos Digitales, 12 de julio de 2019, https://www.derechosdigitales.org/13443/proteccion-de-datos-con-dientes/. Ver también Consejo para la Transparencia, "Comisión de Constitución del Senado aprobó al Consejo para la Transparencia (CPLT) como autoridad a cargo de la protección de datos personales", Consejo para la Transparencia (blog), 6 de agosto de 2019, https://www.consejotransparencia.cl/comision-de-constitucion-del-senado-aprobo-al-consejo-para-la-transparencia-cplt-como-autoridad-a-cargo-de-la-proteccion-de-datos-personales/.

A. Compliance: evaluación de impacto en casos de alto riesgo para los derechos de los titulares, modelo certificado de prevención de infracciones, y deber general de prevenir infracciones

Es común que los responsables busquen prevenir infracciones mediante una evaluación de los riesgos de infracción de la ley asociados al tratamiento que realizan o pretenden realizar, y la adopción de medidas destinadas a prevenir o minimizar ese riesgo. Aquí nos referimos a estas acciones pro-cumplimiento como "compliance", en la medida que su actor principal es el responsable, sin perjuicio de que el derecho pueda canalizarla e incluso exigirla. La LPDP reconoce y promueve la compliance, regulando requisitos y procedimientos, y estableciendo incentivos a su favor.

Específicamente, La LPDP regula dos instrumentos de compliance:

Primero, la ley establece lo que llama una "evaluación de impacto en protección de datos personales" para tratamientos que tienen un "alto riesgo" potencial para los derechos de los titulares. Esta institución incluye una evaluación en sentido estricto –un análisis del tratamiento y sus riesgos– y medidas de mitigación. Realizarla es una obligación del responsable: su incumplimiento acarrea altas sanciones (sección IV.A.1).

Segundo, la LPDP regula un "modelo de prevención de infracciones". Esta forma de compliance es aplicable a todo tipo de tratamientos de datos personales, y también incluye una evaluación de riesgos y medidas de mitigación. Sus elementos son regulados de manera más detalla que la primera forma de compliance. Aunque la LPDP declara que la adopción de un modelo de prevención de infracciones es voluntaria, la ley incentiva su adopción de varias maneras, incluyendo efectos atenuantes sobre las sanciones (sección IV.A.2).

Más allá de estas formas de compliance, la LPDP contempla un deber general de prevenir infracciones. En la práctica, es posible que este deber incentive la adopción generalizada de programas de compliance por parte de los responsables (sección IV.A.3).

La Agencia jugará un rol importante –aunque secundario– en estas formas de compliance. Este órgano deberá guíar su implementación y administrar incentivos a su adopción. Por esta razón, esta sección enmarca las instituciones de compliance de la LPDP en la idea de "gobernanza colaborativa", un modelo regulatorio que también se encuentra en el GDPR (sección IV.A.4).

1. Evaluación de impacto del tratamiento de datos personales en casos de alto riesgo potencial para los derechos de los titulares

El primer tipo de compliance de la LPDP que revisamos es la "evaluación de impacto en protección de datos personales" (art. 15 ter). Más específicamente, ella se refiere a los tratamientos que puedan "producir un *alto riesgo* para los derechos" de los titulares (art. 15 ter inc. 1, énfasis agregado). Bajo esta condición, es un deber de los responsables el realizar esta forma de compliance.

¿Qué tipo de tratamientos de datos personales pueden crear un alto riesgo para los derechos de los titulares? Definir los tipos de operaciones que tienen esta naturaleza será una tarea de la Agencia (art. 15 ter inc. 3). Pero

la ley identifica cuatro hipótesis en las cuales siempre se necesita una evaluación de impacto (art. 15 ter inc. 2). Por ejemplo, exige evaluación cuando el tratamiento es "masivo" o "a gran escala" (art. 15 ter inc. 2 letra d), o "implique observación o monitoreo sistemático de una zona de acceso público" (art. 15 ter inc. 2 letra c)

La "evaluación de impacto" incluye "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" (art. 15 ter inc. 2). Considerando estos criterios, la Agencia debe publicar "orientaciones mínimas para realizar esta evaluación" (art. 15 ter inc. 3).

Los responsables que omiten hacer esta evaluación cuando es debida incurrirán en una "infracción gravísima" de la LPDP (art. 34 quáter letra k). Así, los infractores de este deber se exponen a las sanciones más altas contempladas por esta ley.[163]

2. Modelo de prevención de infracciones certificado por la Agencia

El segundo tipo de compliance regulado por LPDP es lo que ella denomina "modelo de prevención de infracciones" (art. 49), y que según la misma "consis[te] en un programa de cumplimiento" (art. 49 inc. 1). Este programa, como veremos, incluye una evaluación de riesgos y la adopción acciones que sirvan para prevenir esos riesgos. También supone el nombramiento de un "delegado de protección de datos personales".

Los responsables pueden adoptar este programa "voluntariamente", pero su adopción genera beneficios importantes para el responsable (más allá de minimizar el riesgo de infracción de la ley).[164] La Agencia juega un rol muy importante en esta forma de compliance, pues tiene la facultad de "[c]ertificar, registrar y supervisar los modelos de prevención de infracciones" y administrar el registro público en el cual ellos son publicados (art. 30 bis letra m). En ese sentido, el modelo de prevención de infracciones no es un mero programa de compliance del responsable, sino que es certificado por la Agencia.[165]

La LPDP regula varios aspectos de los modelos de prevención, los cuales serán resumidos a continuación. Al mismo tiempo, la LPDP confía la regulación de sus "requisitos, modalidades y procedimientos para la implementación, certificación, registro y supervisión" a un reglamento del Ministerio de Hacienda (art. 51 inc. 3).

2.1. Elementos mínimos del modelo de prevención de infracciones

La LPDP establece siete "elementos" que el programa, "al menos", debe contener (art. 49 inc. 2). Los agruparemos en tres categorías: (a) el delegado de protección de datos, (b) la evaluación de los riesgos legales del tratamiento, y (c) regulación y acciones para prevenir los riesgos.

163 Sobre la responsabilidad administrativa y las infracciones gravísimas, ver abajo sección IV.C.3.

164 Sobre este instrumento de compliance, ver también Ivonne Bueno, "Próxima Protección de Datos Personales en Chile: Ad Portas de un Nuevo Compliance", EstadoDiario, 8 de mayo de 2024, https://estadodiario.com/columnas/proxima-proteccion-de-datos-personales-en-chile-ad-portas-de-un-nuevo-compliance/.

165 Por lo tanto, el modelo de cumplimiento certificado por la Agencia es una institución análoga al sistema de evaluación de impacto ambiental contemplado por la Ley N° 19.300 sobre Bases Generales del Medio Ambiente. Una diferencia importante entre ambas insituciones es que mientras el modelo de cumplimiento de la LPDP es voluntario, las evaluaciones y declaraciones de impacto ambiental son obligatorias.

(a) *Delegado de protección de datos personales*. El responsable debe designar un "delegado de protección de datos personales" y definir "sus medios y facultades" (art. 49 inc. 2 letras a y b).[166] El delegado es la persona encargada de liderar el cumplimiento de las reglas de conducta de la LPDP dentro de la organización del responsable. La ley define las funciones mínimas que debe cumplir (art. 50 inc. 10 letras a-h). Por ejemplo, debe "[i]nformar y asesorar al responsable de datos, a los terceros encargados o mandatarios y a los dependientes del responsable, respecto de las disposiciones legales y reglamentarias relativas al derecho a la protección de los datos personales y a la regulación de su tratamiento" (art. 50 inc. 10 letra a).

El delegado debe ser alguien con experticia en la regulación sobre protección de los datos personales (art. 50 inc. 6), y debe tener "autonomía respecto de la administración, en las materias relacionadas con esta ley" (art. 50 inc. 3). Es "designado por la máxima autoridad directiva o administrativa del responsable de datos" (art. 50 inc. 2). No es necesario que la protección de datos sea su función exclusiva (art. 50 inc. 4). Tampoco es necesario que sea un empleado del responsable. Estas últimas características del delegado hacen posible que su función sea externalizada a estudios de abogados y empresas consultoras.

Un grupo empresarial puede designar un delegado para algunas o todas las empresas que controla (art. 50 inc. 5). En el caso de las micro, pequeñas y medianas empresas, el cargo puede ser asumido por su dueño o alguna de sus máximas autoridades (art. 50 inc. 3).

(b) *Evaluación de riesgos*. Además de designar un delegado de protección de datos, la empresa debe evaluar si el tratamiento de datos que realiza o espera realizar presenta riesgos legales, es decir, en qué medida podría infringir las reglas de conducta de la LPDP. Para ello, debe identificar el ámbito territorial del tratamiento, caracterizar los datos personales tratados y sus titulares, e identificar actividades del responsable "en cuyo contexto se genera o incremente el riesgo de comisión" de las infracciones leves, graves o gravísimas de la LPDP (art. 49 inc. 2 letra c-d).[167]

(c) *Regulación y acciones para prevenir infracciones*. Tras identificar los riesgos legales del tratamiento, el responsable debe crear una regulación interna para prevenirlos. Esta regulación consiste en reglas de conducta internas (art. 49 inc. 2 letra e), mecanismos de reporte interno y reporte a la Agencia (art. 49 inc. 2 letra f), procedimientos de fiscalización internos (art. 49 inc. 2 letra g), sanciones internas (art. 49 inc. 2 letra g), y la formalización de esta regulación en el reglamento interno del responsable o los contratos de trabajo y contratos con terceros que prestan servicios al responsable (art. 49 inc. 3).

2.2. Certificación del modelo de prevención

El responsable debe someter el modelo de prevención del art. 49 a una revisión de la Agencia. Esta entidad está "encargada de certificar que el modelo de prevención de infracciones reúna los requisitos y elementos establecidos en la ley y su reglamento y supervisarlos" (art. 51 inc. 1).[168] Los responsables que han obtenido

166 Es lo que se conoce, en inglés, como "data protection officer" –en Europa– o "data privacy officer" –en los EE.UU.– (o, por sus siglas, como DPO).
167 Estas infracciones son definidas, respectivamente, en los artículos 34 bis, 34 ter y 34 quáter. Sobre ellas, ver arriba sección IV.C.3.
168 El reglamento sobre los modelos de prevención debe ser "expedido por el Ministerio de Hacienda y suscrito por el Ministerio Secretario General de la Presidencia y por el Ministro de Economía, Fomento y Turismo" (art. 51 inc. 3), a partir de una propuesta de la Agencia (art. 30 letra h).

estos certificados deben ser incorporados por la Agencia en un registro público, gratuito y en línea conocido como el "Registro Nacional de Sanciones y Cumplimiento" (arts. 2 letra z, 30 letra m, 39, 51 inc. 2).

La certificación tiene una duración de tres años (art. 52 inc. 1), pero puede quedar sin efecto por varias razones (art. 52), una de las cuales es la "revocación efectuada por la Agencia" (art. 52 inc. 1 letra a). La revocación (regulada en el art. 53) procede "si el responsable no da cumplimiento a lo establecido en este Párrafo" (art. 53 inc. 1). El párrafo en cuestión –el párrafo 5º del Título VII de la LPDP– establece las reglas que hemos mencionado en esta sección, así como un deber general de prevenir infracciones (art. 48, al cual volveremos más abajo).[169] La disposición agrega que "[c]on este objeto, la Agencia podrá requerir toda aquella información que fuere necesaria para el ejercicio de sus funciones" (art. 53 inc. 1).[170] Es más, la Agencia deberá "supervisar" el cumplimiento de los modelos de prevención que ha certificado (art. 30 bis letra m). Así, el responsable no sólo debe presentar ante la Agencia un documento que describa el programa de cumplimiento, sino también tomar las acciones descritas en el mismo, a riesgo de que la Agencia revoque su certificación e imponga otras sanciones.

2.3. Voluntariedad del modelo de prevención e incentivos a su adopción

La LPDP establece que "[l]os responsables de datos podrán *voluntariamente* adoptar un modelo de prevención de infracciones" (art. 49 inc. 1, énfasis agregado). Pese a la naturaleza voluntaria del modelo certificado la ley incentiva su adopción de varias maneras.

Primero, la adopción de un modelo de prevención constituye una circunstancia atenuante que la Agencia debe considerar al fijar multas por incumplimiento de la LPDP (art. 37 inc. 1 Nº 8 y 36 inc. 1 Nº 5).

Segundo, como ya explicamos, los modelos de prevención de infracciones que han sido certificados por la Agencia serán publicados por ésta en el "Registro Nacional de Sanciones y Cumplimiento". Esta publicación es un incentivo al modelo de prevención pues puede ser usada por los responsables para fines de marketing. Es probable que los responsables que obtengan la certificación y quieran "competir en privacidad" hagan referencia a aquélla en sus ofertas de productos y servicios. En la teoría económica ésta es una forma de "*signaling*": la certificación permite reducir la asimetría de información entre el responsable y quienes desean contratar con el mismo (por ejemplo, potenciales titulares), respecto a lo que sucede al interior de la organización del responsable.

Tercero, contar con un modelo certificado de prevención de infracciones debería facilitar que el responsable efectivamente evite realizar infracciones a la LPDP y, así, evite que sea objeto de multas y otras sanciones.

Cuarto, contar con ese modelo y actuar acorde al mismo debería facilitar el cumplimiento del deber de prevenir infracciones que abordaremos en la siguiente subsección (art. 48), y cuya infracción que puede ser sancionada por la Agencia.

169 El párrafo 5º del Título VII también regula la responsabilidad civil por daños patrimoniales y extrapatrimoniales causados al titular por el responsable (art. 47). No es claro cómo esta disposición se relaciona con la revocación de la certificación de un modelo de prevención de infracciones.

170 Constituye una infracción gravísima "[e]ntregar, a sabiendas, información falsa, incompleta o manifiestamente errónea en el proceso de registro o certificación del modelo de prevención de infracciones" (art. 34 quáter letra j).

Quinto, es posible que la adopción de un modelo de cumplimiento también sea considerada por los tribunales de justicia en el contexto de la determinación de responsabilidad civil.[171]

Ya que los responsables que cuenten con un modelo de prevención de infracciones certificado por la Agencia podrán obtener beneficios (o minimizar costos) relacionados con la reputación corporativa, las sanciones impuestas por la Agencia, y la responsabilidad civil, entre otros, es posible que la adopción de estos modelos se transforme en una práctica frecuente de los responsables.

3. Deber general de prevenir infracciones: ¿un deber general de compliance?

La LPDP establece un deber general de prevenir infracciones a esta ley:

> Prevención de infracciones. Los responsables de datos, sean personas naturales o jurídicas, públicas o privadas, *deberán adoptar acciones destinadas a prevenir la comisión de las infracciones* establecidas en los artículos 34 bis, 34 ter y 34 quáter (art. 48, énfasis agregado).

La infracción a este deber es, en sí misma, una infracción a la LPDP que puede generar sanciones, incluyendo multas impuestas por la Agencia.[172] ¿Cómo cumplirán los responsables con el deber general de prevenir infracciones? ¿Qué tipo de acciones serán útiles para acreditar su cumplimiento ante la Agencia? Para estos efectos, probablemente será útil contar con documentos que analicen los riesgos del tratamiento y den cuenta de medidas de prevención que la organización espera realizar, así como la debida implementación estas medidas y documentos que den cuenta de ella. Es decir, acciones similares a las contempladas por las formas de compliance que ya hemos descrito, a saber, el modelo certificado de prevención de infracciones, y la evaluación de impacto del tratamiento de datos personales en casos de alto riesgo potencial para los derechos de los titulares.

Así, si bien el deber de evaluación de impacto solo se refiere a hipótesis específicas de alto riesgo para los derechos de las personas, y si bien el modelo certificado es voluntario, es posible que –como consecuencia del marco regulatorio de estos instrumentos y del deber general de prevenir infracciones– en la práctica los responsables, de manera generalizada, desarrollen programas de compliance.

4. Compliance como gobernanza colaborativa

Al reconocer y promover la compliance, y establecer que la Agencia jugará un rol crucial en su implementación –incluso certificando algunos programas– la LPDP ha adoptado un modelo regulatorio de "gobernanza colaborativa" que ya se encuentra en el GDPR.[173] Este modelo ha sido descrito de la siguiente manera por la

171 De acuerdo al art. 47 inc. 2°, los procesos judiciales civiles son posteriores y suponen una decisión sancionatoria de la Agencia. Así, es probable que si la Agencia ha atenuado el monto de una multa en base a la existencia de un programa de cumplimiento certificado, la defensa de los demandados presente este antecedente en el proceso judicial.

172 La infracción de este deber de prevención del art. 48 constituye, en principio, una infracción "leve" por aplicación de la regla de clausura del art. 34 bis letra f ("Cometer cualquier otra infracción a los derechos y obligaciones establecidas en esta ley, que no sea calificada como una infracción grave o gravísima"). Sin embargo, es posible que algunas conductas que lo infringen sean subsumibles en otras reglas sobre infracciones y, por lo tanto, que ellas sean calificadas como infracciones "graves" o "gravísimas".

173 Sobre este modelo regulatorio, ver Margot E. Kaminski, "Binary governance: Lessons from the GDPR's approach to algorithmic accountability", Southern California Law Review 92 (2018): 1529–1616; Meg Leta Jones y Margot E. Kaminski, "An American's Guide to the GDPR", Denver Law Review 98, nº 1 (2020): 93–128; Ari Ezra Waldman, "The New Privacy Law", UC Davis Law Review 55 (2021): 19–42. Sobre sus

profesora Margot E. Kaminski:

> La gobernanza colaborativa, o "nueva gobernanza", utiliza alianzas público-privadas para alcanzar fines públicos de gobernanza. La gobernanza colaborativa no debe confundirse con la autorregulación, aunque puede incluir o incluso depender en parte sustancial de la gobernanza privada. En su forma ideal, la gobernanza colaborativa no implica intervención ni desregulación. Existe en un espectro entre la regulación tradicional de comando y control, y el ordenamiento privado, y la gobernanza colaborativa puede emplear aspectos significativos de cada uno.[174]

Por ejemplo, esto significa que los responsables contratan los servicios de "profesionales de *compliance*—profesionales de la privacidad, abogados de la privacidad, y otros expertos en *compliance*—que acercarán el derecho a sus organizaciones, traducirán sus requisitos a sus superiores, y lo implementarán en toda la empresa".[175] Y que estas actividades se realizarán en "diálogo con los reguladores", tal como la Agencia.[176] Instituciones de este tipo ya se encuentran en el GDPR,[177] lo cual puede explicar que también hayan sido incluidas en la LPDP.

B. Ejercicio de derechos de los titulares ante los responsables y la Agencia (u

Como ya hemos explicado, la LPDP reconoce los derechos de los titulares al acceso, rectificación, supresión y bloqueo de datos, entre otros derechos, y estos derechos son fuente de deberes correlativos de los responsables.[178] En esta sección enfatizaremos otro aspecto de los derechos del titular: su rol como institución de cumplimiento de la LPDP. Específicamente, abordaremos cómo la LPDP regula el procedimiento mediante el cual el titular ejerce estos derechos ante el responsable (sección IV.B.1), así como el procedimiento de tutela de derechos ante la Agencia que el titular puede utilizar cuando, a su juicio, la respuesta (u omisión de respuesta) del responsable ha infringido la ley (sección IV.B.2).

1. Procedimiento para solicitar ante el responsable el cumplimiento de los derechos del titular

El responsable no sólo debe cumplir con los deberes correlativos a los derechos del titular cuando éste se lo pida, sino que, además, debe crear una infraestructura de comunicación que facilite el envío y recepción de solicitudes. Por ejemplo, debe contar con "mecanismos y herramientas tecnológicas que permitan que el titular ejerza sus derechos en forma expedita, ágil y eficaz", y los medios deben ser "sencillos en su operación" y "gratuitos para el titular" (art. 10 incs. 3 y 4). En la práctica, es probable que ello se traduzca a menudo en proporcionar una dirección de correo electrónico para recibir este tipo de solicitud.

La LPDP también regula pormenorizadamente los requisitos que debe cumplir el titular al enviar una solicitud al responsable (arts. 11 inc. 1 letras a-b).

Una vez que ha recibido una solicitud, el responsable debe acusar recibo y luego responder dentro de quince días hábiles desde su ingreso (art. 11 inc. 2). El responsable puede denegar total o parcialmente la satisfacción de

desafíos de implementación dentro de las empresas, ver Ari Ezra Waldman, Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power (Cambridge: Cambridge University Press, 2021).

174 Kaminski, "Binary governance", 1559.
175 Waldman, "The New Privacy Law", 26.
176 Kaminski, "Binary governance", 1596.
177 Para una descripción de las reglas relevantes del GDPR, ibid.,1595-1610.
178 Ver arriba sección III.E.

un derecho, pero debe hacerlo "indicando la causa invocada y los antecedentes que la justifican" (art. 11 inc. 4).

Además, en su solicitud el titular puede pedir, de manera fundada, el bloqueo temporal del tratamiento de sus datos, aunque solamente si el derecho ejercido es de rectificación, supresión u oposición. Esta solicitud accesoria debe ser respondida en un plazo de dos días hábiles (art. 11. inc. 6).

La LPDP contempla sanciones para los responsables que incumplen este procedimiento.[179] Un responsable que omite responder a la solicitud del titular o entrega respuestas incompletas o fuera de plazo comete una infracción leve (art. 34 bis letra c), o una infracción grave (art. 34 ter letra f) si se trata de solicitudes fundadas de bloqueo temporal del tratamiento de datos personales la infracción es grave.

Además, es infracción grave el "[i]mpedir u obstaculizar el ejercicio legítimo de los derechos de acceso, rectificación, supresión, oposición o portabilidad del titular" (art. 34 ter letra e). Finalmente, la LPDP tiene una regla de clausura que establece que "cualquier otra infracción a los derechos" del titular establecidos en la Ley serán consideradas como infracciones "leves" (art. 34 bis letra g).

Estas sanciones son impuestas por la Agencia en su procedimiento sancionatorio. Este procedimiento probablemente será gatillado por el procedimiento de tutela de derechos del titular que describimos a continuación.

2. Procedimiento ante la Agencia de tutela de derechos del titular

Si el responsable deniega alguna de las solicitudes del titular o no las responde oportunamente, el titular puede reclamar ante la Agencia (art. 11 incs. 5 y 6, y art. 41). Esta última, a su vez, puede iniciar un procedimiento de investigación denominado "procedimiento administrativo de tutela de derechos" (art. 41), que es un procedimiento adversarial que involucra al responsable y al titular como partes y a la Agencia como adjudicador del conflicto.

Un responsable que incumple la decisión de la Agencia que resuelve el conflicto se expone a altas sanciones: es infracción gravísima el "[i]ncumplir una resolución de la Agencia que resuelve la reclamación de un titular sobre el ejercicio de sus derechos de acceso, rectificación, supresión, oposición, portabilidad o bloqueo temporal" (art. 34 quater letra i). En cuanto a los medios de impugnación, tanto el titular como el responsable pueden reclamar contra la decisión de la Agencia ante cortes de apelaciones (art. 43).[180]

Si la Agencia considera que el responsable no ha respetado los derechos del titular y ha cometido una infracción a la LPDP, ella puede iniciar el procedimiento sancionatorio que describiremos en la próxima sección (art. 41 inc. 2 letra f y art. 42).

C. Agencia de Protección de Datos Personales, Fiscalización y Sanciones

A lo largo de este trabajo ya hemos aludido repetidamente al rol de la Agencia como fiscalizador del cumplimiento de la LPDP y algunas de las sanciones que puede imponer a los infractores de esta ley. En esta

179 Respecto a las sanciones asociadas a los distintos tipos de infracciones, ver abajo sección IV.C.3.
180 Sobre este procedimiento judicial, ver abajo IV.C.4

parte profundizaremos en la estructura orgánica y funciones de la Agencia, el procedimiento administrativo por infracción de ley, y la naturaleza de las sanciones. También describiremos el procedimiento judicial mediante el cual los responsables y otros actores pueden reclamar contra las resoluciones de la Agencia.

1. Agencia de Protección de Datos Personales

1.1. Descripción general y función general de la Agencia

La LPDP define a la Agencia como una

> corporación autónoma de derecho público, de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio, que se relacionará con el Presidente de la República a través del Ministerio de Economía, Fomento y Turismo (art. 30 inc. 1).

La Agencia tiene la siguiente función:

> velar por la efectiva protección de los derechos que garantizan la vida privada de las personas y sus datos personales, de conformidad a lo establecido en la presente ley, y fiscalizar el cumplimiento de sus disposiciones (art. 30 inc. 2).

1.2. Estructura orgánica de la Agencia

La Agencia es dirigida por su Consejo Directivo (art. 30 ter). Éste se conforma por "tres consejeros, designados por el Presidente de la República, con acuerdo del Senado, adoptado por los dos tercios de sus miembros en ejercicio" (art. 30 quáter inc. 1).

El cargo de consejero es de dedicación exclusiva (art. 30 quinquies), dura seis años sin posibilidad de una nueva designación, y se renueva individualmente cada dos años (art. 30 quáter inc. 5).[181] Quienes lo ocupan "deberán ser personas de reconocido prestigio profesional o académico en materias de protección de datos personales" (art. 30 quáter inc. 3). Su remuneración es equivalente a la de un Subsecretario de Estado (art. 30 septies). Los tres consejeros eligen, entre sus miembros, al presidente y vicepresidente de la Agencia (art. 30 quáter inc. 4). El Consejo toma sus decisiones por la mayoría de sus miembros; su quorum mínimo para sesionar es de dos consejeros (art. 30 quáter inc. 7).

La LPDP regula detalladamente las inhabilidades e incompatibilidades de los consejeros (art. 30 quinquies), su remoción y causales de cesación (art. 30 sexies), remuneración (art. 30 septies), y las funciones y atribuciones de su presidente (art. 30 nonies). Los consejeros pueden ser removidos por la Corte Suprema por "incapacidad, mal comportamiento o negligencia manifiesta en el ejercicio de sus funciones", a petición

181 Sin embargo, los primeros tres consejeros de la Agencia durarán en sus cargos 2, 4 y 6 años, respectivamente; deberán ser nombrados dentro de los 60 días anteriores a la entrada en vigencia de la LPDP; y asumirán sus cargos junto a la entrada en vigencia de la LPDP. Ver disposiciones transitorias, art. cuarto, del proyecto de ley, aprobado por el Congreso, boletín Nº 11.144-07, Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (refundido con el boletín 11.092-07) (2017), 27 agosto 2024, http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07.

"del Presidente de la República o de la Cámara de Diputados mediante acuerdo adoptado por simple mayoría, o a petición de quince diputados" (art. 30 sexies inc. 1).

La LPDP también establece un mecanismo de coordinación regulatoria de la Agencia con el Consejo para la Transparencia (art. 31), define el marco regulatorio del personal de la Agencia (art. 32), y la naturaleza de su patrimonio (art. 32 bis).

El Presidente de la República debe dictar los Estatutos de la Agencia –en base a una propuesta de ésta– mediante un decreto supremo del Ministerio de Economía, Fomento y Turismo (art. 30 octies).

1.3. Facultades de la Agencia

Para cumplir con su función, la Agencia cuenta con facultades de diversa naturaleza (art. 30 bis inc. 1 letras a-n): (a) dictar instrucciones y normas generales para regular el tratamiento de datos personales, (b) aplicar e interpretar reglas legales e infra-legales sobre protección de datos personales, (c) fiscalizar el cumplimiento de esas reglas, (d) determinar sus infracciones, (e) sancionar a sus infractores, (f) resolver solicitudes y reclamos de los titulares (en el procedimiento administrativo de tutela de derechos que ya hemos resumido),[182] (g) educar al público sobre la protección de sus datos personales, (h-l) colaborar con y aconsejar a una amplia gama de autoridades y organizaciones privadas o públicas, nacionales, extranjeras e internacionales, (m) certificar programas de compliance y administrar el Registro Nacional de Sanciones y Cumplimiento, y (n) otras facultades que le encomiende la ley.

1.4. ¿Expansión de las facultades de la Agencia? El proyecto que regula los sistemas de inteligencia artificial

En mayo del año 2024 el Congreso empezó a tramitar un proyecto de ley que regula los "sistemas de inteligencia artificial".[183] El proyecto busca establecer reglas de conducta y una institucionalidad para estos sistemas. En este último ámbito, el proyecto pretende expandir las facultades de la Agencia: "[l]a fiscalización y el cumplimiento de las disposiciones de esta ley [sobre sistemas de inteligencia artificial] y su reglamento corresponderá a la Agencia" (art. 19), es decir, la "Agencia encargada de la Protección de Datos" (art. 4 inc. 2). Si el proyecto se convierte en ley, la Agencia se convertirá en un regulador de los responsables del tratamiento de datos personales y de los oferentes de sistemas de inteligencia artificial.

182 Ver arriba sección IV.B.

183 Proyecto que regula los sistemas de inteligencia artificial, boletín Nº 16.821-19 (2024), refundido con el proyecto boletín Nº 15.869-19 (2023) (matriz), https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=17429&prmBOLETIN=16821-19. Según la versión original propuesta por el Presidente de la República el 7 de mayo de 2024, el proyecto de ley "regula a proveedores, implementadores, importadores y distribuidores de sistemas de inteligencia artificial" (art. 2). Este concepto de sistema de inteligencia artificial es definido como un "sistema basado en máquinas que, por objetivos explícitos o implícitos infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales. Los distintos sistemas de IA pueden variar en sus niveles de autonomía y adaptabilidad tras su implementación" (art. 3 número 1). El objeto del proyecto de ley es "promover la creación, desarrollo, innovación e implementación de sistemas de inteligencia artificial ("IA") al servicio del ser humano, que sean respetuosos de los principios democráticos, el Estado de Derecho y los derechos fundamentales de las personas frente a los efectos nocivos que determinados usos pudieran irrogar" (art. 1).

2. Procedimiento administrativo por infracción de ley

La Agencia ejerce sus potestades fiscalizadoras, de determinación de infracciones y sancionatorias mediante el así llamado "procedimiento administrativo por infracción de ley" (art. 42). Este procedimiento busca determinar infracciones a cualquiera de "los principios establecidos en el artículo 3º, derechos y obligaciones establecidas en esta ley" (art. 42).

La Agencia inicia el procedimiento de oficio o a petición de parte (art. 42 letra b). En comparación con los procesos judiciales, el procedimiento administrativo por infracción de ley es un proceso relativamente corto, con una duración máxima de seis meses. La Agencia cuenta con "amplias facultades para solicitar antecedentes o informes" al responsable del tratamiento de datos personales (art. 42 letra i). También puede "citar a declarar, entre otros, al titular, a los representantes legales, administradores, asesores y dependientes de quien trate datos personales", entre otras personas (art. 30 bis d). El responsable cuenta con oportunidades para presentar sus descargos y antecedentes (art. 42 letra e).

La Agencia debe poner fin al procedimiento mediante una resolución fundada, la cual puede contemplar sanciones de la naturaleza que detallamos en la próxima sección (art. 42 letras j y k). El responsable y otros actores pueden reclamar contra la resolución que pone fin al procedimiento ante los tribunales, como también explicaremos más abajo.[184]

3. Sanciones administrativas

3.1. Descripción general de las sanciones y medidas relacionadas con ellas

¿Qué sanciones pueden ser impuestas por la Agencia? La LPDP distingue entre las "sanciones" a secas, que incluyen la amonestación escrita y diversos tipos de multas (art. 35), y las "sanciones accesorias", que se refiere la suspensión temporal (pero renovable), total o parcial, del tratamiento de datos personales, y que aplica a casos especiales de multas por infracciones gravísimas reiteradas (art. 38).

Además, al imponer estas sanciones la Agencia puede exigir que la empresa cumpla con "medidas tendientes a subsanar las causales que dieron motivo a la sanción" en un plazo acotado (art. 35 inc. 2; ver también art. 38 inc. 2); su incumplimiento puede afectar el monto de las multas impuestas y la naturaleza de la suspensión.

Finalmente, la Agencia siempre debe anotar la infracción y al infractor en el "Registro Nacional de Sanciones y Cumplimiento" (art. 39), lo cual también se puede considerar como una sanción.

3.2. Infracciones

La LPDP establece 31 tipos infraccionales (arts. 34 bis, ter, y quáter). Ellas dicen relación con el incumplimiento las reglas de conducta que ya hemos analizado en este trabajo.

184 Ver abajo sección IV.C.4.

La ley clasifica estas infracciones "atendida a su gravedad" (art. 34). Específicamente, seis "infracciones leves" (art. 34 bis),[185] catorce "infracciones graves" (art. 34 ter),[186] y once "infracciones gravísimas" (art. 34 quáter).[187] La clasificación es relevante para determinar las sanciones aplicables a quienes incurren en una infracción, tal como explicaremos más abajo.

Las tres categorías –infracciones leves, graves y gravísimas– no son definidas por la LPDP. Ésta se limita a definir infracciones específicas dentro de cada categoría. Sin embargo, a partir del contenido de cada conjunto de infracciones es posible inducir algunas características generales o parcialmente generales de cada categoría.[188]

La mayoría de las infracciones gravísimas son infracciones de la LPDP realizadas con dolo. Por ejemplo, "[o]mitir en *forma deliberada* la comunicación de las vulneraciones a las medidas de seguridad que puedan afectar la confidencialidad, disponibilidad o integridad de los datos personales" (art. 34 quáter letra f; énfasis agregado). Este elemento de dolo no es mencionado en las infracciones leves y graves. Además, la mayoría de las infracciones gravísimas se pueden entender como infracciones dolosas a las reglas de la LPDP sobre "principios" (art. 3).[189] Por ejemplo, el principio de finalidad (art. 3 letra b) parece ser recogido en la infracción gravísima de "[d]estinar maliciosamente los datos personales a una finalidad distinta de la consentida por el titular o prevista en la ley que autoriza su tratamiento" (art. 34 quáter letra b).

185 Art. 34 bis LPDP: Se consideran infracciones leves, las siguientes: a) Incumplimiento total o parcial del deber de información y transparencia, establecido en el artículo 14 ter. b) Carecer de la individualización del domicilio postal, correo electrónico o medio electrónico equivalente que permita comunicarse con el responsable de datos o su representante legal, actualizado y operativo, a través del cual los titulares de datos puedan dirigir sus comunicaciones o ejercer sus derechos. c) Omitir la respuesta, responder en forma incompleta o fuera de plazo, las solicitudes formuladas por el titular de datos en conformidad a esta ley. d) Omitir el envío a la Agencia de las comunicaciones previstas obligatoriamente en esta ley o sus reglamentos. e) Incumplimiento de las instrucciones generales impartidas por la Agencia en los casos que no esté sancionado como infracción grave o gravísima. f) Entregar información incompleta en el proceso de registro o certificación del modelo de prevención de infracciones. g) Cometer cualquier otra infracción a los derechos y obligaciones establecidas en esta ley, que no sea calificada como una infracción grave o gravísima.

186 Art. 34 ter LPDP: Se consideran infracciones graves, las siguientes: a) Tratar los datos personales sin contar con el consentimiento del titular de datos o sin un antecedente o fundamento legal que otorgue licitud al tratamiento, o tratarlos con una finalidad distinta de aquélla para la cual fueron recolectados. b) Comunicar o ceder datos personales, sin el consentimiento del titular, en los casos en que dicho consentimiento sea necesario, o comunicar o ceder los datos para un fin distinto del autorizado. c) Efectuar tratamiento de datos personales innecesarios en relación con los fines del tratamiento vulnerando lo dispuesto en el literal c) del artículo 3°. d) Tratar datos personales inexactos, incompletos o desactualizados en relación con los fines del tratamiento, salvo que la actualización de estos datos corresponda al titular en virtud de la ley o el contrato. e) Impedir u obstaculizar el ejercicio legítimo de los derechos de acceso, rectificación, supresión, oposición o portabilidad del titular. f) Omitir la respuesta, responder tardíamente o denegar la petición sin causa justificada, en los casos de solicitudes fundadas de bloqueo temporal del tratamiento de datos personales de un titular. g) Realizar tratamiento de datos personales de niños, niñas y adolescentes con infracción a las normas previstas en esta ley. h) Realizar tratamiento de datos personales sin cumplir los requisitos establecidos para las personas jurídicas de derecho privado sin fines de lucro y cuya finalidad sea política, filosófica, religiosa, cultural, sindical o gremial, respecto de los datos de sus asociados. i) Vulnerar el deber de secreto o confidencialidad establecido en el artículo 14 bis. j) Vulnerar o infringir las obligaciones de seguridad en el tratamiento de los datos personales establecidas en el artículo 14 quinquies. k) Omitir las comunicaciones o los registros en los casos de vulneración de las medidas de seguridad establecidas en el artículo 14 quinquies. l) Adoptar medidas de calidad y seguridad insuficientes o no idóneas para el tratamiento de datos personales con fines históricos, estadísticos o científicos y para estudios o investigaciones que atiendan fines de interés público. m) Realizar operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley. n) Incumplir una resolución o un requerimiento específico y directo que haya impartido la Agencia.

187 Art. 34 quáter LPDP: Se consideran infracciones gravísimas, las siguientes: a) Efectuar tratamiento de datos personales en forma fraudulenta. b) Destinar maliciosamente los datos personales a una finalidad distinta de la consentida por el titular o prevista en la ley que autoriza su tratamiento. c) Comunicar o ceder, a sabiendas, información no veraz, incompleta, inexacta o desactualizada sobre el titular de datos. d) Vulnerar el deber de secreto o confidencialidad sobre los datos personales sensibles y datos personales relativos a la comisión y sanción de infracciones penales, civiles, administrativas y disciplinarias. e) Tratar, comunicar o ceder, a sabiendas, datos personales sensibles o datos personales de niños, niñas y adolescentes, en contravención a las normas de esta ley. g) Efectuar tratamiento masivo de datos personales contenidos en registros electrónicos de infracciones penales, civiles, administrativas y disciplinarias, que llevan los organismos públicos, sin contar con autorización legal para ello. h) Realizar a sabiendas operaciones de transferencia internacional de datos en contravención a las normas previstas en esta ley. i) Incumplimiento de una resolución de la Agencia que resuelve la reclamación de un titular sobre el ejercicio de sus derechos de acceso, rectificación, supresión, oposición, portabilidad o bloqueo temporal. j) Entregar, a sabiendas, información falsa, incompleta o manifiestamente errónea en el proceso de registro o certificación del modelo de prevención de infracciones. k) Incumplir la obligación establecida en el artículo 15 ter, en los casos que corresponda.

188 Agradecemos a Ivonne Bueno por esta observación y las que son desarrolladas en los siguientes párrafos.

189 Sobre estos principios ver arriba sección III.C.1.

Esa vinculación a los principios es compartida por varias infracciones graves, pero sin una referencia al dolo.

Finalmente, las infracciones leves también omiten una referencia al dolo y tienden a referirse al incumplimiento de reglas procedimentales. Por ejemplo, la infracción leve de "[o]mitir el envío a la Agencia de las comunicaciones previstas obligatoriamente en esta ley o sus reglamentos" (art. 34 bis letra d).[190] Con todo, las infracciones leves también pueden referirse a principios y otras reglas sustantivas, en la medida que son infracciones leves los incumplimientos de derechos, obligaciones e instrucciones generales de la Agencia que no constituyen infracciones graves o gravísimas (art. 34 bis letras e y g).

3.3. Resumen de sanciones

La siguiente tabla resume las sanciones en principio aplicables a las infracciones leves, graves y gravísimas, respectivamente, indicando rangos de montos de multas; específicamente, montos máximos.

Infracciones	Sanciones	Equivalencias aproximadas[191]	
		Pesos (en millones)	Dólares (EE.UU.)
Leves (art. 34 bis)	Amonestación escrita, o	—	—
	Multa de hasta 5.000 unidades tributarias mensuales	$33 M	US$357.000
	Anotación en registro público (complemento necesario de la amonestación o multa)	—	—
Graves (art. 34 ter)	Multa de hasta 10.000 unidades tributarias mensuales	$666 M	US$714.000
	Anotación en registro público (complemento necesario de la multa)	—	—

190 Una excepción es la del art. 34 bis letra a ("Incumplir total o parcial el deber de información y transparencia, establecido en el artículo 14 ter"), que se relaciona con el "principio de transparencia e información" (art. 3 letra g).

191 Las equivalencias utilizan como referencia el valor de una unidad tributaria mensual de noviembre de 2024, es decir, $66.628 (ver Servicio de Impuestos Internos, "UTM - UTA - IPC 2024" (2024), UTM Noviembre, disponible en https://www.sii.cl/valores_y_fechas/utm/utm2024.htm); a su vez, se asume que el valor de dólar de los EE.UU. en pesos es $933.41 (según datos disponibles en https://g.co/finance/USD-CLP al 8 de octubre de 2024).

Gravísimas (art. 34 quáter)	Multa de hasta 20.000 unidades tributarias mensuales	$1.332 M	US$1.428.000
	Sanción accesoria: suspensión total o parcial del tratamiento (en caso de reincidencia reiterada en periodo de 24 meses).	—	—
	Anotación en registro público (complemento necesario de la multa)		

Tabla 1. Sanciones aplicables a las infracciones leves, graves y gravísimas

3.4. Multas y su determinación

La tabla 1 ya resumió los montos máximos que en principio son aplicables a cada tipo de infracción según su gravedad. Pero estos no son los únicos factores relevantes para determinar las multas. Las multas pueden exceder los montos máximos que se encuentran en la tabla en tres tipos de casos, tal como explicaremos a continuación. Tras hacerlo, revisaremos criterios generales de determinación de multas, y un límite a la responsabilidad de las empresas de menor tamaño contemplado para el primer año de vigencia de la LPDP.

(a) I*ncumplimiento de medidas de subsanación de infracciones*. Si el responsable no adopta las medidas señaladas por la Agencia para subsanar sus infracciones, la Agencia le debe imponer un recargo del 50% de la multa cursada (art. 35 inc. 2). Por ejemplo, si la Agencia impuso la multa máxima de una infracción leve (5.000 UTM), la Agencia podría imponer una multa total de 7.500 UTM.

(b) *Infracción con reincidencia*. Si el responsable infractor es además reincidente –"cuando el responsable ha sido sancionado en dos o más ocasiones, en los últimos treinta meses, por infracción a esta ley" mediante "resoluciones firmes o ejecutoriadas" (art. 36 inc. 2)– la Agencia puede aumentar el monto "hasta tres veces el monto asignado a la infracción cometida" (art. 35 inc. 3). Ocupando el mismo ejemplo anterior, la Agencia podría multar a un reincidente que comete una infracción leve con la multa máxima de 15.000 UTM.

(c) *Infracción grave o gravísima con reincidencia cometida por una empresa de mayor tamaño*. Esta hipótesis es un caso especial de la infracción con reincidencia que acabamos de abordar. Si el responsable es una empresa de mayor tamaño –si es "una empresa distinta a aquéllas definidas como empresas de menor tamaño" en la Ley 20.416[192]–, y la infracción es grave o gravísima, y ha habido reincidencia de infracciones

192 La lectura de la Ley 20.416, Fija Normas Especiales para las Empresas de Menor Tamaño, muestra que el aumento de multas de la LPDP que discutimos es aplicable a las empresas cuyos ingresos anuales excedan las 100.000 unidades tributarias mensuales (aproximadamente $6.663 millones o US$ 7,13 millones, según los valores mencionados en la nota 174). La Ley 20.416 establece que el concepto de "empresas de menor tamaño" incluye a las "microempresas", las "pequeñas empresas", y las "medianas empresas" (art. 2 inc. 1); a su vez, esa ley define estos tipos de empresas de la siguiente manera (art. 2 inc. 2): "Son *microempresas* aquellas empresas cuyos ingresos anuales por ventas y servicios y otras actividades del giro no hayan superado las 2.400 unidades de fomento en el último año calendario; *pequeñas empresas*, aquellas cuyos ingresos anuales por ventas, servicios y otras actividades del giro sean superiores a 2.400 unidades de fomento y no exceden de 25.000 unidades de fomento en el último año calendario, y *medianas empresas*, aquellas *cuyos ingresos anuales*

graves o gravísimas –en el sentido del art. 36 inc. 2: dos o más sanciones por infracciones en los últimos treinta meses–, la Agencia puede imponer una sanción ocupando como techo el máximo que resulte de la aplicación, por separado, de los siguientes dos métodos (art. 35 inc. 4).

El primer método consiste en multiplicar el máximo de la infracción por tres (art. 35 inc. 4). Es decir, es el rango de multa contemplado para la infracción con reincidencia que ya hemos explicado (art. 35 inc. 3).

El segundo método consiste en un porcentaje de los "ingresos anuales por ventas y servicios y otras actividades del giro en el último año calendario" del responsable. Específicamente, 2% para infracciones graves y 4% para infracciones gravísimas (art. 35 inc. 4).

Si los dos métodos (tripe de multa y porcentaje) producen techos de distinto monto, el techo más alto (la multa "más gravosa") constituye el máximo monto de la multa que puede imponer la Agencia para este tipo especial de reincidencia.

(d) *Criterios generales de determinación del monto de las multas*. Como ya hemos observado, los montos de las multas son montos máximos. La LPDP se limita a establecer a techos, dejando a la Agencia la tarea de determina el monto preciso "prudencialmente".

Al mismo tiempo, la LPDP establece varios criterios que la Agencia debe considerar en su decisión prudencial (art. 37 inc. 1 Nº 1-7): (1) la gravedad de la conducta, (2) la falta de diligencia (a menos que este criterio ya sea parte del tipo), (3) el perjuicio causado en general y especialmente el número de titulares, (4) el beneficio económico obtenido mediante la infracción, (5) si el tratamiento versó sobre datos personales sensibles o datos personales de niños, niñas y adolescentes, (6) la capacidad económica del responsable infractor y (7) la reincidencia previamente sancionada por la Agencia en las mismas circunstancias.

Además, la Agencia debe considerar un conjunto de circunstancias atenuantes y agravantes (art. 37 inc. 1 Nº 8). Las atenuantes incluyen (a) las acciones de reparación, (b) la colaboración con la Agencia, (c) la ausencia de sanciones previas impuestas al responsable para la misma circunstancia, (e) la autodenuncia ante la Agencia, y (f) la adopción previa de un modelo de prevención de infracciones certificado ella, tal como ya mencionamos en la sección sobre compliance (art. 36 inc. 1).[193]

Por su parte, las agravantes son (a) la reincidencia del responsable (cuando éste ha sido sancionado por infracción de ley en dos o más ocasiones en los últimos 30 meses), (b) el carácter continuado de la infracción y (c) "[e]l haber puesto en riesgo la seguridad de los derechos y libertades de los titulares en relación a sus datos personales" (art. 36 inc. 2).

Si una misma conducta configura dos o más infracciones, o cuando una infracción es un medio para otra, la Agencia solo puede imponer una multa, ocupando como máximo el de la infracción más grave. En cambio, si hay dos o más conductas infraccionales independientes, la Agencia puede aplicar múltiples multas (art. 37 inc. 2).

por ventas, servicios y otras actividades del giro sean superiores a 25.000 unidades de fomento y *no exceden las 100.000 unidades de fomento en el último año calendario*" (énfasis agregado). La expresión "empresa de mayor tamaño" no se encuentra en la Ley 20.416 y la utilizamos para fines meramente pedagógicos.

193 Ver arriba IV.A.2.

(e) *Límite a las sanciones para las empresas de menor tamaño*. Durante el primer año de vigencia de la LPDP, la Agencia solamente podrá aplicar como sanción la mera amonestación por escrito y anotación en el Registro Nacional de Sanciones y Cumplimiento para las "empresas calificadas como de menor tamaño, de acuerdo a las categorías establecidas en el artículo segundo de la ley N° 20.416".[194] Es decir, una sanción que en principio solo es aplicable a las infracciones leves –la amonestación– puede ser utilizada por la Agencia como sanción para las infracciones graves y gravísimas, en reemplazo de las multas.

3.5. Sanción accesoria: suspensión temporal (pero renovable) del tratamiento de datos personales

Más allá de las multas, la LPDP contempla como "sanción accesoria" la suspensión temporal, parcial o total, del tratamiento de datos personales. Esta sanción puede ser aplicada por la Agencia cuando "se impongan multas por infracciones gravísimas reiteradas, en un período de veinticuatro meses" (art. 38 inc. 1), a menos que la suspensión afecte "los derechos de los titulares" (art. 38 incs. 2). La suspensión del tratamiento no alcanza al almacenamiento de datos (es decir, el responsable no debe eliminar los datos).

La duración de la suspensión es de un máximo de 30 días (art. 38 inc. 2). Pero la Agencia puede prorrogar la suspensión, "indefinidamente, por períodos sucesivos de máximo treinta días" (art. 38 inc. 4), si el responsable no adopta "las medidas necesarias con el objeto de adecuar sus operaciones y actividades a las exigencias dispuestas en la resolución que ordenó la suspensión" (art. 38 inc. 3).

3.6. Anotación de la infracción y el infractor en el Registro Nacional de Sanciones y Cumplimiento

Cuando la Agencia constata una infracción a la LPDP e impone una sanción, ella debe dejar constancia de la infracción y del infractor en el Registro Nacional de Sanciones y Cumplimiento. Como ya mencionamos, se trata de un registro en línea, público, de acceso gratuito, y administrado por la Agencia (art. 39 inc. 1). La anotación debe consignar el responsable sancionado, el tipo de infracción (leve, grave o gravísima), la infracción, las circunstancias atenuantes o agravantes, y la sanción (art. 39 inc. 2). Esta anotación queda a disposición del público por cinco años (art. 39 inc. 3).[195]

Esta anotación en el Registro Nacional de Sanciones y Cumplimiento es una sanción, en la medida que puede afectar negativamente la reputación de un responsable.[196]

4. Reclamo judicial de ilegalidad contra la resolución de la Agencia

Las decisiones sobre infracciones y sanciones de la Agencia son susceptibles de impugnación mediante un procedimiento judicial. Las personas "interesadas" pueden interponer, ante los tribunales de justicia, un reclamo de ilegalidad contra la resolución de la Agencia que resuelve el procedimiento sancionatorio o que

194 Disposiciones transitorias, art. sexto, del proyecto de ley, aprobado por el Congreso, boletín Nº 11.144-07, Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (refundido con el boletín 11.092-07) (2017), 27 agosto 2024, http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07.

195 En el registro también se deben "consignar los responsables que adopten modelos certificados de prevención de infracciones, con carácter vigente" (art. 39 inc. 2). Sobre estos modelos y sus certificados, ver arriba sección IV.A.2.

196 Ver Bueno, "Próxima Protección de Datos Personales en Chile". La misma LPDP sugiere que la anotación en el registro es una sanción, pues la regula en su Título VII, cuyo nombre es "De las infracciones y sus sanciones, de los procedimientos y de las responsabilidades".

lo paraliza (art. 43 inc. 1). Este procedimiento se conoce como el "procedimiento de reclamo de ilegalidad".

El tribunal competente es la Corte de Apelaciones de Santiago o bien la Corte de Apelaciones correspondiente al domicilio del reclamante, a elección de este último (art. 43). La LPDP regula las etapas de este procedimiento de reclamación judicial, remitiéndose para algunos efectos al Código de Procedimiento Civil y al Código Orgánico de Tribunales (art. 43). Por ejemplo, el término probatorio se rige por las reglas sobre incidentes del Código de Procedimiento Civil (art. 43 letra d).

Cuando el reclamo busca impugnar la resolución de la Agencia que resuelve el procedimiento sancionatorio (por ejemplo, imponiendo multas), el tribunal competente tiene potestad para "confirmar o revocar la resolución impugnada, establecer o desechar la comisión de la infracción (...) y, mantener, dejar sin efecto o modificar la sanción impuesta al responsable" (art. 43 letra g).

Es probable que este mecanismo sea utilizado por los responsables para impugnar las sanciones, así como también por titulares que consideran que la Agencia ha sido muy "tímida" al sancionar (o no sancionar) a un responsable.

D. Responsabilidad civil: acción de indemnización de perjuicios

Según la LPDP, los titulares de datos personales tienen un derecho a acudir a los tribunales civiles, en un procedimiento sumario, para obtener que el responsable indemnice "el daño patrimonial y extrapatrimonial" causado por la infracción de un principio, derecho u obligación de la LPDP (art. 47).

Para ejercitar la acción indemnizatoria el titular debe cumplir con algunos presupuestos de carácter procesal. La acción sólo es procedente si el titular reclamó por la infracción ante la Agencia y ésta "resolvió favorablemente el reclamo" (art. 47 inc. 2).[197] Además, vale la pena recordar que si la infracción se refiere a los derechos del titular la reclamación ante la Agencia solamente es procedente tras agotar el procedimiento de ejercicio de derechos ante el responsable; en este caso, el titular necesita haber pasado por el responsable y la Agencia antes de poder acudir a los tribunales.[198] Finalmente, si la resolución de la Agencia fue impugnada –por ejemplo, por el responsable– ante una Corte de Apelaciones en el procedimiento de reclamo de ilegalidad,[199] el titular debe esperar a que el tribunal lo resuelva antes de accionar civilmente (art. 47 inc. 2).

La disposición que acabamos de resumir (el art. 47 inc. 2) presenta algunos desafíos interpretativos. La norma omite abordar expresamente algunos escenarios de litigación posibles. Su texto completo dice:

> La acción indemnizatoria señalada en el inciso anterior podrá interponerse una vez ejecutoriada la resolución que resolvió favorablemente el reclamo interpuesto ante la Agencia o la sentencia se encuentre firme y ejecutoriada, en caso de haber presentado un reclamo de ilegalidad, y se tramitará de conformidad a las normas del procedimiento sumario establecidas en los artículos 680 y siguientes del Código de Procedimiento Civil.

De la lectura del texto normativo, es claro que el titular puede accionar civilmente si cuenta con una resolución

197 Sobre el procedimiento ante la Agencia ver arriba sección IV.C.2.
198 Sobre el procedimiento de ejercicio de derechos ante el responsable ver arriba sección IV.B.1.
199 Sobre el procedimiento de reclamo judicial ver arriba IV.C.4.

favorable de la Agencia y una sentencia judicial que también es favorable, es decir, que resuelve el reclamo de ilegalidad a favor de la Agencia. También pareciera que el titular puede accionar civilmente si la resolución de la Agencia fue *desfavorable* pero el tribunal declaró que está era ilegal, de manera favorable al titular. Pero, ¿puede el titular accionar civilmente si la sentencia judicial que resuelve el reclamo de ilegalidad es *desfavorable* al titular?

En cualquier caso, que el titular deba cumplir con pasos previos antes de demandar judicialmente la indemnización de perjuicios puede valorarse de manera positiva o negativa. Por un lado, es un desincentivo a la litigación frívola o temeraria. Además, la intervención de la Agencia puede jugar a favor del titular: sus decisiones pueden motivar al responsable a mejorar la protección de datos personales, y la investigación y resolución de la Agencia pueden aportar evidencia, análisis jurídico, y argumentos de autoridad que sean favorables al titular en el juicio civil. Por otro lado, los pasos previos pueden ralentizar la satisfacción del legítimo interés del titular en obtener compensación por daños relacionados con un derecho fundamental.

V. OTRAS REGULACIONES SOBRE DATOS PERSONALES Y SU RELACIÓN CON LA LPDP

La LPDP interactuará con un cúmulo regulatorio que incluye no solo el derecho de la libre competencia, sino también derechos constitucionales y decisiones de tribunales que resuelven procesos iniciados mediante la acción constitucional de protección (sección V.A), las regulaciones sectoriales, por ejemplo, de salud, financiera y de telecomunicaciones (sección V.B), y la regulación sobre ciberseguridad (sección V.C), entre otras. Todas ellas regulan aspectos del tratamiento de datos personales. La subsección V.B.3 discutirá, además, las reglas de la LPDP y otras leyes que se refieren a la relación entre la Agencia y los órganos sectoriales. Con todo, nuestro fin aquí no es ofrecer un tratamiento comprehensivo de estas materias; ello es imposible en los confines de este trabajo. En cambio, buscamos sensibilizar a la lectora o lector respecto del contexto regulatorio de la LPDP y la respuesta que ella da a los potenciales conflictos de normas y de competencia que se puedan suscitar.

A. Derechos fundamentales y protección de datos personales

Como ya se anticipó, la Constitución Política de la República se refiere al tratamiento de datos personales en su catálogo de derechos.[200] Lo hace de manera general y expresa en el art. 19° Nº 4, y a propósito un tipo específico de datos personales y de manera menos directa en el art. 19 Nº 1. En ambos casos, la Constitución habilita a los particulares a utilizar la acción constitucional de protección –el "recurso de protección"– frente a eventuales infracciones de los derechos (art. 20). Infracciones que, según el texto constitucional y la práctica asentada chilena, pueden provenir no sólo del Estado, sino que también de los particulares.

1. El derecho constitucional a la protección de los datos personales y el mandato de regulación de su tratamiento

Desde el año 2018, el art. 19 Nº 4 inc. 1 de la Constitución garantiza el derecho de las personas a "la

200 Ver arriba sección II.A.

protección de sus datos personales". La disposición agrega que "[e]l tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley". Todo lo anterior fue agregado al derecho al "respeto y protección a la vida privada y a la honra de la persona y su familia", que ya era parte de la Constitución al momento de la reforma.[201]

Como ya observamos al resumir los fines generales de la LPDP, esta ley buscó cumplir con el mandato constitucional dirigido al legislador. En efecto, la misma LPDP establece una vinculación a la norma constitucional en su art. 1:

> La presente ley tiene por objeto regular la forma y condiciones en la cual se efectúa el tratamiento y protección de los datos personales de las personas naturales, en conformidad al artículo 19 N° 4 de la Constitución Política.

Por otra parte, la reforma constitucional de 2018 hizo extensiva la la acción constitucional del art. 20 Constitución al derecho a la protección de los datos personales. Esta acción permite acudir a la corte de apelaciones competente para que adopte "de inmediato las providencias que juzgue necesarias para restablecer el imperio del derecho y asegurar la debida protección del afectado", cuando ha habido "actos u omisiones arbitrarios o ilegales" que causan "privación, perturbación o amenaza en el legítimo ejercicio" al derecho a "la protección de sus datos personales".

¿Cuál es el contenido del derecho constitucional a la protección de los datos personales en el contexto de la acción de protección? Según la historia de la reforma constitucional de 2018, tal como ha sido explicada por el profesor Pablo Contreras, el legislador constitucional buscó "constitucionalizar las facultades conocidas como derechos 'ARCO', esto es, los derechos de acceso, rectificación, cancelación y oposición".[202]

Si bien la versión de la Ley 19.628 anterior a la LPDP ya contaba con una acción judicial para hacer valer esos derechos –la acción de *habeas data*– en la práctica ésta ha sido poco utilizada.[203] En contraste con la habeas data, el recurso de protección es una acción judicial de tramitación relativamente breve, y a su alero se ha desarrollado una industria de servicios legales. El objetivo de la reforma constitucional fue aprovechar las ventajas de la acción constitucional de protección para favorecer el resguardo de los datos personales.

---

201 Ley 21.096 consagra el derecho a protección de los datos personales, 2018. Sobre la reforma constitucional ver arriba sección II.A.

202 Contreras, "El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena", 94.94.","plainCitation":"Contreras, "El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena", 94.","noteIndex":147},"citationItems":[{"id":41116,"uris":["http://zotero.org/users/1504437/items/FQ34NDAR"],"itemData":{"id":41116,"type":"article-journal","abstract":"The paper examines the recognition of the right to the protection of personal data as a fundamental right in the Chilean Constitution. To this end, it reviews the legislative history of the constitutional amendment and the main debates that took place. In particular, three dilemmas are reviewed: first, the need to constitutionalize or not informational self-determination as a fundamental right; second, the normative density required to constitutionalize the right; and, third, the legal relationship of entitlement or ownership over personal data. The text concludes by anticipating two challenges for the legal regulation of the right: first, regarding the type of constitutional referral to the legislator to protect personal data and, second, the jurisdictional protection of informational self-determination and, in particular, the protection of the right through the recurso de protección, through habeas data and through a specialized agency as control authority.","container-title":"Estudios constitucionales","ISSN":"0718-5200","issue":"2","journalAbbreviation":"Estudios constitucionales","language":"es","page":"87-120","source":"DOI.org (Crossref El trabajo de Contreras también explica porqué el legislador optó por una redacción del texto que no se refiere expresamente a los derechos ARCO. Los legisladores, para bien o para mal, creyeron que una redacción vaga evitaría "la obsolescencia del texto constitucional". *Ibid*., p. 115.

203 Ver Pablo Contreras, "¿Una segunda oportunidad? Protección de datos personales y autodeterminación informativa en una nueva Constitución chilena", *Revista Brasileira de Políticas Públicas* 12, nº 2 (2022): 132 ("la LPVP sólo ha motivado un escaso número de acciones de habeas data, en procedimientos extensos y costosos para los titulares de datos y sin generar una jurisprudencia civil relevante sobre tratamientos ilegales de datos personales").

Lamentablemente, y según otro estudio del profesor Pablo Contreras, la jurisprudencia sobre el nuevo derecho del art. 19 Nº 4 ha sido deficiente en tres sentidos.[204]

Primero, "pese a que se reconoce como un derecho fundamental, la protección de datos personales no juega ningún rol relevante en ciertas decisiones o derechamente es omitido en su conceptualización y aplicación".[205]

Segundo, la jurisprudencia ha malentendido quiénes son los titulares del derecho, extendiéndo la titularidad desde las personas naturales a las jurídicas. Esto ha ocurrido en "casos de comunicación de deudas sin el consentimiento de la persona jurídica, para ser reportado en el boletín comercial y de deudas de los bureau de crédito".[206]

Tercero, la jurisprudencia no ha entendido bien el objeto del derecho fundamental, al omitir reconocer todos los derechos ARCO. Por ejemplo, "la Corte Suprema ha respaldado el tratamiento de datos personales recolectados de la página web del Poder Judicial, para comunicar la oferta de prestación de servicios personales de defensa jurídica", omitiendo reconocer el derecho de oposición de la persona afectada.[207]

El derecho fundamental a la protección de datos personales, y el desarrollo que reciba en la jurisprudencia en el contexto de la acción constitucional de protección, convivirán con la LPDP y sus mecanismos para proteger los derechos de los titulares. Esto crea un riesgo de concurrencia de las competencias de los tribunales y de la Agencia.

2. La regulación constitucional especial del tratamiento de datos personales realizado con neurotecnologías

Desde el año 2021, la Constitución contiene una regulación especial sobre neurotecnologías en su art. 19 Nº 1. Según una interpretación plausible de dicha regulación ella es aplicable al tratamiento de ciertos datos personales.

Las neurotecnologías son dispositivos que se conectan directa o indirectamente al cerebro con el fin de registrar la actividad cerebral (o intervenirla). Por lo tanto, se puede decir las neurotecnologías permiten extraer datos personales en el sentido de la LPDP. Varias empresas están desarrollando y ofreciendo neurotecnologías para fines de salud, por ejemplo, para permitir que personas parapléjicas controlen el teclado de un computador. Pero también están siendo desarrolladas para usos masivos, por ejemplo, como un dispositivo que los consumidores pueden utilizar para controlar sus computadores.[208] Las comercialización y masificación de las neurotecnologías suscitan preguntas morales y jurídicas que han atraído la atención de académicos y otros actores a nivel nacional e internacional.[209]

204 Ibid.
205 *Ibid.*, p. "¿Una segunda oportunidad?", 135.
206 *Ibid.*, p. 138.
207 *Ibid.*, p. 139.
208 Ver, por ejemplo, Alex Heath, "This Is Meta's AR / VR Hardware Roadmap for the next Four Years", *The Verge*, 1 de marzo de 2023, https://www.theverge.com/2023/2/28/23619730/meta-vr-oculus-ar-glasses-smartwatch-plans.
209 Sobre las neurotecnologías y sus desafíos morales y políticos, ver Nita A. Farahany, *The Battle for Your Brain: Defending the Right to Think Freely in the Age of Neurotechnology* (New York: St. Martin's Press, 2023); Sjors Ligthart et al., "Minding Rights: Mapping Ethical and Legal

La materia es regulada por la Constitución desde el año 2021. Su artículo 19 Nº 1 fue reformado gracias a un proyecto de ley constitucional impulsado por el entonces senador Guido Girardi.[210] La reforma agregó el siguiente texto al derecho a la vida y la integridad física y psíquica (art. 19 Nº 1, inc. 5):

> El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, *debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella* (énfasis agregado);

En estricto rigor, la conducta a la cual se refiere la regla es "la "utilización en las personas" del "desarrollo científico y tecnológico", sin mencionar la palabra "neurotecnologías". Sin embargo, la historia legislativa de la reforma muestra que, en efecto, el principal objetivo del texto fue regular dichas tecnologías. Por ejemplo, el título del proyecto de ley constitucional que originó la reforma indicaba que se trataba de un proyecto "para proteger la integridad y la indemnidad mental con relación al avance de las neurotecnologías".[211]

Esa historia fidedigna del establecimiento y el texto de la disposición también dejan claro que la regla se refiere, en parte, al tratamiento de datos personales. El texto habla del uso de las neurotecnologías respecto de la "información proveniente" de "la actividad cerebral". En la práctica estos "neurodatos" serán, probablemente, datos sobre una persona identificada o identificable; es decir, datos personales.

¿Cuál es la consecuencia jurídica de la disposición? Por una parte, el mismo artículo deja claro que la norma busca mandatar al legislador para regular las neurotecnologías. Es más, ya existe un proyecto de ley que busca cumplir con el mandato constitucional cuyo origen es contemporáneo al de la reforma constitucional.[212]

Por otra parte, la disposición se relaciona con la acción constitucional de protección. Esta acción, según el art. 20 de la Constitución, puede ser utilizada para amparar los derechos del art. 19 Nº1. Así, esta sería una nueva base legal –independiente del art. 19 Nº 4– para proteger a un titular de datos personales mediante la acción de protección. ¿Con qué fin? Una interpretación posible es que también permite exigir el acceso, rectificación, cancelación, y oposición a los datos personales obtenidos mediante neurotecnologías, así

Foundations of 'Neurorights'", *Cambridge Quarterly of Healthcare Ethics*, 15 de mayo de 2023, 1–21; Ross Andersen, "The Right to Not Have Your Mind Read", *The Atlantic*, 21 de agosto de 2023, https://www.theatlantic.com/technology/archive/2023/08/mind-reading-brain-data-interrogation-mri-machines/675059/; Rafael Yuste, Jared Genser, y Stephanie Herrmann, "It's Time for Neuro-Rights", *Horizons: Journal of International Relations and Sustainable Development* 18 (2021): 154–65.

210 Ley Nº 21.383, Modifica la carta fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas, D.O. 25 octubre 2021, disponible en https://www.bcn.cl/leychile/navegar?idNorma=1166983.

211 Ver Moción de Juan Antonio Coloma Correa, Alfonso De Urresti Longton, Guido Girardi Lavín, Carolina Goic Boroevic y Francisco Chahuán Chahuán, Modifica el artículo 19, número 1°, de la Carta Fundamental, para proteger la integridad y la indemnidad mental con relación al avance de las neurotecnologías, Boletín Nº 13827-19, 7 de octubre de 2020, http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=13827-19.

212 Ver el proyecto de ley sobre protección de los neuroderechos y la integridad mental, y el desarrollo de la investigación y las neurotecnologías, Boletín N° 13828-19, 7 octubre 2020, disponible en http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=13828-19. Este proyecto de ley y el de proyecto de reforma constitucional (que eventualmente se convirtió en ley) fueron presentados el mismo día y por los mismos senadores. El Senado aprobó el proyecto en primer trámite constitucional el 7 de diciembre de 2021. Desde esa fecha al momento del cierre de este trabajo a mediados de octubre de 2024 la Cámara de Diputados no ha trabajado en el proyecto de ley. Para críticas al proyecto de ley, ver Vladimir Garay, María Paz Canales, y Michele Bordachar, "Neuroderechos para qué, maldita sea", *Derechos Digitales* (blog), 29 de abril de 2021, https://www.derechosdigitales.org/15760/neuroderechos-para-que-maldita-sea/. Ver también las críticas a la reforma constitucional sobre neurotecnologías de los trabajos citados arriba en la nota al pie 191.

como a su tratamiento. Al mismo tiempo, si esto es así, el art. 19 Nº1 sería redundante, pues la materia ya es regulada en el art. 19 Nº 4.[213]

A la fecha de la publicación de este trabajo conocemos de un solo caso en el cual se invocó la disposición constitucional sobre neuroderechos. El caso tuvo como protagonista al creador de la reforma constitucional: el exsenador Girardi. Éste utilizó la acción constitucional de protección para exigir que una empresa de neurotecnologías –Emotiv– eliminara datos neuronales de Girardi obtenidos mediante un dispositivo que había sido vendido por esa empresa.

En primera instancia la pretensión fue rechazada por la Corte de Apelaciones de Santiago.[214] Pero en segunda instancia, la Tercera Sala de la Corte Suprema, en una sentencia pronunciada con extraordinaria rapidez por la entonces ministra Ángela Vivanco.[215]

Específicamente, la Tercera Sala de la CS ordenó a Emotiv eliminar la información recolectada del cerebro de Girardi. También ordenó al Instituto de Salud Pública que examinara la neurotecnología en cuestión con el fin de evaluar si se ajustaba a la Ley 20.120 sobre la investigación científica en el ser humano, su genoma, y [que] prohíbe la clonación humana. La decisión citó como justificación el art. 19 de la Constitución, específicamente su número 1 (sobre neurotecnologías) y su número 4 (protección de datos personales). Lamentablemente, la sentencia de la CS omitió clarificar las relaciones conceptuales entre estos derechos en relación a los neurodatos.

Una vez que entre en vigencia la LPDP será tarea de la jurisprudencia constitucional dilucidar la relación entre esta ley, los números 1 y 4 del art. 19 de la Constitución, y la Ley 20.120, en relación a las neurotecnologías y los neurodatos.

B. Regulaciones sectoriales

El tratamiento de datos personales también es regulado por varias leyes y órganos sectoriales. Antes de la dictación de la LPDP, los profesores Pablo Contreras, Pablo Trigo y Leonardo Ortiz observaron que la regulación chilena sobre tratamiento de datos personales experimentaba un "proceso de fragmentación regulatoria". Este proceso

> se caracteriza por la existencia de distintos organismos públicos que, en el ámbito de su competencia y sobre la base de sus atribuciones genéricas, han venido a regular –con mayor o menor extensión– diversos aspectos relacionados con la tutela de los sujetos titulares de

213 Sobre esta crítica y otros aspectos deficitarios del proyecto, ver Alejandra Zúñiga Fajuri et al., "La trivialidad de los neuroderechos", *Revista Bits de Ciencia*, nº 22 (2022): 24–24; Danielle Zaror Miralles, Michelle Bordachar Benoit, y Pablo Trigo Kramcsák, "Acerca de la necesidad de proteger constitucionalmente la actividad e información cerebral frente al avance de las neurotecnologías: Análisis crítico de la reforma constitucional introducida por la Ley 21.383", *Revista Chilena de Derecho y Tecnología* 10, nº 2 (31 de diciembre de 2021): 1–10. Para una defensa de la reforma constitucional y en general de la creación de "neuro-derechos", ver Yuste, Genser, y Herrmann, "It's Time for Neuro-Rights".

214 Corte de Apelaciones de Santiago, *Guido Girardi contra Emotiv*, protección rol N°49852-2022, 24 mayo 2023. Para un comentario de esta sentencia, ver Lucas MacClure, "Las neurotecnologías ante la Corte de Apelaciones de Santiago: olvidando el derecho de cancelación de datos personales", Diario Constitucional, 19 de julio de 2023, https://www.diarioconstitucional.cl/articulos/las-neurotecnologias-ante-la-corte-de-apelaciones-de-santiago-olvidando-el-derecho-de-cancelacion-de-datos-personales/.

215 Corte Suprema, *Guido Girardi contra Emotiv*, apelación rol 105.065-2023, 9 agosto 2023. Para un comentario de la sentencia de la Corte Suprema, ver Lucas MacClure, Pablo Fuenzalida, y Lucas Sierra, "Fallo sobre neurotecnologías: ¿otro supremazo?", *Diario Financiero*, 17 de agosto de 2023, https://www.df.cl/opinion/columnistas/fallo-sobre-neurotecnologias-otro-supremazo.

datos personales o con los deberes que recaen sobre las entidades responsables de las bases de datos.[216]

La dictación de la LPDP es un paso hacia la concentración regulatoria, especialmente gracias a la creación de la Agencia. Sin embargo, la transformación no ha sido completa. Persisten competencias y regulaciones sectoriales, tal como ejemplificaremos a continuación (sección V.B.1). Y hay preguntas abiertas sobre la coordinación y los conflictos entre, por un lado, las regulaciones y órganos sectoriales y, por otro, la LPDP y su Agencia, pese a que esta ley intenta regular algunos aspectos de esa relación (sección V.B.2).

1. Ejemplos de regulaciones sectoriales que regulan el tratamiento de datos personales

1.1. Derecho del consumidor y SERNAC

Hasta hace poco, el SERNAC tenía la potestad de fiscalizar el cumplimiento de las reglas de la Ley 19.496, Sobre Protección de los Derechos de los Consumidores (en adelante "LPC"), "respecto de los datos personales de los consumidores, en el marco de las relaciones de consumo" (art. 15 bis Ley 19.496).[217] Esta potestad fue creada a fines del año 2021.[218]

Al alero de esta regulación, el SERNAC se consolidó como una especie de "mini" agencia de protección de datos personales.[219] Por ejemplo, el SERNAC dictó una resolución "sobre criterios de equidad en las estipulaciones contenidas en contratos de adhesión referidas a la recolección y tratamiento de datos personales de consumidores".[220]

La ley que reformó la Ley 19.628 para transformarla en la LPDP eliminó el art. 15 bis de la Ley 19.496 (en estricto rigor la reforma, al igual que la LPDP, entrará en vigencia hacia fines de 2026 o principios del 2027).[221] Así, bajo la LPDP el SERNAC pierde su potestad expresa de protección de los datos personales. El legislador de la LPDP consideró que no era necesario contar con una mini agencia de protección de datos cuando ya existe una autoridad de protección con amplios poderes como la Agencia. Esta reforma debería reducir el rol del SERNAC en esta materia.

---

216 Pablo Contreras, Pablo Trigo, y Leonardo Ortiz, "Un sistema fragmentado: La protección sectorial de los datos personales en Chile", *Revista de Derecho Administrativo Económico*, nº 35 (2022): 38–39.

217 Ley Nº 19.496, que Establece Normas Sobre Protección de los Derechos de los Consumidores, versión del 25 de abril de 2022, disponible en https://www.bcn.cl/leychile/navegar?idNorma=1160403

218 Ley 21.398, establece medidas para incentivar la protección de los derechos de los consumidores, publicada en el Diario Oficial el 24 de diciembre de 2021, disponible en https://www.bcn.cl/leychile/navegar?idNorma=1170464&idVersion=2022-04-25. El texto completo de la norma era el siguiente: "Artículo 15 bis.- Las disposiciones contenidas en los artículos 2 bis letra b, 58 y 58 bis serán aplicables respecto de los datos personales de los consumidores, en el marco de las relaciones de consumo, salvo que las facultades contenidas en dichos artículos se encuentren en el ámbito de las competencias legales de otro órgano". Sobre la historia y significado de esta reforma ver Contreras, Trigo, y Ortiz, "Un sistema fragmentado", 42–47.

219 Renato Jijena, "Sernac y datos biométricos de los consumidores", *Diario Financiero*, 30 de abril de 2024, https://www.df.cl/opinion/columnistas/sernac-y-datos-biometricos-de-los-consumidores.

220 Servicio Nacional del Consumidor, Resolución Exenta N° 174, "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", 28 febrero 2022, disponible en https://www.sernac.cl/portal/618/articles-65388_archivo_01.pdf.

221 Ver artículo tercero del proyecto de ley, aprobado por el Congreso, boletín Nº 11.144-07, Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (refundido con el boletín 11.092-07) (2017), 27 agosto 2024, http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07.

Con todo, está por verse cómo el SERNAC interpretará sus competencias generales –por ejemplo, para interponer acciones colectivas por vulneración de las normas de protección de los consumidores– en relación con la protección de los datos personales de los consumidores. En la economía digital es difícil separar la protección de los consumidores de la protección de los datos personales. El SERNAC podría concluir que todavía es competente en ámbitos que son regulados por la LPDP.

Es más, ya antes de la reforma del 2021 que estableció el art. 15 bis de la LPCP el SERNAC había ejercido sus potestades para proteger los datos personales de los consumidores,[222] y parte de la doctrina había invocado la LPC como mecanismo para proteger los datos personales.[223]

Otro elemento que complica el análisis es la regla de la LPC que define su ámbito de aplicación –y el de las competencias del SERNAC– vis-à-vis otras leyes y órganos especializados (art. 2 bis). Se trata de una regla indeterminada, confusa y, por lo tanto, de difícil aplicación.[224] Así, para entender la regulación de datos personales será necesario prestar atención a las posiciones que tome el SERNAC sobre sus propias competencias.

1.2. Bancos y otras instituciones financieras, y la Comisión para el Mercado Financiero

Los bancos y otras instituciones financieras tratan datos personales rutinariamente, por ejemplo, cuando almacenan datos sobre la deuda bancaria de personas específicas.

El tratamiento de datos personales realizado por instituciones financieras es regulado de manera general y especial por la LPDP. Ya hemos examinado las reglas generales a lo largo de este trabajo. En relación a las especiales, a las cuales solo hemos aludido, cabe señalar que la LPDP limita la libertad de esas instituciones para publicar o comunicar a terceros varios tipos de deudas, a riesgo de incurrir en infracciones sancionables por la Agencia (arts. 17-19). Por ejemplo, la LPDP indica que "[n]o podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas" (art. 17 inc. 2); pero sí se puede comunicar "el incumplimiento de obligaciones derivadas de mutuos hipotecarios y de préstamos o créditos de bancos" (art. 17 inc. 1).[225]

Junto a las reglas generales y especiales de la LPDP, coexisten una multitud de leyes del sector financiero que regulan diversos aspectos del tratamiento de datos personales. Y, dado que la fiscalización de su cumplimiento y desarrollo mediante normas administrativas corresponde a la Comisión para el Mercado Financiero, ésta tiene un rol que jugar en la protección de los datos personales en este sector.[226]

Un ejemplo reciente de ello se encuentra en la Ley 21.521, que promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros, o Ley Fintech, del año 2023.[227]

222 Ver Contreras, Sistema 43-45.
223 Ver Rodrigo Momberg Uribe et al., "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, nº 2 (diciembre de 2019): 157–80. el artículo analiza los supuestos para la declarar como abusiva una cláusula sobre uso y tratamiento de datos personales. El estudio se efectúa desde la perspectiva del derecho del consumidor, en particular, a partir de los dispuesto en el artículo 16 letra g
224 Sobre el significado de esta disposición y la jurisprudencia que ha generado, ver Iñigo De la Maza, "Lex Specialis: sobre el artículo 2º bis de la ley 19.496", *Revista de derecho (Concepción)* 88, nº 247 (junio de 2020): 83–116; Iñigo De la Maza y Hernán Cortez, "La Ley 19.496 como un supuesto de descodificación material y su relación con las leyes especiales a las que alude el artículo 2 bis", *Revista de derecho (Valparaíso)*, nº 56 (julio de 2021): 115–43.
225 Ver también arriba sección III.B.2.1.
226 Ver Contreras, Trigo, y Ortiz, "Un sistema fragmentado", 52–60.
227 Ley Nº 21.521, promueve la competencia e inclusión financiera a través de la innovación y tecnología en la prestación de servicios financieros, Ley Fintech, D.O. 4 enero 2023, disponible en https://www.bcn.cl/leychile/navegar?idNorma=1187323.

Esta ley busca "establecer un marco general para incentivar la prestación de servicios financieros a través de medios tecnológicos que realicen los proveedores regidos por ella" (art. 1 inc. 1).

Uno de los principios de la Ley Fintech es el "adecuado resguardo de los datos tratados" (art. 1 inc. 2). Una expresión del principio es que determinadas instituciones –"las Instituciones Proveedoras de Información, los Proveedores de Servicios basados en Información, las Instituciones Proveedoras de Cuentas y los Proveedores de Servicios de Iniciación de Pagos participantes en el Sistema de Finanzas Abiertas"– deben tomar medidas adecuadas para resguardar la seguridad de los datos que tratan y minimizar riesgos a los sistemas que controlan. Al evaluar y prevenir los riesgos, las instituciones "[d]eberán tener en consideración para tales efectos, el riesgo inherente a cada tipo de información, como, asimismo, *la calidad de dato sensible conforme a las disposiciones de la ley* N° 19.628" (art. 22 inc. 1, énfasis agregado). Además, cuando hay un incidente de seguridad, la institución debe notificar a la Comisión (art. 22 inc. 2). La Comisión del Mercado Financiero tiene la potestad para desarrollar estos deberes mediante normas generales (art. 22).

1.3. Telecomunicaciones y Subtel

Los proveedores de servicios de internet (ISPs) rutinariamente acceden a datos personales, como la información sobre los sitios web y aplicaciones utilizadas por las personas.

La regulación sectorial de las telecomunicaciones contiene reglas sobre este tratamiento de datos personales. La Ley 18.168 General de Telecomunicaciones (LGT) establece que los ISPs "procurarán preservar la privacidad de los usuarios" (art. 24 H letra a).[228] Buena parte de esa privacidad está constituida por la protección de datos personales de los usuarios de internet. Consecuentemente, el Reglamento de Servicios de Telecomunicaciones dispone:

> Los datos personales de suscriptores y usuarios recabados por los proveedores de servicios de telecomunicaciones con motivo de la contratación y suministro de los servicios de telecomunicaciones regulados en el presente reglamento, sólo podrán utilizarse para los fines específicos asociados a la prestación del servicio, debiendo someterse en el tratamiento de tales datos a lo previsto al efecto en la Ley Nº19.628, Sobre Protección de la Vida Privada (art. 24).[229]

El mismo reglamento dice que el contrato de suministro de servicios de telecomunicaciones proporcionado por el ISP debe referirse al "[c]ambio de datos personales a solicitud del suscriptor" (art. 14 letra h): este es un derecho análogo al derecho a la rectificación de datos personales de la LPDP.

El órgano encargado de aplicar esta regulación es el Ministerio de Transporte y Telecomunicaciones, a través de su Subsecretaría de Telecomunicaciones (Subtel).[230]

1.4. Salud y Superintendencia de Salud

La profesión médica, los hospitales y otros establecimientos de salud a menudo acceden a datos personales

228 Ley 18.168 General de Telecomunicaciones, D.O. 2 octubre 1982, disponible en https://www.bcn.cl/leychile/navegar?idNorma=29591. A su vez, el artículo 50 del Reglamento de Servicios de Telecomunicaciones, Decreto 18, Ministerio de Transportes y Telecomunicaciones, 2014, disponible en https://www.bcn.cl/leychile/navegar?idNorma=1059429, establece que "[l]os ISP procurarán preservar la privacidad y seguridad de los usuarios en la utilización del servicio de acceso a Internet".
229 *Ibid*.
230 Ver arts. 7, 8 y 28 bis de la LGT, arts. 1 y 68 del Reglamento de Servicios de Telecomunicaciones, y el Decreto Supremo Núm. 194/2012, "Reglamento sobre Tramitación y Resolución de Reclamos de Servicios de Telecomunicaciones", D.O 16 de febrero de 2013.

sensibles relativos a la salud de los titulares.

Varios de estos datos se encuentran en la ficha clínica de cada paciente, esto es, el "instrumento obligatorio en el que se registra el conjunto de antecedentes relativos a las diferentes áreas relacionadas con la salud de las personas".[231]

El tratamiento de datos realizado por prestadores de servicios de salud está normado por la Ley Nº 20.584, que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención de salud. Dicha ley fue recientemente modificada por una ley sobre interoperabilidad de las fichas clínicas.[232] En materia de salud también son relevantes otras reglas, de rango constitucional, legal e infra-legal.[233] El cumplimiento de buena parte de esta regulación es fiscalizado por la Superintendencia de Salud.

2. Coordinación y conflictos entre la LPDP y la Agencia, y las leyes y autoridades sectoriales

Los ejemplos anteriores sugieren que la implementación de la LPDP deberá lidiar con el problema de cómo conviven las regulaciones sectoriales del tratamiento de datos personales y la regulación general de la LPDP. ¿Qué ocurre en casos de conflictos de normas? ¿Quién es competente para aplicar las distintas reglas?

La LPDP omitió reformar las leyes sectoriales que regulan el tratamiento de datos personales, con la excepción de las competencias del SERNAC.[234] Tampoco se encuentra en la LPDP una disposición general que regule la relación entre sus reglas de conducta y las reglas de las leyes sectoriales.

Lo que la LPDP sí hace es regular la interacción entre la Agencia y las autoridades sectoriales. Sin embargo, lo hace de manera confusa.[235]

A primera vista, la LPDP empodera a la Agencia para fiscalizar el cumplimiento de todas las reglas sobre protección de datos personales, ya sea que se encuentren en la LPDP o en otras leyes. Una de sus facultades es "[a]plicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de protección de los datos personales" (art. 30 bis inc. 1 letra b).[236]

Sin embargo, ¿cómo se compatibiliza esta facultad de la Agencia con las leyes sectoriales que empoderan a sus órganos sectoriales para velar por la protección de los datos personales? Por ejemplo, como ya advertimos, la Subtel tiene competencias para velar por el cumplimiento de reglas legales y reglamentarias de

231 Art. 12, Ley 20.584, que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención de salud, D.O. 24 abril 2012, disponible en https://www.bcn.cl/leychile/navegar?idNorma=1039348.

232 Ley Nº 21.668, modifica la Ley Nº 20.584 con el objeto de establecer la interoperabilidad de las fichas clínicas, D.O. 24 mayo 2024, disponible en https://www.bcn.cl/leychile/navegar?idNorma=1203827.

233 Ver Carlo Benussi, "Obligaciones de seguridad en el tratamiento de datos personales en Chile: escenario actual y desafíos regulatorios pendientes", *Revista Chilena de Derecho y Tecnología* 9, nº 1 (30 de junio de 2020): 227–79.

234 Ver arriba sección V.B.1.1 Más allá de las leyes sectoriales, la ley que reformó la Ley 19.628 para crear la LPDP también modificó la Ley N° 20.285, sobre acceso a la información pública, para eliminar la facultad del Consejo Para la Transparencia para velar por el cumplimiento de la Ley 19.628 respecto de los órganos de la Administración del Estado, facultad que fue traspasada a la Agencia). Ver art. segundo del proyecto de ley, aprobado por el Congreso, boletín Nº 11.144-07, Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales (refundido con el boletín 11.092-07) (2017), 27 agosto 2024, http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11144-07.

235 Además, la LPDP contempla un mecanismo de coordinación regulatoria con el Consejo para la Transparencia en su art. 31. Omitimos abordarlo en consideración al alcance de este paper.

236 Nótese que esta regla no dice que la Agencia solamente pueda aplicar e interpretar las reglas de "esta ley".

telecomunicaciones que ordenan a los proveedores de servicios de internet a proteger los datos personales.[237] ¿Qué debe hacer la Subtel cuando recibe un reclamo de un usuario en esta materia? ¿Quién es competente?

Por lo pronto, la Agencia tiene facultades colaboración con las autoridades sectoriales, y en uso de ellas podría buscar un entendimiento con órganos sectoriales competentes en materia de datos personales. La LPDP establece que la Agencia puede "[r]elacionarse y colaborar con los órganos públicos en el diseño e implementación de políticas y acciones destinadas a velar por la protección de los datos personales y su correcto tratamiento" (art. 30 bis inc. 1 letra j), y "[s]uscribir convenios de cooperación y colaboración con entidades públicas (…) que tengan competencia o estén relacionadas al ámbito de los datos personales" (art. 30 bis inc. 1 letra k).[238] ¿Pero qué ocurre cuando no existe un convenio en materia de superposición de competencias, o cuando ese convenio es impugnado por un responsable?

El potencial conflicto de competencias entre la Agencia y los órganos sectoriales es abordado expresamente por el art. 30 bis inc. 2 de la LPDP. A su vez, esta regla se remite al art. 14 de la Ley N° 19.880, que Establece Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado (LBPA). Para facilitar la interpretación de estas reglas, a continuación reproducimos los textos en una tabla, agregando un espacio entre el hecho operativo y el deber de cada disposición:

Art. 30 bis inc. 2 LPDP	Art. 14 inc. 2 LBPA
Requerido un organismo de la Administración para el ejercicio de las funciones o atribuciones que esta ley le entrega a la Agencia, deberá dar cumplimiento a lo dispuesto en el inciso segundo del artículo 14 de la ley N° 19.880	Requerido un órgano de la Administración para intervenir en un asunto que no sea de su competencia, enviará de inmediato los antecedentes a la autoridad que deba conocer según el ordenamiento jurídico, informando de ello al interesado.

Es claro que el art. 30 bis inc. 2 de la LPDP, leído a la luz del art. 14 inc. 2 de la LBPA, establece un deber de los órganos sectoriales de enviar asuntos a la Agencia informando de ello al interesado. Lo que no es claro es el supuesto de hecho del deber de remitir el asunto.

Según una primera interpretación, el supuesto de hecho del deber se encuentra exclusivamente en la primera parte del art. 30 bis inc. 2 de la LPDP: "Requerido un organismo de la Administración *para el ejercicio de las funciones o atribuciones que esta ley le entrega a la Agencia*". Este supuesto de hecho no exige contestar si el órgano sectorial es o no competente para aplicar reglas sobre protección de datos según su regulación sectorial; lo único que es relevante es que la Agencia es competente, es decir, que el asunto cae bajo "las funciones o atribuciones que esta ley le entrega a la Agencia". Y, como observamos arriba, la Agencia tiene una facultad amplia para aplicar e interpretar todas las reglas sobre protección de datos personales, ya sea que se encuentren en la LPDP o en otras leyes, incluidas las sectoriales. Por lo tanto, el efecto práctico de esta

237 Ver arriba sección V.B.1.3.

238 De manera similar, el art. 30 bis inc. 1 letra i faculta a la Agencia a "[p]restar asistencia técnica, cuando le sea requerida, al Congreso Nacional, al Poder Judicial, a la Contraloría General de la República, al Ministerio Público, al Tribunal Constitucional, al Banco Central, al Servicio Electoral, a la Justicia Electoral y los demás tribunales especiales creados por ley, en la dictación y ejecución de las políticas y normas internas de estos organismos, con el objeto que sus operaciones y actividades de tratamiento de datos personales se realicen conforme a los principios y obligaciones establecidos en esta ley".

interpretación es que los órganos sectoriales que conozcan asuntos sobre protección de datos personales, por regla general, deberán enviarlos a la Agencia.

Pero otra interpretación es posible: que el supuesto de hecho del deber incluye la primera parte del art. 14 inc. 2 de la LBPA, es decir, que se haya "[r]equerido un órgano de la Administración para intervenir en un asunto *que no sea de su competencia*" (énfasis agregado). Bajo esta hipótesis, no basta que la Agencia sea en principio competente según sus amplias facultades. Además es necesario que el órgano sectorial sea incompetente, según su regulación sectorial. Y ésta es una condición que a menudo no se cumple, por aplicación de los tipos de regulaciones sectoriales que revisamos en las secciones anteriores. La implicancia práctica de esta interpretación sería que los órganos sectoriales que tienen estos tipos de competencia no deberían remitir asuntos sobre protección de datos personales a la Agencia. La Subtel, por ejemplo, podría negarse a remitir a la Agencia un requerimiento de un usuario sobre el tratamiento de datos personales realizado por un ISP argumentando que la regulación de telecomunicaciones le entrega a la Subtel competencia en esta materia y que, por lo tanto, no se daría el supuesto del art. 14 inc. 2 de la LBPA (y, en consecuencia, del 30 bis inc. 2 de la LPDP).

¿Cuál interpretación es correcta? Lamentablemente, la correcta interpretación del art. 30 bis inc. 2 de la LPDP no es clarificada por la historia fidedigna del establecimiento de esta disposición.[239] Con todo, la historia legislativa de otras normas de la LPDP sugiere que el legislador buscó que esta fuera la "ley principal" de la protección de datos personales.[240] Ésta y otras razones nos hacen pensar que la LPDP probablemente concentró las competencias de aplicación de toda la regulación de protección de datos personales en la Agencia. Es decir, que la primera interpretación sería correcta.[241] Pero está por verse qué práctica se desarrollará en esta materia.

¿Qué ocurre con los conflictos de competencia entre la Agencia y los órganos sectoriales respecto de la dictación de normas generales? La expresión "asunto" del art. 30 bis inc. 2 de la LPDP puede entenderse de manera amplia, de manera que incluya el ejercicio de potestades normativas. Si esto así, las preguntas interpretativas que acabamos de plantear también son relevantes para los conflictos de potestades normativas. Sin embargo, la LBPA contiene otra regla más sobre coordinación de distintos órganos administrativos que puede ser relevante en este nivel de análisis. Específicamente, una regla sobre los actos administrativos "de carácter general":

> Cuando un órgano de la Administración del Estado deba evacuar un acto administrativo de carácter general que tenga claros efectos en los ámbitos de competencia de otro órgano, le remitirá todos los antecedentes y requerirá de éste un informe para efectos de evitar o precaver conflictos de normas, con el objeto de resguardar la coordinación, cooperación y

239 Ver Comisión de Constitución de la Cámara de Diputados, "Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento, Respecto al Proyecto de Ley Refundido que Regula la Protección y el Tratamiento de los Datos Personales y Crea la Agencia de Protección de Datos Personales – Boletines Nº 11.144-07 y 11.092-07", 7 marzo 2023, pp. 397-398. Ver también Lucas Sierra Iribarren y Lucas MacClure, "Agencia de Protección de Datos y telecomunicaciones: ¿quién es competente?", *El Mercurio Legal*, 4 de septiembre de 2024, https://www.elmercurio.com/Legal/Noticias/Opinion/2024/09/02/914161/agencia-proteccion-datos-y-telecomunicaciones.aspx.

240 Ver el registro audiovisual de la sesión de la Comisión de Constitución del Senado en "Comisión de Constitución - 16 de Abril 2019", 7:15-8:17, https://youtu.be/Pr9oMCa_jew?si=VIf4PycpBMsE1KWU&t=435; cfr. Comisión de Constitución del Senado, "Segundo Informe de la Comisión de Constitución, Legislación, Justicia y Reglamento del Senado, Legislación", 16 de marzo de 2020, p. 46, cuya transcripción de esta parte de la sesión es imprecisa.

241 Ver Lucas Sierra Iribarren y Lucas MacClure, "Agencia de Protección de Datos y telecomunicaciones: ¿quién es competente?", *El Mercurio Legal*, 4 de septiembre de 2024, https://www.elmercurio.com/Legal/Noticias/Opinion/2024/09/02/914161/agencia-proteccion-datos-y-telecomunicaciones.aspx.

colaboración entre los órganos involucrados en su dictación (art. 37 bis inc. 1).

El órgano –por ejemplo, un órgano sectorial– que ha recibido el informe de otro órgano –por ejemplo, de la Agencia– debe considerar el informe en su decisión, pero no está forzado a adoptar del órgano informante (art. 37 bis inc. 2).[242] ¿Cuáles son las consecuencias de esta regla de la LBPA respecto del 30 bis inc. 2 de la LPDP y en general de las facultades de la Agencia vis-à-vis las de los órganos sectoriales?

La falta de reglas claras en la LPDP sobre la superposición de competencias de la Agencia y los órganos sectoriales, y la existencia de reglas de coordinación en la LBPA, sugieren que la relación entre estos órganos exigirá la cuidadosa atención de los distintos reguladores (y los sujetos regulados). Es posible que, eventualmente, esta cuestión deba ser resuelta por la judicatura[243] o incluso mediante reformas legales.[244]

C. Regulación de la ciberseguridad

En la sección anterior abordamos el fenómeno del cúmulo de regulaciones sobre tratamiento de datos personales mediante algunos ejemplos de regulaciones sectoriales. En esta parte abordaremos una regulación de alcance general que también interactuará con la LPDP: la de la ciberseguridad.

1. Ley Nº 21.663 Marco de Ciberseguridad

La Ley Nº 21.663 Marco de Ciberseguridad de 2024 (en adelante "LMC") establece obligaciones para un gran número de personas, privadas y públicas, en relación a los incidentes de seguridad. También crea la Agencia Nacional de Ciberseguridad. Al momento de escribir estas líneas esta ley todavía no había entrado en vigencia.[245]

Las personas reguladas son aquellas instituciones que prestan servicios que la ley califica como "esenciales" o "de importancia vital". Estas categorías cubren un amplio abanico de industrias que incluye, entre otras, a las empresas de telecomunicaciones, las de "servicios digitales y servicios de tecnología de la información gestionados por terceros", y la "banca, servicios financieros y medios de pago" (art. 4). La aplicación de la LMC puede ser extendida a otras instituciones mediante regulaciones de la Agencia Nacional de Ciberseguridad (art. 5).

¿Cómo se conecta esta ley con la regulación de los datos personales? La LMC contiene obligaciones relacionadas con los "incidentes de seguridad" que afectan a los datos personales.[246] Es más, varias de esas

242 Para otros aspectos procedimentales de este mecanismo de coordinación, ver los incisos 2 a 5 de la misma disposición.

243 Aquí puede cobrar relevancia la jurisprudencia de la Corte Suprema sobre el "principio de coordinación". Ver, por ejemplo, Corte Suprema, Servicios Visa Internacional Limitada y otros con Tribunal de Defensa de la Libre Competencia, rol N.º 105.997- 2022, 7 junio 2024, disponible en https://centrocompetencia.com/wp-content/uploads/2022/08/FALLO_ROL_N%C2%B0105997-2022.pdf.

244 Un posible modelo regulatorio para algunos aspectos de la coordinación es el art. 31 de la LPDP, que regula la "coordinación regulatoria con el Consejo para la Transparencia". Otro modelo regulatorio interesante es la Ley Marco de Ciberseguridad (Ley Nº 21.663). Esta ley regula de manera mucho más clara y detallada que la LPDP las relaciones entre su autoridad de control –la Agencia Nacional de Ciberseguridad– y los órganos sectoriales (ver arts. 25, 26 y 37).

245 Ley Nº 21.663, Ley Marco de Ciberseguridad, D.O. 8 abril 2024, disponible en https://www.bcn.cl/leychile/navegar?idNorma=1202434. Según el artículo transitorio primero de esta ley, su entrada en vigencia está supeditada a la dictación de uno o más decretos con fuerza de ley del Presidente de la República. El Presidente debe dictarlo(s) dentro de un año desde la publicación de la ley, y debe fijar una fecha de entrada en vigencia de la ley que ocurra a los seis meses o más tarde desde la publicación de la ley.

246 Un "incidente de seguridad", según la LMC, es "*todo evento que perjudique o comprometa la confidencialidad o integridad de la información*, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos" (art. 2 Nº 10, énfasis agregado). Esta definición es aplicable a incidentes relacionados con la seguridad de

obligaciones son muy similares a deberes de la LPDP que ya hemos revisado. Por ejemplo, la LMC dice que las instituciones obligadas deben aplicar

> medidas para prevenir, reportar y resolver incidentes de ciberseguridad. Estas medidas podrán ser de naturaleza tecnológica, organizacional, física o informativa, según sea el caso.
>
> El cumplimiento de estas obligaciones exige la debida implementación de los protocolos y estándares establecidos por la Agencia, así como de los estándares particulares de ciberseguridad dictados de conformidad a la regulación sectorial respectiva (art. 7).

Esta obligación es similar al "principio" de seguridad de la LPDP (art. 3 letra f) y al deber de adoptar medidas de seguridad (art. 14 quinquies).[247]

La LMC también obliga a las instituciones a reportar incidentes de seguridad a la Agencia Nacional de Ciberseguridad (art. 9 LMC). De manera similar, la LPDP obliga al responsable, en algunos casos, a reportar a la Agencia las vulneraciones a sus medidas de seguridad que afectan los datos personales que almacena (art. 14 sexies).[248]

La conexión del ámbito material de la LMC y de la LPDP creará concurrencia de competencias en el rol fiscalizador de la Agencia Nacional de Ciberseguridad y la Agencia de Protección de Datos Personales respecto de un mismo incidente. Desde la perspectiva del *compliance*, los responsables tendrán que diseñar sus medidas de seguridad de datos y sus protocolos de reporte considerando las obligaciones de las dos leyes.

2. Ley sobre delitos informáticos

La Ley Nº 21.459 sobre Delitos Informáticos de 2022 (en adelante "LDI")[249] castiga penalmente a quienes son responsables por los incidentes de seguridad y otras conductas similares.

La LDI incluye tipos penales que se refieren a "datos informáticos", un concepto que alcanza a los datos personales almacenados en formatos digitales.[250] Estos tipos incluyen el "ataque a la integridad de los datos informáticos" (art. 4 LDI), la "falsificación informática" o de datos informáticos (art. 5 LDI), la "receptación de datos informáticos" (art. 6 LDI), y el "fraude informático" (art. 7 LDI).

El delito de receptación de datos informáticos puede ser de particular relevancia para los responsables que adquieren bases de datos personales de otros responsables. La LDI define este delito así (art. 6):

---

los datos personales. La definición utiliza el concepto de "información", y un tipo de información son los datos. Además, cuando las empresas transfieren datos personales –algo que hacen rutinariamente– lo hacen utilizando "las redes y sistemas informáticos", otra expresión que se encuentra en la definición legal de incidente de seguridad. Así, los incidentes de seguridad en el sentido de la LMC se pueden referir a los datos personales en poder de las responsables y a las transferencias de los mismos, entre otras formas de tratamiento de datos personales. Por lo tanto, varias obligaciones impuestas por la LMC a los responsables en relación a los incidentes de seguridad se refieren, en parte, a incidentes que afectan los datos personales.

247 Sobre estos deberes ver arriba secciones III.C.1 y III.C.3.

248 Ver arriba seción III.C.3.

249 Ley Nº 21.459, establece normas sobre delitos informáticos, deroga la Ley Nº 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest, D.O. 20 junio 2022, disponible en https://www.bcn.cl/leychile/navegar?idNorma=1177743.

250 La LDI define los "datos informáticos" como "Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función" (art. 15 letra a).

> Receptación de datos informáticos. El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, datos informáticos, provenientes de la realización de las conductas descritas en los artículos 2° [delito de acceso ilícito a un sistema informático], 3° [delito de interceptación ilícita de transmisión no pública de información en uno o más sistemas informáticos] y 5° [delito de falsificación de datos informáticos], sufrirá la pena asignada a los respectivos delitos, rebajada en un grado.

3. Ley de delitos económicos

La Ley N° 21.595 de Delitos Económicos de 2023 (en adelante "LDE") también relevante para evaluar las obligaciones de los responsables en materia de ciberseguridad y, por esa vía, sus obligaciones en relación a los datos personales.[251]

En parte, ello se debe a que la LDE se remite a la LDI. La primera dice:

> Serán (...) considerados como delitos económicos los hechos previstos en las disposiciones legales que a continuación se indican, siempre que el hecho fuere perpetrado en ejercicio de un cargo, función o posición en una empresa, o cuando lo fuere en beneficio económico o de otra naturaleza para una empresa:
>
> (...)
>
> 20. Los artículos 1º, 2º, 3º, 4º, 5º, 6º, 7º y 8º de la ley N° 21.459, que establece Normas sobre delitos informáticos, deroga la ley Nº 19.223 y modifica otros cuerpos legales, con el objeto de adecuarlos al Convenio de Budapest (art. 2, encabezado y número 20).

Así, la infracción de estas normas de la LDE puede generar responsabilidad penal para los responsables que sean personas jurídicas. Por ejemplo, en relación con el delito de receptación de datos informáticos que mencionamos en la subsección anterior.

Además, la LDE modificó varias normas del Código Penal para introducir delitos informáticos. Por ejemplo, reguló el delito de manipulación de datos en un sistema informático para obtener provecho o perjudicar patrimonialmente a un tercero, un tipo que podría aplicar a la manipulación de datos personales (ver art. 468 del Código Penal).

CONCLUSIÓN

Este trabajo ha explicado porqué, una vez que la LPDP entre en vigencia, el derecho de la libre competencia chileno probablemente incorporará aspectos de la protección de datos personales en sus decisiones. Si esto es así, hemos sugerido, es importante que los profesionales de libre competencia

251 Ley N° 21.595 de Delitos Económicos, D.O. 17 agosto 2023, disponible en https://www.bcn.cl/leychile/navegar?idNorma=1195119.

empiecen a familiarizarse con esta ley.

En consecuencia, este ofreció un resumen descriptivo de la LPDP. Explicamos que el legislador dictó esta ley para mejorar el estándar de protección de los datos personales, y porque ella facilitará la transferencia internacional de datos personales en la medida que sea considerada como "adecuada" por la Unión Europea. Luego explicamos LPDP regula el tratamiento de datos sobre personas naturales realizado por responsables, incluyendo responsables establecidos en Chile y en el extranjero. Esta ley exige que el responsable trate datos cumpliendo con una fuente de licitud, así como con una batería de deberes a los cuales se refiere como "principios", "obligaciones", y "deberes". Además, la LPDP contempla varias instituciones para fomentar su cumplimiento. Entre ellas los programas de *compliance*, el ejercicio de derechos por el titular ante el responsable, el enforcement realizado por la Agencia –la cual puede imponer altas sanciones– y las acciones civiles ante los tribunales de justicia.

Finalmente, este trabajo hizo referencia al contexto regulatorio en el cual operará la LPDP –otras leyes y regulaciones supra- e infra- legales que se refieren al tratamiento de datos personales–, así como la manera imperfecta como la LPDP intentó regular la relación entre la Agencia y otros órganos.

Por sobre todo, este artículo ha sido una invitación a la colaboración entre profesionales de la libre competencia y profesionales de la protección de datos personales, con el fin de alcanzar la adecuada implementación de la LPDP y el cambio cultural positivo que muchas y muchos esperamos de esta importante ley.

Cómo citar este artículo:
Lucas MacClure, Lucas Sierra y Pablo Fuenzalida, "Una introducción a la nueva Ley sobre Protección de Datos Personales y su relevancia para el Derecho de la Libre Competencia", Diálogos CeCo (noviembre, 2024),
http://www.centrocompetencia.com/category/dialogos
Envíanos tus comentarios y sugerencias a info@centrocompetencia.com
CentroCompetencia UAI – Av. Presidente Errázuriz 3485, Las Condes, Santiago de Chile


UNIVERSIDAD ADOLFO IBÁÑEZ
CeCo
CentroCompetencia