REGULACIONES DE PRIVACIDAD DE DATOS ONLINE EN CHILE Y AUSTRALIA: REVISIÓN CRÍTICA Y DESAFÍOS FUTUROS

Andrés Salas Retamal*

Resumen
La privacidad ha sido un derecho protegido por convenciones internacionales y algunas leyes domésticas. Sin embargo, la protección de datos en internet no parece resultar eficiente. Los datos personales actualmente poseen un ascendente valor económico, y debido al desarrollo de tecnología nueva y económicamente asequible, así como a la profusa utilización de redes sociales, la cantidad de información personal disponible y generada está incrementándose significativamente a cada momento. Así y todo, la tecnología de fácil acceso presenta diversos desafíos para la preservación de datos personales por medio del derecho. En internet es difícil hacer cumplir un marco jurídico práctico, especialmente en lo relativo a velar por el cumplimiento del derecho y el flujo transfronterizo de información personal. La discusión estará enfocada en una descripción de los regímenes de protección de datos en Australia y Chile, esto es, ambos marcos jurídicos, a lo que se agrega una revisión crítica, particularmente acerca del ambiente online. Tras ello proporcionarémos un panorama del enfoque internacional que se ha otorgado al flujo transfronterizo de datos, los esfuerzos para alcanzar una armonización y responder a la necesidad de contar con autoridades provistas de facultades apropiadas en el ámbito de la protección de datos. Finalmente, concluiremos que tanto el sistema australiano como el chileno carecen de completa eficiencia en el ambiente de internet, y entregaremos ciertas propuestas para mejorar estos regímenes jurídicos.

Palabras clave: *Datos personales, Protección de datos, Privacidad, Tratamiento de datos, Internet.*

1. INTRODUCCIÓN

La privacidad es un derecho protegido por diversos tratados y convenciones internacionales. En varios instrumentos internacionales, la privacidad es reconocida como un derecho consagrado por la ley o como un derecho constitucional.[1]

* asalasretamal@gmail.com. Artículo recibido el 19 de mayo de 2018, aceptado para su publicación el 26 de julio de 2018. Traducción de Mauricio Reyes.

1 Ver Declaración Universal de los Derechos (*Universal Declaration of Human Rights*), GA Res 217ª (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/180 (1948), Art 12; Pacto Internacional de Dere-

Los datos personales son parte de este derecho, ya que se trata de información que "identifica a un individuo".[2]

Dado que los datos personales en internet poseen un elevado valor económico,[3] su protección presenta desafíos crecientes. El masivo y constante uso de las redes sociales genera diariamente una cantidad colosal de información,[4] y la conducta en internet no es necesariamente privada y anónima,[5] a lo que se agrega que la gigantesca cantidad de datos personales online constituye un escenario complejo para una apropiada protección de datos.[6] Consecuentemente, no todas las personas confían en la seguridad de su información en internet. En Australia, tan solo el 40% de los usuarios online "tienen confianza en que su configuración de privacidad en sitios web funciona correctamente".[7] En los Estados Unidos, los usuarios de internet están más preocupados de la *vigilancia en la red*: un 86% de los usuarios de la red han tomado diferentes medidas para "remover o cubrir sus huellas digitales".[8]

Asimismo, si bien Australia y Chile tienen diferentes sistemas jurídicos y judiciales, ambos comparten la necesidad de ajustar sus marcos jurídicos de protección de datos.[9] Para los propósitos de este trabajo, su estructura será la que sigue: en la primera sección se proporcionará una breve descripción de los datos personales y su valor digital. La sección siguiente presenta una revision panorámica de los regímenes de privacidad de datos tanto en Australia como en Chile, así como de la manera como sus marcos jurídicos interactúan con internet. Para ambos regímenes,

chos Económicos, Sociales y Culturales (*International Covenant on Economic, Social and Cultural Rights*), abierta para firma el 16 de diciembre de 1966, 993 UNTS 3 (en vigencia desde el 3 de enero de 1976), Art 17; Convención para la Protección de los Derechos del Hombre y las Libertades Fundamentales (*Convention for the Protection of Human Rights and Fundamental Freedoms*), abierta para firma el 4 de noviembre de 1950, 213 UNTS 221 (en vigencia desde el 3 de septiembre de 1953).

2 Jackson y Hughes (2015), p. 6.

3 Jackson y Hughes (2015), p. 197.

4 En el año 2015, 72% de los adultos en los Estados Unidos utilizaba Facebook, 28% Instagram, 25% Linkedin, y 23% Twitter. Al tiempo que los usuarios están constantemente actualizando su "estado", "retuiteando" textos y subiendo imágenes a Instagram, un reporte de junio de 2015 informó que Facebook tenía mensualmente 1,49 miles de millones de usuarios activos en el mundo. Sloan y Quan-Haase (2017), p. 4.

5 Jay y Hamilton (2003), p. 645.

6 "La creciente cantidad de datos almacenados y usados por firmas puede traer consigo muchos beneficios a los consumidores […] Sin embargo, también crea el riesgo de infracciones en materia de datos, exponiendo grandes cantidades de información sensible de los clientes *('The growing amount of data stored and used by firms can bring many benefits to consumers […] However, it also creates the risk of a data breach exposing large amounts of sensitive customer information')*. Financial System Inquiry (2014), pp. 4-55.

7 Australian Communications and Media Authority (2013), p. 1.

8 Pew Research Center (2013), p.1.

9 La comunidad internacional ha abordado la necesidad de ajuste de los sistemas de protección de datos de Australia y Chile, como se detalla y explica en la sección 3 de este trabajo.

la discusión se limitará a la información personal en general, no extendiéndose a clases especiales de información persona.[10] Se utilizarán dos criterios para llevar a cabo la comparación: cinco principios generales de protección de datos serán considerados como un punto de partida común para ambos regímenes, y el desafío del cumplimiento del derecho en el evento de una vulneración de la privacidad de datos, particularmente en el ambiente de internet, concluyendo que ambos regímenes son débiles en lo relativo a la privacidad de datos. La sección que le sigue busca abordar dichas fallas en base a tres materias clave: los enfoques internacionales para el flujo transfronterizo de datos y la necesidad consecuente de armonización; así como la necesidad de contar con una autoridad provista de facultades apropiadas para hacer cumplir las regulaciones. Finalmente, habremos concluido que ambas jurisdicciones dispensan insuficiente protección de datos. Sin embargo, una aproximación global armonizada en lo que respecta a la privacidad de datos y un ajuste legislativo apropiado a estándares internacionales en el derecho interno, mejorarán suficientemente el ejercicio efectivo del derecho a la privacidad en lo relativo a los datos personales.

2. INFORMACIÓN PERSONAL Y SU VALOR DIGITAL

Es información personal (o datos personales) aquella que "identifica a un individuo".[11] La protección de datos (o privacidad de datos) es la protección de los individuos contra cualquier uso indebido o no autorizado de su información personal por parte de terceros.[12] El uso de datos personales se llama tratamiento de datos.

En internet, los usuarios generan y dejan volúmenes colosales de datos personales. Esta información es una mezcla entre los datos personales proporcionados por los propios individuos,[13] información proporcionada por terceros,[14] o la información generada por la navegación de los usuarios en la red, llamada huellas digitales. Huella digital es el rastro, pista o "huellas que las personas dejan tras de sí en línea".[15]

La huella digital es el principal contenido de "*big data*", el que incluye almacenamientos con altos volúmenes de datos y alta velocidad en cuanto a la cantidad de datos de entrada y salida a o desde estos bancos, de una amplia variedad de tipos y

10 Ambas jurisdicciones tienen reglas especiales para tipos específicos de datos personales, tales como datos sensibles, financieros, entre otros. Para los propósitos de este artículo, nos enfocaremos únicamente en la información personal general y proporcionaremos sólo algunos ejemplos de clases especiales de datos personales.

11 Jackson y Hughes (2015), p. 6.

12 Davara (2015).

13 Por ejemplo, al firmar formularios de compra en línea, para contratar un servicio, navegar en un determinado sitio web, o completar encuestas.

14 Tales como entidades financieras o grandes empresas.

15 Australian Communications and Media Authority (2013), p. 14.

fuentes de información.[16] Esta inmensa cantidad de datos depende de pequeños ingresos de datos, tales como información sobre personas, lugares, sensores, teléfonos celulares, patrones de clics, entre otros. Lo datos se generan por medio de actividades cotidianas, actividades en línea, hábitos de consumo y comunicaciones de un individuo determinado.[17] La idea de *big data* es recolectar suficiente información acerca del comportamiento de un individuo y, usando la herramienta analítica apropiada, encontrar conexiones y correlaciones entre los datos recolectados.[18] El resultado de esta técnica radica en generar prediciones precisas acerca del futuro, sin que sea necesario el conocimiento del individuo.

Los datos personales tienen un alto valor económico. La información entregada por los usuarios de internet (voluntariamente o sin su conocimiento) y los datos personales generados (como *big data*) es el "nuevo petróleo" de nuestro tiempo.[19] Los datos personales son el componente clave de nuestra economía digital.[20] El acceso a la mayoría de las páginas web es gratuito para el usuario de internet, y las corporaciones generan ganancias a través de la publicidad. La información personal es crucial para direccionar dicha publicidad de acuerdo a los intereses de las personas, determinados en base a sus clics. Más del 90% de los ingresos de Google están basados en publicidad. [21] En los Estados Unidos, más de dos mil millones de dólares son pagados anualmente para obtener información personal de terceros.[22] Los avisos dirigidos son más efectivos que la publicidad no dirigida o genérica. Por ejemplo, la segmentación demográfica, que involucra significativa recolección y análisis de datos, incluyendo "género, ubicación, edad, raza, religión, profesión o ingreso".[23] La segmentación según el comportamiento, vincula el historial de navegación de los usuarios con la publicidad.[24]

16 Jackson y Hughes (2015), p. 198.

17 Jackson y Hughes (2015), p. 199.

18 Lerman (2013), p. 57.

19 El término "los datos son el nuevo petróleo" se ha utilizado desde 2006 en diversas ocasiones por varios individuos. Parece que la primera declaración con dichos términos fue hecha por Clive Humby, matemático británico. Él empleó el término en la *Senior Marketer's Summit* de la Asociación de Publicistas Nacionales (*Association of National Advertisers*) en el Kellog School, en 2006. Palmer (2006) La Autoridad Australiana de Comunicación y Medios atribuye este término al Foro Económico Mundial. *Australian Communications and Media Authority* (2013), p.1.

20 Jackson y Hughes (2015), p. 197.

21 *Alphabet Inc.* (2016).

22 Zax (2011).

23 Goldberg y Wine (2012), p. 31.

24 Goldberg y Wine (2012), p. 31.

3. MARCO LEGAL DE LA PROTECCIÓN DE DATOS: DESCRIPCIÓN, PRINCIPIOS Y CONSECUENCIAS PRÁCTICAS

Australia y Chile son diferentes en cuando a su aproximación jurídica a la protección de datos. Mientras que ambos tienen diferentes sistemas jurídicos, la comunidad internacional ha abordado la necesidad que tanto Australia[25] como Chile[26] tienen de ajustar y mejorar sus respectivos estándares jurídicos de protección de datos personales, proporcionando una sólida oportunidad para explorar las fortalezas y debilidades de ambas jurisdicciones por medio de cinco principios comunes.[27] El análisis de las consecuencias prácticas de las infracciones a la legislación sobre privacidad de la información probará la insuficiencia de la protección de datos en ambos regímenes legales.

3.1. Sistemas de protección de la privacidad en Australia y Chile: descripción

Una breve revisión de los sistemas australiano y chileno de protección de datos, incluyendo las significativas similitudes y diferencias entre ambos, será el objeto de discusión en esta sección. Dado que Australia tiene un gobierno federal, nos enfocaremos exclusivamente en la legislación federal.[28]

3.1.1 El sistema australiano de protección de la privacidad de datos

La protección de la privacidad y datos en Australia está regulada en la *Privacy Act 1998* (Cth) (en lo sucesivo "Ley de Privacidad").[29] La Ley de Privacidad regula el procesamiento de datos personales en lo concerniente a individuos por parte de

25 Hace varios años, el Grupo de Trabajo de Protección de Datos de la Comunidad Europea emitió una recomendación, abordando varias inquietudes relativas a la transferencia de datos a Australia. La recomendación abordó la Ley de Enmienda de la Legislación de Privacidad (Sector Privado) de 2000 (*Australian Privacy Amendment (Private Sector) Act 2000*), la cual contiene enmiendas a la Ley de Privacidad. Estas inquietudes estaban principalmente enfocadas en los sectores y actividades excluidos del ámbito de aplicación de la Ley de Privacidad, transparencia hacia los usuarios, así como uso y recolección de datos para marketing directo. La opinión recomendó perseguir el mejoramiento de la aplicación general de la Ley de Privacidad, por ejemplo, adoptando códigos de conducta cuyo cumplimiento sea exigido por el propio Comisionado de Privacidad, o por cualquier adjudicador independiente. *Article 29 Data Protection Working Party of the European Community (2001).*

26 El sistema legal chileno de protección de datos no se ajusta con el estándar establecido por la Organización para la Cooperación y el Desarrollo Económico – OCDE. Se discutió un proyecto de ley en el Congreso, con el propósito específico de ajustar la legislación local a dicho estándar. Sin embargo, esta ley nunca fue aprobada (Boletín N° 8143-03 del 11 de enero de 2012).

27 Mientras que ambas jurisdicciones tienen distintos principios aplicables a sus marcos jurídicos de protección de datos (y varios de ellos son similares), para los propósitos de este trabajo consideraremos cinco principios comunes. Estos principios están más o menos en línea con las directrices sobre protección de la privacidad establecidas por la OCDE.

28 Como un estado constitucional federal parlamentario, Australia combina un gobierno "general" (derecho federal) con gobiernos regionales (estados). De ese modo, todos los estados y territorios australianos pueden tener (y de hecho tienen) diferente legislación en materia de protección de datos. La Ley de Privacidad de 1998 es federal, por lo que es aplicable al país en su totalidad. Para evitar diversas conclusiones en este trabajo, nos enfocaremos en el derecho federal.

29 Hay muchas leyes estatales acerca de cuestiones relativas a la privacidad. Sin embargo, para los propósitos de esta investigación, nos enfocaremos únicamente en la legislación federal.

entidades o agencias públicas, así como de datos sensibles (información de salud) procesada tanto por controladores de datos públicos como privados. Se considera "información personal" a aquella información u opinion que concierne a un individuo identificado o razonablemente identificable.[30] De tal modo, no cualquier información puede ser considerada como información personal en sí misma, pero si, combinada con otra información, se identifica o puede razonablemente identificarse a un individuo vinculado a esta, se transforma en información personal.[31] Dado este amplio enfoque, los datos personales pueden incluir el nombre de un individuo, su dirección, información crediticia, registros médicos, lugar de trabajo, así como sus opiniones personales.[32]

Conforme a la Ley de Privacidad, los individuos tienen derecho a que su información personal sea protegida. Como regla general, los individuos tienen derecho a saber que su información personal está siendo recolectada, cuánta información está siendo recolectada, cómo va a ser utilizada y por quién.[33] El Anexo 1 a la Ley de Privacidad establece los Principios de Privacidad Australianos (en lo sucesivo, "APPs").[34] Hay trece APPs que, en términos generales, se refieren a cinco conceptos básicos: administración, recolección, uso y divulgación, seguridad y acceso, y corrección de información personal.

El primer concepto está reflejado en el APP 1 "administración abierta y transparente de información personal"[35] y APP 2 "anonimidad y pseudonimidad".[36] La recolección está regulada en el APP 3 "recolección de información personal solicitada",[37] APP 4 "manejo de información personal no solicitada",[38] y APP 5 "notificación de la recolección de información personal".[39] El uso y divulgación de datos personales están reflejados en el APP 6 "uso o divulgación de información personal",[40] APP 7 "marketing directo",[41] APP 8 "divulgación transfronteriza de información personal",[42] y APP 9 "adopción, uso o divulgación de identificadores vinculados con el gobierno".[43] La seguridad de los datos personales está contemplada en el APP 10

30 *Privacy Act*, s. 6.

31 *Office of the Australian Information Commissioner, guide* (2015), p. 5.

32 *Office of the Australian Information Commissioner, guide* (2015), p. 5.

33 *Office of the Australian Information Commissioner, rights and responsibilities* (2015).

34 *Privacy Act*, sch. 1.

35 *Privacy Act*, sch. 1, cl. 1.

36 *Privacy Act*, sch. 1, cl. 2.

37 *Privacy Act*, sch. 1, cl. 3.

38 *Privacy Act*, sch. 1, cl. 4.

39 *Privacy Act*, sch. 1, cl. 5.

40 *Privacy Act*, sch. 1, cl. 6.

41 *Privacy Act*, sch. 1, cl. 7.

42 *Privacy Act*, sch. 1, cl. 8.

43 *Privacy Act*, sch. 1, cl. 9.

"calidad de la información personal"[44] y en el APP 11 "seguridad de la información personal".[45] Finalmente, el acceso y corrección de datos personales está reflejado en el APP 12 "acceso a información personal"[46] y en el APP 13 "corrección de información personal".[47]

En lo que respecta a la seguridad de la información personal, el APP 11 dispone que los controladores de datos deben: "adoptar medidas que en las circunstancias resulten razonables para proteger la información: (a) del mal uso, interferencia y pérdida; y (b) de acceso no autorizado, modificación o divulgación".[48] Así y todo, la legislación no indica qué es lo que sería razonable[49] para mantener la información segura, de modo que lo que constituye una "medida razonable" tendría que ser analizado caso a caso.[50] El Comisionado Australiano de la Información (*Australian Information Commissioner*) es la autoridad provista de competencia para investigar reclamos sobre privacidad por parte de individuos.[51] El comisionado puede promover conciliación entre las partes, efectuar determinaciones e iniciar procedimientos; pero no tiene la facultad de hacer cumplir la ley por sí mismo, aun cuando puede incoar acciones para hacer cumplir sus determinaciones.[52] El tribunal analizará cada caso y determinará si hubo una infracción de ley, estableciendo si hay mérito para la imposición de penas civiles.[53]

En enero de 2015, la Oficina del Comisionado Australiano de la Información (*Office of the Australian Information Commissioner*, "OAIC"), emitió una guía de consulta sobre seguridad de la información.[54] Si bien esta guía no es legalmente vinculante,

44 *Privacy Act*, sch. 1, cl. 10.

45 *Privacy Act*, sch. 1, cl. 11.

46 *Privacy Act*, sch. 1, cl. 12.

47 *Privacy Act*, sch. 1, cl. 13.

48 *Privacy Act*, sch. 1, cl. 11. 1.

49 De acuerdo a la Oficina del Comisionado de la Información Australiano (*Office of the Australian Information Commissioner*), "razonable" (*'reasonable'*) y "razonablemente" (*'reasonably'*) deben ser considerados en su "significado ordinario, siendo bases conformes a la razón y capaces de una explicación sólida" (*'their ordinary meaning, as being bases upon or according to reason and capable of sound explanation'*). *Office of the Australian Information Commissioner, guidelines* (2015), sch. B, 22.

50 El test de medidas razonables es un examen objetivo y "debe ser aplicado de la misma manera que ´razonable´". (*The reasonable steps test is an objective test, and 'is to be applied in the same manner as "reasonable"'*). *Office of the Australian Information Commissioner, guidelines* (2015), sch. B, 23.

51 La Oficina del Comisionado de la Información Australiano (*Office of the Australian Information Commissioner*) recibe reclamos luego de que el individuo ha reclamado directamente a la agencia u organización involucrada en la infracción a la seguridad de los datos. Si dicha agencia u organización no responde dentro de treinta días, o si la respuesta es insatisfactoria, entonces el individuo tiene el derecho a presentar un reclamo ante la Oficina del Comisionado de la Información Australiano.

52 *Privacy Act*, pt. V.pt V.

53 *Privacy Act*, pt V.

54 Conforme a las funciones del Comisionado provistas en la Ley de Privacidad, s. 28 (1).

fue elaborada para ayudar a agencias de gobierno y a organizaciones privadas a ajustar su conducta a sus obligaciones de acuerdo con la Ley de Privacidad. La OAIC indica que la guía puede ser relevante incluso para organizaciones que no se encuentran dentro del ámbito de aplicación de la Ley de Privacidad. La OAIC acudirá a la guía al investigar un reclamo sobre seguridad de la información.[55] En marzo de 2015, la OAIC publicó también directrices acerca de los APPs,[56] a fin de "promover la comprensión y aceptación"[57] de los mismos.[58]

En lo que respecta al consentimiento del titular de los datos, como regla general, la Ley de Privacidad requiere que dicho consentimiento sea expreso o tácito[59], mientras que el procesamiento de datos sensibles[60] requiere de consentimiento expreso[61]. La Ley de Privacidad se aplica a actividades realizadas en Australia. También se aplicará a actividades que tienen lugar en el exterior si hay una vinculación con la jurisdicción australiana.[62] Todos los APPs se aplican, en principio, a entidades privadas y agencias u oganismos estatales o federales. Están exceptuadas de la aplicación de la Ley de Privacidad las organizaciones de medios (durante la realización de actividades periodísticas), partidos políticos registrados, autoridades, individuos actuando fuera del ámbito de los negocios, empleadores actuando en lo concerniente a los registros de sus empleados, y pequeñ*os operadores de negocios.*[63]

3.1.2 El Sistema chileno de protección de la privacidad de datos

Desde junio de 2018, la protección de datos es un derecho constitucional en Chile.[64] La Ley N° 19.628 sobre Protección de la Vida Privada regula el tratamiento de los datos personales (en lo sucesivo, "LPD").[65]

55 *Office of the Australian Information Commissioner, guide* (2015), p. 2.

56 *Office of the Australian Information Commissioner, guidelines* (2015), sch. B, 22.

57 *Privacy act*, s. 28 (1)(c)(i), "*promote and understanding and acceptance*".

58 *Office of the Australian Information Commissioner, guidelines* (2015), sch. B, 22 (i).

59 *Privacy Act*, s. 6 (1).

60 Bajo la Ley de Privacidad, "información sensible" es información u opinión sobre el origen étnico o racial de un individuo, sus opiniones políticas, creencias religiosas o filosóficas, orientación sexual, registros de antecedentes penales, información de salud, información genética o biométrica (*Privacy Act*, s. 6 (1)).

61 *Privacy Act*, sch. 1, cl. 3.3. .

62 *Privacy Act*, ss. 5B, 13D, 16C. .

63 *Privacy Act*, ss. 7B-7C.

64 La reforma constitucional fue introducida para lograr un más alto estándar de protección de datos, en conformidad con el estándar internacional de la OCDE, buscando seguir la tendencia europea. Asimismo, en el resto de Latinoamérica, varios países ya contaban con este nivel constitucional de protección de datos. En Chile, la Ley Nº 21.096 del 16 de junio de 2018 consagra el derecho a protección de los datos personales.

65 Ley Nº 19.628 LPD.

La LPD establece una amplia definición de datos personales, como "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables".[66] De tal modo, dato personal será aquella información sobre un individuo en internet, generada por el usuario en línea. El sujeto sobre quién versa la información solo puede ser un individuo ("persona natural"),[67] no una persona o entidad moral o jurídica.

Banco de datos (o base de datos) es cualquier fuente de datos personales.[68] La LPD aplica al responsable por los datos (o recolector de datos), quien puede ser una persona natural o jurídica, una entidad privada o un organismo o agencia gubernamental.[69] La LPD también aplica al tratamiento de datos, el que consiste en cualquier operación o procedimiento técnico que permita la recolección, almacenamiento, grabación, organización, elaboración, selección, extracción, confrontación, interconexión, disociación, comunicación, cesión, transferencia, transmisión o cancelación de datos personales, o su uso en cualquiera otra forma.[70]

Conforme a lo anteriormente expuesto, la información generada u obtenida en internet puede ser considerada como dato personal si dicha información puede ser asociada a un individuo específico. El responsable por la información será cualquier persona que lleva a cabo el tratamiento de los datos. Considerando el amplio ámbito que abarca el procesamiento de datos, de acuerdo a la LPD, incluso el almacenamiento de datos personales en un sitio web[71] podría calificar como tratamiento de datos.

El tratamiento de datos, como regla general, solo puede ser realizado mediando el consentimiento previo, informado y por escrito del sujeto titular de los datos. De acuerdo con el artículo 4, el titular de los datos debe ser informado acerca de las fuentes de los datos recolectados; el propósito por el cual están siendo recolectados; la identidad de todas las entidades o individuos que recibirán regularmente los datos; y en relación a datos para investigaciones, estudios de mercado o encuestas de opinión pública, si acaso las respuestas son obligatorias u opcionales.[72]

66 Art. 2 f) LPD.

67 Art. 2 ñ) LPD.

68 Banco de datos es, de acuerdo a la LPD, el "registro o banco de datos, el conjunto organizado de datos de carácter personal, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos." (Art. 2 m) LPD).

69 Art. 2 n) LPD.

70 Art. 2 o) LPD.

71 Tales como datos personales entregados o creados en plataformas de redes sociales, juegos online, entre otros.

72 Art. 4 LPD.

Exenciones a la necesidad de recabar el consentimiento del individuo son los tratamientos de datos que involucran a la libertad de expression y las actividades de prensa,[73] funciones o actos de autoridades, seguridad nacional o práctica nacional, así como la información recolectada de fuentes públicas.[74]

La LPD no establece expresamente los principios de la protección de datos, pero consagra los derechos del titular de los datos y las obligaciones del controlador de los datos. Las personas tienen el derecho a requerir información al responsable de los datos acerca de los datos que tiene en su poder y que se vinculan con el titular de los datos, su fuente y receptores, el propósito de la recolección y almacenamiento de los mismos, e información acerca de las personas o entidades a quienes sus datos son transferidos regularmente.[75] El titular de los datos también posee el derecho a que los datos se modifiquen en caso de que sean erróneos, imprecisos, conduzcan errores o sean incompletos,[76] así como el derecho a la eliminación de los datos, en caso de que su almacenamiento carezca de base jurídica o si esta ha expirado.[77] Este derecho también se aplica cuando el individuo ha autorizado voluntariamente el uso de sus datos personales para propósitos comerciales, pero desea dejar de recibir dicho tipo de comunicación.[78]

La LPD regula la transmisión de datos personales como tratamiento de datos. Por ello, la comunicación de datos personales a terceros requiere de la autorización escrita del titular de los datos. "Comunicación de datos" o su "transmisión" es definida como "dar a conocer de cualquier forma los datos de carácter personal a personas distintas del titular, sean determinadas o indeterminadas".[79] La LPD no regula la transferencia transfronteriza de datos personales, y no hay restricciones para la transferencia de datos personales a ciertos países o jurisdicciones. La LPD aplica a todos los datos personales recolectados en Chile y en relación a un sujeto titular de datos que está localizado en Chile. Así, aún si los datos han sido transferidos al extranjero, el tratamiento de dichos datos debe ser realizado, en principio, conforme a las disposiciones de la LPD. [80]

Las sanciones dependen de las regulaciones infringidas. El titular de los datos está legitimado para ejercer los derechos de información, modificación, cancelación o bloqueo de datos personales por medio de un requerimiento directo dirigido al

73 Ley N° 19.733.

74 Art. 4, 9, 15, 20 LPD.

75 Art. 12 LPD.

76 Art. 6 LPD.

77 Art. 9, 12 LPD.

78 Art. 12 LPD.

79 Art. 2 c) LPD.

80 Esta aplicación de las regulaciones chilenas en el extranjero es teórica, considerando el elevado consumo de tiempo y los costos de los procedimientos destinados a hacer cumplir la LPD en el extranjero, y que no hay tratados internacionales específicos a este respecto. Hasta donde sabemos, y hasta la fecha, no hay jurisprudencia relativa al cumplimiento de las regulaciones chilenas en materia de datos en el extranjero.

controlador de los datos. Este último debe responder dentro de dos días hábiles. Si le toma más tiempo responder, o si deniega la solicitud por cualquier razón que no sea seguridad nacional o interés público,[81] se le podrá imponer multas. Por lo tanto, el responsable por los datos está sujeto a una regla de responsabilidad estricta. Todas las multas que se impongan serán a beneficio fiscal, sin perjuicio del derecho general a demandar por daños al responsable de los datos.

No hay una autoridad o agencia de protección de datos en Chile.[82] Para hacer cumplir las disposiciones de la LPD, así como para imponer multas y obtener indemnizaciones de perjuicios, el titular de los datos tiene que interponer acciones ante los tribunales de justicia.

3.1.3 Análisis

Ambas jurisdicciones presentan similitudes y diferencias en cuanto al marco jurídico de la privacidad de los datos. Dada la amplia definición de información personal, la información proporcionada o generada en línea es considerada como datos personales en ambos regímenes. La LPD ofrece un regimen sancionatorio bajo una regla de responsabilidad estricta únicamente en cuanto a las multas, pero no en lo concerniente a los daños. En Australia, el titular de los datos tiene que probar los daños ante los tribunales de justicia, y las regulaciones se aplican únicamente a agencias de gobierno u organismos estatales en tanto controladores de datos (excepto en el caso de procesamiento de datos sensibles). Australia contempla en su legislación disposiciones expresas de APPs, así como una autoridad de privacidad de datos, y el consentimiento tácito es permitido, incluso en silencio del individuo. En Chile no hay autoridad de protección de datos, el consentimiento expreso es la regla general, y los individuos, entidades privadas y organismos estatales pueden ser considerados controladores de datos.

A pesar de estos enfoques jurídicos relativamente diferentes, ambos marcos legales son insuficientes para proporcionar adecuada protección de datos, debido a su inhabilidad para observar ciertos principios básicos de protección de datos. Las siguientes secciones ponen en evidencia estas debilidades por medio de dos análisis: cinco principios comunes de privacidad de datos y las consecuencias prácticas de las infracciones de regulación en materia de protección de datos.

81 Si el titular de los datos impugna el argumento de "seguridad nacional" o "interés público" entregado por el controlador de los datos, los tribunales serán competentes para decidirla controversia. (Art. 16 LPD).

82 El Consejo para la Transparencia fue establecido por la Ley N° 20.285 sobre Transparencia y Acceso a la Información Pública. El Consejo es el organismo estatal cuya principal tarea es fiscalizar la transparencia del Estado, el derecho a acceder a información pública, así como los procedimientos para ejercer dicho derecho y su protección. En este sentido, el Consejo está facultado a exigir el cumplimiento de las normas de transparencia en caso de que haya agencias estatales involucradas. Sin embargo, un proyecto de ley que busca modificar significativamente la LPD está considerando al Consejo como la autoridad a cargo de fiscalizar y hacer cumplir la LPD. Detallamos esta propuesta en la sección 4.2 de esta investigación.

3.2 Principios de protección de datos

La protección de datos tiene como objetivo garantizar la privacidad de las personas, asumiendo un control práctico y realista del uso y propósitos de sus datos personales, así como de la habilidad del individuo para desafiar este uso en caso de que se extienda a propósitos que vayan más allá del ámbito de su consentimiento.[83] Los siguientes cinco principios son transversales, esto es, son la base de la mayor parte de las legislaciones domésticas que protegen la identidad e información de los individuos.[84]

El primer principio es el consentimiento, lo que generalmente significa que el titular de los datos es el único que tiene derecho a proporcionar autorización para el procesamiento de datos. Las exenciones a este principio incluyen los datos recolectados de fuentes públicas y la seguridad pública. El segundo principio es la calidad de los datos: los datos a ser procesados deben ser pertinentes, adecuados y delimitados a los propósitos del procesamiento de datos. Este principio está vinculado a la permanente actualización de los datos. El tercer principio es la información en la recolección de datos: el controlador de los datos debe proporcionar información precisa al titular de los datos, respecto del tipo de información recolectada, el propósito del procesamiento de datos y los receptores de la información. El responsable de los datos debe también informar al titular de los mismos sobre su derecho de acceso, rectificación y cancelación de la información proporcionada. El cuarto principio es la transferencia de datos personales: la garantía de que la información personal recolectada solo será transferida a terceros mediando el consentimiento previo del titular de dicha información, y en relación a los propósitos del procesamiento de datos. Finalmente, el quinto es el principio de no discriminación: el procesamiento de datos no puede crear discriminación arbitraria en lo relativo a raza, color, vida sexual, religión, opinión política o cualquier otra creencia o convicción.[85]

El siguiente análisis está enfocado en determinar hasta qué punto estos principios han sido implementados en Australia y Chile, lo que es relevante para entender por qué ambos regímenes no son suficientes ni eficientes para lograr un adecuado nivel de protección de datos.

3.2.1 Consentimiento

(a) Australia

La sección 6 de la Ley de Privacidad dispone que el consentimiento del titular de los datos se define como "consentimiento expreso o implícito",[86] sin ninguna otra guía. El OAIC, en sus directrices de los APPs[87] indica que el controlador de datos no debe asumir el consentimiento de un individuo sobre la base de que éste "no objetó

83 Aponte (2007), p. 112.

84 Barrera (2013), p. 13.

85 Aponte (2007), pp. 115-116.

86 *Privacy Act*, s. 6.

87 *Office of the Australian Information Commissioner, guidelines* (2015), sch. B, 22.

una propuesta de manejar la información personal en una determinada forma",[88] incluso si el procesamiento de datos personales o la divulgación de los mismos "parezca ser ventajosa para dicha persona".[89]

El consentimiento tácito debe ser admitido cuando pueda ser razonablemente inferido. De acuerdo a las directrices de la OAIC, es "muy difícil" considerar el silencio como consentimiento tácito.[90] Por ello, el consentimiento debe ser voluntario e informado.[91] El consentimiento parece ser relevante en la aplicación de varios APPs. Sin embargo, no está expresamente contemplado como principio. En algunas situaciones, el consentimiento "es una excepción a la prohibición general"[92] como en APP 3.3(a) y APP 6.1(a). Un usuario de internet proporcionará y generará información personal diversa y significativa. Entonces, el consentimiento acerca del procesamiento de datos personales puede fácilmente ser considerado implícito, por ejemplo sólo para usar o navegar en un sitio web, como en la mayor parte de las transacciones comerciales basadas en internet. Con todo, sacrificar la privacidad de los datos es la aproximación correcta. Con el consentimiento expreso como regla general, el titular de los datos tendría (al menos) que leer y reconocer la información general de los datos procesados.[93]

En algunas circunstancias no será possible para el titular de los datos retirar su consentimiento.[94] Considerando el consentimiento tácito, es (al menos) cuestionable que el silencio del individuo pueda constituir consentimiento. El silencio nunca debiera ser tenido por consentimiento. Esto tendría consecuencias tales como transacciones de negocios más lentas. Sin embargo, las transacciones comerciales efectuadas por medio de internet no debieran traer consigo un sistema de datos privados desprotegido.

(b) Chile

Bajo el marco jurídico chileno, el consentimiento del titular de los datos para su procesamiento debe ser expreso y por escrito.[95] No hay consentimiento implícito, y el silencio no es una forma de consentimiento. Esta aproximación proporciona certeza legal tanto para el sujeto titular de los datos como para el controlador de los mismos, en lo que respecta a la información recibida y alámbito del procesamiento de datos.

88 *Office of the Australian Information Commissioner*, *guidelines* (2015), sch. B, 9.

89 *Office of the Australian Information Commissioner, guidelines* (2015), sch. B, 9.

90 *Office of the Australian Information Commissioner, guidelines* (2015), sch. B, 10.

91 *Office of the Australian Information Commissioner, guidelines* (2015), sch. B, 10.

92 *Office of the Australian Information Commissioner, guidelines* (2015), sch. B, 9.

93 No estamos asumiendo que cada usuario de internet realmente lea y entienda los "términos y condiciones" o la "política de privacidad" de los diferentes sitios web. Pero el objetivo es proporcionar información al usuario de los datos, y contar con un registro o prueba de dicho consentimiento relativo al tratamiento de los datos.

94 Jackson y Hughes, p. 204.

95 Art. 4 LPD.

Por otra parte, no pueden existir cláusulas contractuales (como los "términos y condiciones" de una página web) con limitaciones a los derechos de información (acceso), modificación, supresión, y bloqueo de datos personales.[96] El consentimiento expreso permite al usuario de los datos conocer una base legal relativa a qué información será procesada, el propósito de su recolección, sus derechos, así como la identidad del banco de datos. En el ambiente en línea este consentimiento usualmente se refleja en el mecanismo de la casilla de verificación ("estoy de acuerdo con los términos y condiciones"). Por lo tanto, es posible tener un registro de dicho consentimiento.

3.2.2 Calidad de los datos

(a) Australia

De acuerdo al APP 10, el controlador de los datos debe tomar medidas razonables para asegurar que la "información personal sea fidedigna, actualizada y completa".[97] La OAIC reconoce que la "mala calidad" de los datos personales puede impactar la privacidad de los individuos.[98] Los datos personales son fidedignos cuando no contienen errores o defectos. Que estén actualizados significa que deben ser contemporáneos y actuales. Que la información personal sea completa significa que esta presenta una visión verídica o completa (esto es, opuesto a una visión engañosa o parcial). Los datos personales serán relevantes si poseen una conexión con el propósito para el cual están siendo procesados.[99]

(b) Chile

La LPD dispone que los datos personales deben ser eliminados cuando no hay base legal para registrar y archivar información personal. Adicionalmente, la información que contenga errores o sea incompleta, debe ser corregida/modificada. Se bloquearán los datos personales inexactos o información de dudosa validez (en cuanto a su vigencia).[100] Asimismo, los datos personales deben ser fidedignos, estar actualizados y ser "fieles a la situación real del titular de los datos".[101]

La LPD otorga el derecho al titular de los datos a solicitar la modificación de los datos personales en caso de que la información sea errada, inexacta, conducente a error o incompleta[102], y el derecho a bloquear o eliminar datos personales obsoletos o datos para cuya retención ya no hay base legal.[103]

96 Art. 13 LPD.

97 *Privacy Act*, sch. 1, cl. 10.1.

98 Por ejemplo, la información personal de mala calidad puede conducir a errores en materias tales como: información acerca de hechos (nombre, fecha de nacimiento, dirección); una opinión diferente de aquella genuinamente sostenida por el individuo; o falta de una acreditación que el individuo obtuvo subsecuentemente. *Office of the Australian Information Commissioner, guidelines* (2015), sch. 10, 2 5.

99 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 10, 4-6.

100 Art. 6 LPD.

101 Art. 9 LPD.

102 Art. 12 LPD.

103 Art. 12 LPD.

Sin embargo, es difícil vislumbrar la manera adecuada de observar estas disposiciones. Por ejemplo, la industria financiera utiliza datos personales para evaluar el riesgo financiero de un individuo. Algunas empresas podrían estar utilizando datos inválidos. Y ya que no hay un registro obligatorio de bancos de datos o recolectores de datos, es difícil rastrear dichas compañías.[104] Un control práctico a ejercer por parte del titular de los datos sobre la calidad de la información podría lograrse si la autoridad competente en materia de protección de datos mantuviera un registro de controladores de datos.

3.2.3. Información

(a) Australia

Un controlador de datos recolectará información si dichos datos se obtienen directamente del titular de los datos o de un "registro o publicación generalmente disponible".[105] El APP 3 dispone cuándo y cómo un banco de datos puede recolectar información personal. De acuerdo con la OAIC, el recolector de datos tiene derecho a requerir información personal directa o razonablemente relacionada con sus funciones o actividades, o si es necesaria para el desarollo de las mismas.[106] Adicionalmente, la recolección debe ser realizada conforme a derecho y por medios justos y, en principio, obtenida directamente del titular de los datos. Sin perjuicio de la distinción entre solicitar y recolectar datos personales, este APP se aplica a ambas actividades.[107]

Si bien el APP 3 dispone que la recolección de datos debe ser realizada por medios legales, la Ley de Privacidad no define qué debe entenderse por medios legales. La OAIC proporciona algunos ejemplos de medios antijurídicos, tales como recolectar por medio de piratería informática o usando interceptación.[108]

De acuerdo con el APP 4, los datos personales no solicitados recibidos por un controlador de datos deben ser destruidos, des-identificados y siempre deben ser procesados conforme con los APPs.[109] Ya que la ley no define que debe entenderse por "no solicitados", la OAIC expresa que los datos personales no solicitados son la información recibida sin tomar medidas para su recolección.[110] El APP 5 dispone que los titulares de datos deben ser notificados de que sus datos están siendo recolectados tan pronto ello sea practicable. La OAIC considera que el contenido de dicha notificación debe incluir la identidad de la entidad recolectora de datos y sus detalles de contacto, las circunstancias de la recolección, si la recolección es requerida o autorizada por la ley, los propósitos del procesamiento de datos, las consecuencias de no

104 Asimismo, en Chile, al igual que en Australia, no hay un derecho explícito al olvido o a ser suprimido.

105 *Privacy Act*, s. 6 (1).

106 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 3.3.

107 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 3.4.

108 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 3, 14.

109 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 4, 2.

110 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 4, 3.

recolectar los datos personales, la exhibición habitual de la clase de datos personales recolectados, datos de la política de privacidad (si es aplicable) y si los datos personales serán divulgados en otros países.[111] El APP 12 indica que, como regla general, el titular de los datos tiene derecho a acceder a su información y que mantiene un controlador de datos[112], y el APP 13 dispone que el controlador de los datos debe tomar medidas razonables en orden a corregir cualquier dato personal a requerimiento del titular de los datos. Dicha corrección debe ser efectuada considerando el propósito del procesamiento de datos, su fidelidad, actualidad, completitud, relevancia y que no conduzca a error.[113]

En directa relación con el consentimiento, el consentimiento tácito es un obstáculo para la observancia del principio de información. Si el consentimiento no es expreso, es difícil informar adecuadamente al titular de los datos. La notificación (APP 5) no equivale a consentimiento. La acción de obtener el consentimiento expreso de un titular de datos, realizada por un controlador de datos, necesariamente involucraría la información acerca de la clase de datos personales recolectados, sus propósitos, los receptores de los datos y los derechos del titular de los datos en lo que respecta al procesamiento de datos.

La OAIC ha determinado que, en el ambiente online, los recolectores de datos deben tomar medidas razonables para poner a los usuarios en conocimiento de los propósitos de la recolección de su información personal, v.gr. la dirección IP del usuario de internet.[114]

(b) Chile

El titular de los datos debe ser informado acerca de la fuente de los datos recolectados, los propósitos de la recolección y la posible divulgación de sus datos personales.[115] La LPD otorga al titular de los datos el derecho a requerir al controlador de los datos información acerca de sus datos personales, fuentes de los datos y sus receptores, el propósito del tratamiento de datos, así como la identidad de todas las entidades o individuos que recibirán regularmente los datos.[116]

Adicionalmente, la ley dispone que los datos personales deben ser procesados únicamente para los propósitos para los cuales fueron obtenidos.[117]

111 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 5, 2.

112 *Office of the Australian Information Commissioner*, *guidelines* (2015), sch. 12, 1.

113 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 13, 2.

114 *'HW' and Freelancer International Pty Limited*, AICmr 86 (2015).

115 Art. 4, 6 LPD.

116 Art. 12 LPD.

117 A menos de que los datos sean creados o recolectados de fuentes accesibles al público (Art. 9 LPD).

3.2.4 Transferencia

(a) Australia

El APP 6 dispone que el controlador de los datos solo puede usar o divulgar datos personales para el propósito primario de su recolección, o para un propósito secundario relacionado.[118] Este examen se acerca más a una visiónobjetiva en relación al propósito primario. En lo que respecta al propósito secundario, por regla general, aplicable sólo a datos no sensibles, el controlador de datos desarrollará un análisis subjetivo, a fin de establecer la "probabilidad de que un individuo pueda razonablemente esperar que su información será utilizada o divulgada para un propósito secundario".[119] El término "divulgar" no está definido en la Ley de Privacidad. La OAIC s*eñala que el acto de divulgar datos personales* consiste en hacer accesible dicha información a terceros distintos del controlador de datos o banco de datos. Al realizar esta divulgación (o transferencia), la parte que divulga pierde el control efectivo sobre los datos personales.[120]

El análisis presenta un riesgo cuando se adopta la aproximación subjetiva para determinar la probabilidad de la expectativa del titular de los datos[121], en particular en lo que respecta a la situación general permitida.[122] Si bien la OAIC expresa que este test es "objetivo",[123] la determinación de la probabilidad es más bien un análisis de cada caso en particular, dependiendo directamente de la motivación y voluntad de cada titular de datos. Para que este test sea propiamente objetivo, requiere de estándares y aproximaciones permitidas establecidas en la ley. No en las directrices de la OAIC, las que no son vinculantes.

Para realizar transferencia transfronteriza de datos, el controlador de datos debe haber creído razonablemente que el receptor extranjero está vinculado a obligaciones de privacidad similares a las establecidas por los APPs, o tomar medidas razonables para asegurarse de que el receptor de datos extranjero no vulnere los APPs.[124] La parte que divulga es responsable por cualquier acto del receptor extranjero que importe una infracción de los APPs.[125] De acuerdo con la OAIC, la interacción entre el APP 8 y la s 16C de la Ley de Privacidad crea un marco que incentiva al recolector de los datos a buscar un receptor extranjero que lleve a cabo el procesamiento de datos en conformidad con los APPs. Este es el propósito principal

118 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 6, 3.

119 Jackson y Hughes (2015), p. 224.

120 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 6, 5.

121 *Office of the Australian Information Commissioner*, *guidelines* (2015), sch. 6, 4. I

122 La Ley de Privacidad contempla siete situaciones generales permitidas en su sección 16A. Asimismo, esta parece ser una situación a ser analizada en cada caso concreto. *Office of the Australian Information Commissioner, guidelines* (2015), sch. C, 1-8.

123 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 6,7.

124 *Privacy Act*, sch. 1, cl. 8.1. .

125 *Privacy Act*, s. 16C.

de la Ley de Privacidad, el cual es "facilitar el libre flujo de información a través de fronteras nacionales y al mismo tiempo asegurar que la privacidad de los individuos sea respetada".[126]

El hecho de que el controlador de los datos sea responsable por posibles infracciones de los APPs efectuadas por receptores extranjeros, es un ejemplo macizo de efectiva protección de datos. Considerando el posible conflicto de leyes entre la legislación australiana y la jurisdicción del país del receptor, es altamente probable que el importador de los datos esté en la necesidad de tomar todas las medidas de seguridad necesarias para asegurarse de que el receptor extranjero no vulnerará los APPs. Desde luego, esto no es seguro al cien por ciento, pero es difícil visualizar un escenario en el cual el controlador de los datos estaría dispuesto a tomar un riesgo tan alto de infringir la ley.

En internet, la OAIC ha determinado que la divulgación del nombre del usuario de un sitio web por parte del sitio web mismo o de un blog es una vulneración contra la privacidad de los datos, dado que dicho propósito no es el propósito primario de la recolección de datos ni tampoco un propósito secundario relacionado. El titular de los datos no podría haber, razonablemente, esperado que sus datos personales sean divulgados en línea.[127]

(b) Chile

La LPD no regula la transferencia transfronteriza de datos personales, y no hay restricciones para la transmisión de datos personales a ciertos países o jurisdicciones. Dado lo arriba expresado, es razonable asumir que las disposiciones de la LPD son aplicables a las transferencias transfronterizas de datos personales. La LPD es aplicable a todos los datos personales recolectados en Chile y en relación con titulares de datos localizados en Chile. Incluso si los datos personales han sido transferidos internacionalmente, dicho tratamiento de datos debe ser realizado en conformidad con las disposiciones de la LPD.

Sin embargo, la exigibilidad de la ley en el nivel doméstico es difícil. Los titulares de datos tendrían que interponer acciones por sí mismos, sin el apoyo de una agencia o entidad estatal. Considerando los altos costos y el consumo de tiempo que involucran los procedimientos internacionales, el ya ineficiente mecanismo de protección de la privacidad de datos llega a ser todavía menos eficiente.[128]

126 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 8, 3.

127 *'HW' and Freelancer International Pty Limited*, AICmr 86 (2015), 49 [158].

128 Como fue explicado con anterioridad, en order a interponer acciones en contra de un demandado que se encuentra en el extranjero, el titular de los datos tendría que llevar a cabo una notificación internacional e incoar un proceso judicial en Chile, a fin de establecer jurisdicción en el país de destino. Este proceso tiene asociados elevados costos y consume una gran cantidad de tiempo. Hasta donde sabemos, a la fecha no hay procesos internacionales iniciados por chilenos titulares de datos intentando establecer jurisdicción en el extranjero.

3.2.5 No discriminación

(a) Australia

La Ley de Privacidad contempla un nivel de protección más elevado tratándose de datos sensibles. De acuerdo a la OAIC, el procesamiento de datos de este tipo puede provocar consecuencias adversas para el titular de los datos, tales como "discriminación y mal trato" basado en la raza del individuo, su origen étnico o pertenencia a sindicatos.[129] Asimismo, de acuerdo al APP 3 la recolección de datos debe ser llevada a cabo únicamente por medios legales.[130] Un ejemplo de medio antijurídico sería la recolección de datos personales "en conexión con, o para el propósito de, un acto de discriminación".[131] Adicionalmente, mientras que el APP 12 establece el derecho del titular de los datos a acceder a su información personal, dicho derecho puede ser denegado por el controlador de los datos en caso de que "proporcionarlo sería antijurídico".[132] La OAIC indica que la actividad antijurídica puede incluir discriminación contraria a derecho.[133] La misma lógica es considerada en el APP 13, tratándose de la notificación entre controladores de datos de la corrección de datos personales. Si dicha notificación conduce a discriminación arbitraria o acoso, el controlador de los datos puede abstenerse de realizarla.[134]

Otra manera de observer el imperativo de no discriminación basada en datos personales, es la opción de elegir anonimidad y pseudonimidad cuando esta sea aplicable.[135] La importancia de este APP radica en que habilita a los individuos a "ejercer un mayor control sobre su información personal y a decidir cuanta información personal será compartida o revelada a otros".[136]

Estas son sólidas razones para prevenir la descriminación en el procesamiento de datos personales, particularmente en los diferentes escenarios de responsabilidad por empleo de medios antijurídicos de procesamiento de datos. Dado que la ley no define qué ha de entenderse por "medios antijurídicos", y que las directrices de la OAIC no son vinculantes, debiera haber una disposición expresa en la ley prohibiendo la discriminación arbitraria basada en el tratamiento de datos.

129 *Office of the Australian Information Commissioner, guidelines* (2015), sch. B, 28.

130 *Privacy Act*, sch. 1, cl. 3.5. Ley de Privacidad) sch 1 cl 3.5.

131 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 3, 14.

132 *Privacy Act*, sch. 1, cl. 12.3(f).

133 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 12, 12.

134 *Office of the Australian Information Commissioner*, *guidelines* (2015), sch. 13, 13.

135 *Privacy Act*, sch. 1, cl. 2.1.

136 *Office of the Australian Information Commissioner, guidelines* (2015), sch. 2, 3.

(b) Chile

La LPD establece el principio de no discriminación en el tratamiento de datos, pero únicamente en relación con datos personales de carácter financiero. Los distribuidores de datos personales y los bancos de datos deben observar el mandato de no discriminación en el procesamiento de datos, entre otros principios.[137]

Sin embargo, no hay una disposición expresa general para la no discriminación en el tratamiento de datos. Podría argumentarse que los principios relativos a los datos de carácter financiero también son aplicables a otros tipos de datos, o que la discriminación vulnera las reglas generales en materia de tratamiento de datos. Es deber de los tribunales de justicia interpretar esta disposición.

Globalmente hablando, varias debilidades relacionadas a estos principios están presentes en ambas jurisdicciones, tales como el consentimiento y la ausencia de un deber de registro de los controladores de datos. Un defecto particular radica en la existencia de una autoridad carente de facultades para hacer cumplir la ley (o la inexistencia de autoridad alguna). La siguiente sección analizará las consecuencias prácticas de la vulneración de las reglas de protección de datos.

3.3 Consecuencias prácticas de la vulneración a la protección de datos

En esta sección se analizarán las consecuencias para la protección de datos en cada sistema jurídico, por medio de dos ejemplos hipotéticos. El análisis revelará una insuficiencia general en el sistema sancionatorio.

La efectividad de las sanciones como consecuencia de una infracción de la ley es una cuestión clave en lo que respecta al marco jurídico de la privacidad de los datos. No se alcanzará la responsabilidad, sin sanciones eficientes y prácticas. Por una parte, el uso indebido de información personal no siempre será considerado como una infracción de ley en el ámbito de la protección de datos. Más bien habrá infracción de ley en la medida en que dicho uso indebido cause daño a un individuo. Por otro lado, el uso indebido de datos o su procesamiento no autorizado puede ser llevado a cabo sin causar ningún daño real a su titular. Los dos marcos jurídicos analizados adoptan enfoques diferentes en cuanto a sanciones y penalidades. ¿Cuál enfoque es más apropiado para cada uno de ambos escenarios? Dos ejemplos diferentes de uso indebido de datos personales ilustrarán el funcionamiento del sistema sancionatorio en cada país. El marco legal chileno parece ser más adecuado y funcional para el tratamiento del uso indebido de datos privados, considerando que, al menos parcialmente, sigue un régimen de responsabilidad estricta. El enfoque australiano está basado en el daño efectivamente causado. Sin embargo, ninguno de estos enfoques asegura la aplicación de sanciones.

137 Otros principios aplicables a los datos personales de carácter financiero son los de legitimidad, acceso y oposición, información, calidad de los datos, finalidad, proporcionalidad, transparencia, limitación en el uso, y seguridad en el tratamiento de datos privados (Art. 17, 18, 19 LPD).

El primer ejemplo hipotético es el de un individuo utilizando un motor de búsqueda en internet. La huella digital generada por la búsqueda en internet es utilizada por una corporación para generar publicidad direccionada al usuario. Luego, un correo electrónico no solicitado es dirigido a esta persona, incluyendo publicidad relativa a la búsqueda en internet. El individuo requiere la suspensión de comunicaciones comerciales, y sin embargo se siguen enviando correos electrónicos no solicitados.

El segundo ejemplo hipotético es un individuo postulando a un préstamo bancario. Algunas compañías tienen como negocio la creación y mantenimiento de registros financieros de individuos (y de otras compañías). Este servicio es utilizado para categorizar el riesgo financiero de un individuo o compañía, usando información personal concerniente al estatus financiero del titular de los datos. Es improbable que un banco o entidad financiera le otorgue un préstamo a una persona con registro de cesación de pagos, por ejemplo. Sin embargo, el individuo ya regularizó su situación financiera, pero el controlador de los datos (que posee el registro financiero del individuo) no tiene la información personal actualizada.

En el primer ejemplo, el titular de los datos no otorgó su autorización expresa para recibir publicidad relativa a búsquedas de internet.[138] El resultado de este uso indebido de datos personales es un correo electrónico con publicidad. Si el correo es indeseado, el usuario de internet lo puede eliminar o marcar la dirección del remitente como *spam*, o incluso solicitarle al remitente la suspensión de comunicaciones comerciales (v.gr. "cancelar suscripción"). Es difícil vislumbrar que esto constituya daño efectivo. Podría haber un escenario en el que enviar un correo electrónico o un correo convencional basado en datos personales constituiría per se un detrimento. Por ejemplo, en los Estados Unidos se reportó una vez un caso en el que una tienda de retail envió avisaje relativo a productos de bebé a la familia de una adolescente, basado en la conducta de consumo de esta última. El resultado fue que la familia de la muchacha descubrió que ella se encontraba embarazada.[139] Pero en la situación hipotética, la asunción es que el correo electrónico es inofensivo.

En el segundo ejemplo, el *daño* provocado por el uso indebido de información es más claro. El titular de los datos podría haber dado su autorización para el procesamiento de datos personales de carácter financiero. Sin embargo, dichos datos no se encontraban actualizados. Si el individuo albergaba expectativas razonables (dentro

138 En este escenario asumiré que el consentimiento debe ser previo, informado y por escrito, pese a que hay jurisdicciones en las cuales las regulaciones de privacidad de datos permiten a los controladores de datos señalar en sus términos y condiciones que el consentimiento del titular de los datos se subentiende, o jurisdicciones que tienen un sistema de opt-in para el marketing directo.

139 En 2014, la tienda de retail '*Target*', en los Estados Unidos, recolectó varios datos personales de sus consumidores. Usando su información personal y en base a sus compras pasadas, la tienda creó un perfil exacto de cada consumidor, a fin de enviarles publicidad orientada especialmente a cada uno de ellos. La tienda predijo el embarazo en base a la adquisición de productos que las mujeres tienden a comprar durante las primeras etapas del embarazo (calcio, magnesio o suplementos de zinc). La tienda envió publicidad especialmente orientada a la adolescente embarazada, a la casa de esta última. El padre no supo que su hija estaba embarazada sino hasta que tuvo una conversación con ella, tras recibir la publicidad. Wagstaff (2012).

de la entidad financiera) de recibir el préstamo, y este último fue negado en base a datos inexactos o inválidos, entonces el *daño* es la pérdida de esa legítima expectativa,[140] incluyendo la injusta categorización del individuo como financieramente "riesgoso".

3.3.1 Australia

La Ley de Privacidad está enfocada en el cada caso concreto. Es improbable que el individuo del primer ejemplo demande daños ante un tribunal de justicia.[141]

Una acción por daños en el segundo ejemplo será más probable. Sería más probable que el demandante argumente que el controlador de datos no adoptó las medidas razonables para mantener sus datos personales actualizados. Si el titular de los datos presenta una queja ante la OAIC (asumiendo un controlador de datos sujeto a las decisiones de dicha agencia) y esta última emite una determinación, tendrá que aparecer ante el tribunal de justicia para hacer cumplir dicha determinación, debiendo asumir todos los costos asociados a ello. Parece que la protección efectiva de datos personales no se puede obtener a costos razonables, a menos que el controlador de los datos acepte la mediación o acuerdo de la OAIC.

3.3.2 Chile

En el primer ejemplo, es improbable que el individuo sea capaz de probar daño concreto. Sin embargo, en el contexto de la LPD, si el titular de los datos requiere que el controlador de los mismos los elimine, y este último no responde dentro de dos días hábiles, se impondrán multas sin que se requiera el acaecimiento de daño alguno. Además, el marketing directo está regulado específicamente en las regulaciones de protección al consumidor, con un sistema de *opt-out*: si el individuo expresamente require la suspensión de la comunicación comercial, y el proveedor sigue enviándolos, eso podría ser considerado una infracción de ley. En ambos escenarios, las sanciones podrían consistir en multas, sin discutir la existencia de daño indemnizable.

En el segundo ejemplo, el daño sufrido por el titular de los datos es claro. Consecuentemente, es muy probable que el tribunal falle en favor del individuo y condene al pago de una indemnización por daños.

No hay agencia o autoridad con competencia en materia de protección de datos en Chile. Para hacer cumplir la LPD, aplicar multas y demandar por daños, el titular de los datos necesita interponer acciones directamente ante el tribunal de justicia. En ambos ejemplos, el demandante deberá probar los hechos y el daño, asumiendo todos los costos asociados a las acciones judiciales. La realidad ha demostrado que no se logra una protección efectiva de los datos por medio de estos mecanismos.

140 Puede haber una infinita cantidad de razones por las cuales la persona requirió ese préstamo. Cualquiera de ellas puede ser considerada como el daño causado por el controlador de los datos. Por ejemplo, la necesidad de un boleto de avión para viajar al extranjero y acordar un enorme acuerdo de negocios, el pago de aranceles a una institución académica, la compra de una casa, entre muchas otras.

141 La Oficina del Comisionado de Información Australiano (*Office of the Australian Information Commissioner*) no posee la facultad de imponer multas o sanciones. Se requiere interponer acciones judiciales ante un tribunal de justicia.

3.3.3 Análisis

El marco de protección de la privacidad de datos solo se aplica en Australia, por regla general, a organismos estatales.[142] Mientras que en Australia hay una agencia que recibe reclamaciones concernientes a la protección de datos, esta no parece ser efectiva para lograr una protección adecuada de la privacidad de los datos. En 2014 y 2015, la OAIC recibió 2.841 reclamos y concluyó 1.976 de ellos. De estos últimos, 34.2% fueron objeto de una investigación, mientras que el 36.4% se cerraron sin investigación.[143] Durante dicho período, la OAIC emitió siete determinaciones.[144]

La OAIC no cuenta con las facultades para hacer cumplir la ley. El responsable de los datos puede ajustar su conducta voluntariamente a las consideraciones de la OAIC. Sin embargo, si no hay voluntad por parte del controlador de los datos, entonces será necesario interponer acciones ante un tribunal de justicia, con todos los costos involucrados.

En Chile no hay agencia o autoridad para asuntos de privacidad de datos. La jurisdicción sobre las actividades de procesamiento de datos se limita a los tribunales chilenos. Si bien los tribunales chilenos pueden condenar a indemnizar perjuicios y aplicar multas, las decisiones de los tribunales, al igual que en la mayor parte de los sistemas de derecho continental, no producen jurisprudencia vinculante. Más bien, las decisiones de los tribunales contribuyen a facilitar la interpretación de la ley en casos futuros.

Aproximadamente setenta sentencias relativas a infracciones de ley han sido dictadas por la Corte Suprema desde la puesta en vigencia de la LPD en 1999 hasta julio de 2018.[145] Como una cuestión de acceso a la justicia, este reducido cumplimiento de la LPD puede deberse al costo del proceso judicial, a mecanismos judiciales no efectivos y a disposiciones deficientemente redactadas.[146] La LPD es una ley de protección de datos que otorga varios derechos, pero sin proporcionar vías eficientes para hacerlos valer, y sin contemplar una autoridad de protección de datos. En este escenario, algunos han caracterizado a la LPD como un "lobo sin dientes"[147],

142 A menos de que información sensible sea sujeta al tratamiento de datos.

143 *Office of the Australian Information Commissioner, annual report* (2015), p. 67.

144 *Office of the Australian Information Commissioner, annnual report* (2015), p. 74.

145 Hay una jurisprudencia inconsistente y básicamente impredecible con respectoa la LPD. Esta aparece ampliamente mencionada en diferentes acciones judiciales –entre varias otras regulaciones–, pero su aplicación en definitiva es descartada en la resolución. Asimismo, una enorme cantidad de acciones de protección de derechos constitucionales son interpuestas mencionando e invocando la LPD. Sin embargo, estas resoluciones están dirigidas a proteger derechos constitucionales, de modo que aún en aquellos casos en que se falla a favor del titular de los datos, las cortes no pueden condenar al pago de indemnizaciones de perjuicios ni imponer sanciones. En cualquier caso, estas resoluciones en recursos de protección no siguen una línea clara, sino que oscilan entre diversas orientaciones. De acuerdo a www.poderjudicial.cl (última visita en julio de 2018), de 124 casos relacionados con la LPD, sólo 74 efectivamente aplican dicha regulación.

146 Silva (2015).

147 Silva (2015).

y hay un consenso entre los académicos en torno a los defectos clave de la regulación chilena de privacidad de datos: ausencia de sanciones efectivas, falta de regulación transfronteriza, y el hecho de que el sistema de *opt-out*[148] en el marketing directo no sería constitutivo de consentimiento expreso,[149] así como amplias excepciones para el consentimiento del usuario de los datos, procedimientos inefectivos de tutela judicial, como también la ausencia de una agencia estatal de control, entre otros.[150]

Por consiguiente, ambos sistemas jurídicos, Australia y Chile, presentan significativas diferencias e impedimentos para una apropiada protección de datos personales.

4. ¿SOLUCIONES?

La sección previa explicó cómo los regímenes legales domésticos no son capaces de proporcionar adecuada protección de datos. En nuestra opinion, las cuestiones clave para abordar esta materia residen en los enfoques internacionales para el flujo transfronterizo de datos y la consecuente necesidad de armonización, así como en atender a la necesidad de contar con una autoridad con facultades apropiadas para hacer cumplir las regulaciones (un esfuerzo de una autoridad chilena encaminado a hacer cumplir la protección de datos en internet ante un tribunal de justicia ilustrará esta necesidad).

4.1. Tratamiento y armonización de datos transfronterizos

El procesamiento transfronterizo de datos puede ser considerado como el tratamiento de datos que consiste en la transmisión o transporte de datos personales llevado a cabo en el extranjero por el responsable de los datos y transmitidos directamente a la persona natural o jurídica que tiene que recibirlos en un tercer país, para, de ese modo, sujetarse a un nuevo tratamiento de datos, a ser realizado por él mismo o en representación del transmisor de los datos.[151]

El flujo transfronterizo de datos personales actualmente está incrementándose significativamente, dados los desarrollos tecnológicos, la conectividad y el internet,[152] y debido al flujo de datos en el sector privado y en las entidades estatales. En el sector privado, las multinacionales privadas necesitan que fluya permanentemente infor-

148 Este sistema no requiere de consentimiento previo para la comunicación comercial: *opt-out* significa que el titular de los datos recibe el marketing directo, y tras la recepción, el individuo tiene el derecho a requerir la suspensión de las comunicaciones.

149 Algunos académicos creen que los así llamados *"browse agreements"* (aceptación del usuario basada en el hecho de ingresar a un sitio web) no involucran consenso en lo absoluto, por lo que "en todos esos casos el uso de información [personal] es ilegal". De la Maza y Momberg (2017), p. 53.

150 Viollier (2017), p. 4.

151 Matus y Montecinos (2006).

152 European Commission, "La privacidad de los europeos será un gran desafío en la próxima década, dice el Comisionado de la UE" (*'Europeans' Privacy will be big challenge in next decade, says EU Commissioner'*). Press Release (2010), IP/10/63.

mación entre sus diversas oficinas, y es altamente atractiva la obtención de servicios en países con bajo costo de tratamiento de datos, v.gr. centros de llamado, asistencia técnico. En lo que respecta a las entidades estatales, agencias de distintos países intercambian datos personales. Razones para este intercambio pueden ser la seguridad nacional, la cooperación internacional, el terrorismo, entre varias otras.[153]

En el contexto del flujo transfronterizo, siempre habrá un exportador de datos (remitente de la información personal) y un importador de datos (receptor de la información personal). Una de las cuestiones clave respecto a este flujo internacional es el marco jurídico que protege este intercambio, como también la capacidad del receptor de los datos para adaptarse legalmente a dicho marco jurídico.[154] En otras palabras, cuando se establece la protección jurídica del flujo internacional de datos personales, la parte receptora tendrá que cumplir con dicho estándar legal.

Considerando lo anterior, una solución apropiada podría ser, por ejemplo, la armonización. A este respecto, la antigua Directiva 95/46/CE del Parlamento Europeo y el Consejo Europeo establece que cada estado debe garantizar la libre circulación de datos personales entre estados miembros,[155] reconociendo que la legislación sobre privacidad de los datos puede tener diferentes estándares de protección entre los estados miembros. La Directiva y las legislaciones domésticas recomiendan la realización de flujo transfronterizo de datos sólo a estados miembros con protección apropiada.[156] La Directiva fue derogada por medio del Reglamento 2016/679, Reglamento General de Protección de Datos (en lo sucesivo, "RGPD").[157] Este reglamento dispone la armonización de cada regulación de protección de datos en la Unión Europea, lo que trae consigo la aplicación del RGPD a la transferencia transfronteriza de datos en caso de que se lleve a cabo tratamiento de datos a sujetos titulares de datos que residan en la Unión Europea, aún si el controlador de los datos está ubicado fuera de la Unión.[158]

Otro sólido ejemplo de un esfuerzo de armonización es el Acuerdo Transpacífico de Cooperación Económica (*Trans-Pacific Partnership Agreement*, en lo sucesivo "TPP"),[159] en el cual están incorporados Australia y Chile, entre otros países. El TPP estipula que cada estado miembro debe adoptar un marco legal "que disponga la protección de la información personal de los usuarios del comercio electrónico".[160] "Información personal" significa "cualquier información, incluyendo datos, sobre

153 Guasch (2012), p. 416.

154 Barrera (2013), p. 14.

155 *Directive 95/46/CE of the European Parliament and of the Council* (1995), OJ L 281/31.

156 *Directive 95/46/CE of the European Parliament and of the Council* (1995), OJ L 281/31, Art. 25.

157 *Regulation (EU) 2016/679 of the European Parliament and of the Council* (2016), OJ L 119/1.

158 *Regulation (EU) 2016/679 of the European Parliament and of the Council* (2016), OJ L 119/1, p. 101.

159 *Trans-Pacific Partnership Agreement*, firmado el 4 de febrero de 2015, (2016) ATNIF 2 (no vigente todavía).

160 *Trans-Pacific Partnership Agreement*, Art. 14. 8.

una persona natural identificada o identificable".[161] El TPP expresamente exige que estado miembro permita la transferencia transfronteriza por medios electrónicos "incluyendo la información personal, cuando esta actividad sea para la realización de un negocio de una persona cubierta".[162] Algunos académicos están preocupados por la falta de una definición de "realización de un negocio": debido a este enfoque amplio, puede involucrar toda clase de negocios, incluidos aquellos que no persiguen propósitos comerciales.[163]

Las legislaciones chilena y australiana debieran seguir el ejemplo de armonización del RGPD. Este enfoque haría aplicables las futuras disposiciones del TPP a las relaciones comerciales entre ambos países.

4.2 Protección de datos e internet: la necesidad de una autoridad de protección de datos

Cantidades colosales de datos personales son procesados en internet, tanto aquellos entregados por el usuario de los datos o creados por el uso o navegación en un sitio web. Si bien internet no es una entidad legal y no hay ninguna autoridad supervigilándola, ello no significa que internet escape a toda forma de regulación.[164] Por ejemplo, la Corte Europea de Justicia resolvió en 2014 que bajo circunstancias específicas, los individuos tienen derecho a requerirle a motores de búsqueda online que supriman vínculos con sus datos personales.[165] Esto se conoce como el derecho al olvido.[166] Pero la efectividad de esta clase de regulaciones es dudosa, o al menos presenta desafíos que no existen en el mundo real.

Las acciones en internet no son necesariamente privadas y anónimas.[167] Algunos académicos creen que el uso de dispositivos móviles que generan big data revela información sensible del individuo (comportamiento, creencias religiosas y preferencias sexuales, entre otras), pero no otorgan al titular de los datos control sobre sus datos personales.[168] Mientras que las transacciones por internet se incrementan y pasan a ser más complejas, la amenaza a la privacidad también aumenta con ellas.[169]

161 *Trans-Pacific Partnership Agreement*, Art. 14.1.

162 *Trans-Pacific Partnership Agreement*, Art. 14. 11.

163 Ow (2015).

164 Jay y Hamilton (2003), p. 637.

165 Estas circunstancias son cuando los datos personales no son fidedigos, son inadecuados, irrelevantes o excesivos para los propósitos del procesamiento de datos. *Google Spain SL, Google Inc. con Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (2014).

166 Jackson y Hughes (2015), p. 65.

167 Jay y Hamilton (2003), p. 645.

168 DPM, *Data Privacy Management, and Security Assurance* (2016), p. 245.

169 DPM, *Data Privacy Management, and Security Assurance* (2016), p. 217.

Debido a la rapidez de los cambios tecnológicos,[170] es improbable poder anticipar los cambios que se sucederán.[171] Así, es pertinente que las regulaciones sean neutrales ante la tecnología, lo que significa proveer principios y claras obligaciones legales, pero no modos específicos o particulares de cumplimiento de aquellos o estas. Tal vez esta sea la razón por la cual los comisionados en materia de privacidad desarrollan directrices para la aplicación de la legislación estatutaria en este ámbito, como la OAIC.

Debido a esta falta de regulaciones de seguridad en línea para datos personales, las agencias de gobierno tratan de usar regulaciones de protección al consumidor o legislación de competencia desleal a fin de hacer responsables a los controladores de datos por la seguridad de la información.[172] En algunas jurisdicciones, una falla en mantener segura la información puede ser interpretada como una infracción a las obligaciones de protección a los consumidores o de prácticas comerciales.[173]

En Chile, el Servicio Nacional del Consumidor ("SERNAC") ha interpuesto diversas acciones para obtener el cumplimiento de la LPD. Estas acciones siempre son deducidas en el contexto de una vulneración de la Ley N° 19.496 Sobre Protección de los Derechos de los Consumidores (LPC).[174]La autoridad busca hacer respetar los derechos de privacidad de los datos de los consumidores, en caso de que estos hayan sido vulnerados por un proveedor sujeto a la LPC. Estas reclamaciones no están dirigidas a cautelar el derecho de *opt-out* de comunicaciones comerciales (como correos electrónicos); como se explicó anteriormente, dicho derecho no está consagrado en la LPD, sino en la LPC.[175]

El SERNAC, en sus demandas, ha argumentado que la LPC es aplicable si el interés colectivo de los consumidores es afectado, particularmente en caso de que la infracción a la privacidad de los datos de los consumidores emerge de un acto de consumo. La aplicación de la LPC a casos de protección de datos inicialmente fue aceptada por la Corte Suprema,[176] dado que la LPD establece un ámbito de protección exclusivamente individual, mientras que la LPC protege el interés colectivo de los consumidores.[177] Sin embargo, en la última de estas reclamaciones, y en el contexto de una demanda colectiva dirigida contra los términos y condiciones y la política de privacidad del sitio web de un proveedor,[178] la Corte Suprema, en definitiva, rechazó

170 Jackson y Hughes (2015), p. 134.

171 Koltay (2014), p. 65.

172 Tales como la Comisión Federal de Comercio de los Estados Unidos de América y la Autoridad de Servicios Financieros del Reino Unido. Jackson y Hughes (2015), p. 140.

173 Jackson y Hughes (2015), p. 143.

174 Ley N° 19.496 de 1997.

175 Art. 28 B LPC.

176 *Servicio Nacional del Consumidor con Ticketmaster* (2016).

177 *Servicio Nacional del Consumidor con Créditos Organización y Finanzas S.A.* (2016).

178 Un sitio web tenía en su política de privacidad varias cláusulas "abusivas" en los términos de la

la interacción entre las regulaciones de protección al consumidor y la de protección de datos.[179] El principal argumento de la Corte Suprema para fundamentar este rechazo fue que la LPD es esencialmente individual, careciendo de procedimientos colectivos.[180]

Una preocupación especial emergió de esta resolución de la Corte Suprema: parece que la aplicación de la LPC sería lógica, dado que hay una relación de consumo, un acuerdo formal estándar, y el interés colectivo de los consumidores se vio afectado.[181]

Hay un sólido esfuerzo legislativo en adaptar el actual régimen de protección de datos. El Congreso chileno está discutiendo un Proyecto de Ley que apunta a enmendar la LPD en conformidad con los estándares de la OCDE, creando una agencia de protección de datos.[182] Una de las últimas indicaciones a este Proyecto establece que el Consejo para la Transparencia[183] será esa agencia. No es posible anticipar si esta reforma legislativa será aprobada ni tampoco cuando sucederá.

4.3 Propuestas

Las propuestas siguientes son lo suficientemente amplias para calzar en la legislación vigente o en una futura.[184] Conceptos y principios extensivos llevan a que las regulaciones sobre privacidad de datos funcionen, sobre todo, con una base *ex-post* y restringen la prevención de infracciones a la ley. Esta clase de enfoque genera diversas dificultades en la capacidad de las autoridades de hacer cumplir la ley. Si una regulación ha de ser aplicada en un ambiente online, debiera abordar apropiadamente el ámbito jurídico cubierto por sus disposiciones.

LPC, incluyendo la limitación de los derechos otorgados por la LPD. Bajo la LPC, los términos y condiciones de uso, incluyendo la política de privacidad, son considerados como "contratos de adhesión"; de acuerdo a las regulaciones de protección de los consumidores, estas clases de contratos no pueden contener cláusulas abusivas (Art. 16 LPC).

179 *Servicio Nacional del Consumidor con Ticketek* (2016).

180 *Servicio Nacional del Consumidor con Ticketek* (2016).

181 Momberg (2017), p. 362.

182 Boletines N° 11144-07 y N° 11092-07 refundidos (Chile), enero y marzo de 2017.

183 Véase más arriba nota 82.

184 La extension y límites de cada propuesta debieran ser establecidos utilizando soporte técnico adecuado, i.e. cifras y estadísticas de cada país. Aparte del Proyecto de Ley explicado en la sección 4.2, proponer cambios específicos a los estatutos legales existentes o proponer nuevas regulaciones, es algo que excede el ámbito de este ensayo. Asimismo, estamos en conocimiento de diversos esfuerzos encaminados a mejorar las regulaciones de protección de datos, tanto pasados como actualmente en curso, en Australia y en Chile. Por ejemplo, el Congreso chileno está discutiendo un proyecto de ley que otorga al titular de los datos el derecho al olvido.

Para Australia, ver Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Final Report N°123 (2014); Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report N° 108 (2008).

Para Chile, ver *Boletín N° 10819-07 del 2 de agosto de 2016; Boletín N° 10608-07 del 7 de abril de 2016.*

Primero, la privacidad de los datos en el ambiente online se conseguirá si todos los usuarios de internet otorgan expresamente su consentimiento para el procesamiento de datos. El controlador de datos estará forzado a informar al titular de los mismos respecto a los datos recolectados, los propósitos del procesamiento de datos y los derechos que corresponden al titular, así como la identificación del usuario o controlador de los datos. El mecanismo de casilla de verificación es adecuado para estos propósitos. No todo usuario de internet efectivamente lee los términos y condiciones,[185] pero este mecanismo otorga certeza jurídica.

Segundo, las jurisdicciones debieran tener una agencia pública con competencia en cuestiones de privacidad de datos, en especial para aquellas online. Si bien Australia tiene una autoridad, esta no tiene facultades para hacer cumplir la ley. En el caso chileno, sin perjuicio del derecho constitucional a la protección de datos personales, no hay absolutamente ninguna autoridad. Una agencia estatal (oficina nacional o un defensor del pueblo) a cargo de cuestiones de privacidad de asuntos debiera lidiar con las reclamaciones presentadas por los titulares de datos, realizar investigaciones a los recolectores de datos y contar con la facultad de imponer sanciones administrativas (tales como multas) e interpretar administrativamente la ley. Por consiguiente, las autoridades no estarían forzadas a acudir a regulaciones de libre competencia o de protección al consumidor para tratar asuntos de protección de datos. El acceso a este procedimiento administrativo debiera ser de bajo costo (o gratis) para los individuos. Un procedimiento informal es recomendable. Para observar el debido proceso, las resoluciones de estas agencias debieran poder ser revisadas por un tribunal de justicia.

Tercero, estas agencias debieran tener el poder de convertir en anónimo a un individuo en caso de que este lo solicite desde un ambiente online. Si hay motivos sólidos para creer que la identidad de un individuo ha sido adquirida de un recolector de datos en infracción de la privacidad de los datos, el titular de estos debería tener el derecho a solicitar que la agencia haga cumplir su anonimidad.

Finalmente, el RGPD es un gran ejemplo y guía hacia la armonización: dado que la regulación está dentro del RGPD, no hay necesidad de que cada legislación doméstica sea ajustada. Considerando que ni Australia ni Chile son parte de la Unión Europea, el TPP es una buena oportunidad para lograr la armonización de las regulaciones de protección de la privacidad de datos entre ambos países, v.gr. todos los individuos y entidades capaces de realizar tratamiento de datos debieran sujetarse a regulaciones de privacidad de datos.[186]

185 En 2010, un sitio web de videojuegos, en sus términos y condiciones, expresó que cada usuario de internet que hiciera una compra el primero de abril de 2010, le otorgaría al sitio web una "opción no transferible a reclamar, ahora y para siempre, su alma inmortal" ('*non transferable option to claim, for now and for ever more, your immortal soul*'), a menos que hicieran clic en un vínculo contenido en los términos y condiciones para "anular" ('*nullify*') esta "transferencia de alma" ('*soul transfer*'). Más de 7.500 usuarios no leyeron los términos y condiciones e hicieron clic en el vínculo para "transferir" sus almas al sitio web. La tienda de juegos de internet expresó, luego de que un usuario efectivamente hizo clic en los términos y condiciones, que ellos realizaron el experimento de broma para probar que solo "un doce por ciento de los compradores" leen los términos y condiciones al comprar online. Smith (2010).

186 En el marco jurídico australiano, solo las agencias estatales están sujetas a la Ley de Privacidad, a menos de que la información sensible sea sujeta al tratamiento de datos.

5. CONCLUSIONES

De todos los datos registrados y grabados en la historia humana, la mayor parte han sido creados desde 2010.[187] La conectividad permanente a la red, así como la interminable interacción entre usuarios y sitios web generan una cantidad creciente de información y datos nunca antes vista. La información personal posee enorme valor comercial. Y con el volumen masivo de datos personales en línea, pareciera que que la privacidad en internet ha dejado de ser una norma social.[188]

Consideradas globalmente, las regulaciones de privacidad de datos en internet, no están funcionando apropiadamente. Si bien la privacidad es un derecho jurídicamente protegido, las regulaciones de privacidad de datos son estrechas en Australia y presentan diversos desafíos de aplicación práctica en Chile. Estas regulaciones están funcionando sobre una base ex-post, sin prevención adecuada.

Si bien la ley debiera siempre permanecer tecnológicamente neutral, un enfoque extremadamente amplio no es adecuado para una regulación apropiada en el ambiente online. Contar con los principios de protección de datos establecidos en la ley (como en el caso australiano) incentiva que las resoluciones judiciales se acerquen más a lograr una protección efectiva. Sin embargo, obra en contra de la obtención de protección efectiva, establecer conceptos sin definición, como el de "medidas razonables". Un régimen de responsabilidad estricta es más adecuado para la protección de datos, particularmente en internet.

Australia tiene una autoridad de protección de datos, pero su carencia de facultades para hacer cumplir la ley impide que aquella asegure una protección apropiada. En Chile, diversas decisiones judiciales se relacionan con la LPD, pero esta se ha aplicado directamente solo en setenta resoluciones de la Corte Suprema en el curso de los últimos 19 años. Leyes que contemplan diversos derechos pero que no proporcionan enfoques prácticos apropiados son, justamente, lobos sin dientes.

Asimismo, los desafíos que presenta el procesamiento de datos a nivel doméstico y transfronterizo son bastante similares. El flujo transfronterizo de datos personales es cada día más significativo. ¿Qué constituiría una protección adecuada? Un sólido régimen jurídico de privacidad de datos en cada legislación doméstica promovería, en su interconexión internacional, un marco jurídico internacional globalmente eficiente. La ciberseguridad será un desafío clave en la transferencia transfronteriza de datos, especialmente si la libertad del flujo de datos e información es un principio adoptado, e.g. en el caso del TPP. [189] Dicho tratado constituye una oportunidad sólida (aunque todavía riesgosa) de lograr un regimen jurídico de protección de datos armonizado entre cada uno de sus miembros, y obtener marcos legales internos apropiados en estas materias. Si no se obtiene la armonización

187 Shirky (2013).

188 Johnson (2010).

189 *Trans-Pacific Partnership Agreement*, Arts 14.11, 14.13.

entre jurisdicciones, un ajuste de las legislaciones domésticas sobre protección de datos resulta urgente, en orden a lograr estándares internacionales, v.gr. estándares de la OCDE.[190]

El consentimiento para el procesamiento de datos debiera ser una cuestión clave para Australia y Chile. En el ambiente online, debería ser la regla general. Los titulares de datos, con la enorme cantidad de datos personales en internet, debieran contar con un mecanismo apropiado para ejercer sus derechos en materia de privacidad de datos. Si bien algunos individuos logran que sus datos personales sean efectivamente eliminados o removidos de ciertos controladores de datos en internet, seguimos estando muy lejos de contar con un derecho al olvido efectivo y practicable. En el futuro cercano no parece probable que dicho derecho llegue a ser alcanzable. La cuestión aparentemente trasciende a ese derecho: la extensión del anonimato en internet. No existe una solución simple "en ausencia de una filosofía universalmente compartida".[191]

190 Por ejemplo, académicos chilenos están profundamente preocupados en lo que respecta a la necesidad de ajustar la legislación de protección de datos, en orden a alcanzar los estándares internacionales de la OECD. A este respecto, "la dictación de nuevas leyes es la oportunidad más importante (...) para tener una regulación enfocada en la protección de derechos individuales", considerando particularmente que en Chile, tras 17 años de vigencia de la LPD "hay consenso entre los académicos y la sociedad civil sobre la debilidad de la regulación de la información personal". Viollier (2017), p. 47.

191 Jackson y Hughes (2015), p. 73.

BIBLIOGRAFÍA CITADA

Alphabet Inc. (2016): "Alphabet Announces Second Quarter 2016 Results", en: https://abc.xyz/investor/news/earnings/2016/Q2_alphabet_earnings/index.html.

Article 29 Data Protection Working Party of the European Community, "Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000", Recommendation, enero 2001, en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2001/wp40_en.pdf.

Aponte, José (2007). "La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano", *Revista de Derecho Privado*, N° 12-13, pp. 109-124.

Australian Communications and Media Authority (2013): "Digital footprints and identities – Community attitudinal research", en: http://www.acma.gov.au/~/media/Regulatory%20Frameworks%20and%20International%20Engagement/Information/pdf/Digital%20footprints%20and%20identities%20community%20attitudinal%20research%20pdf.pdf.

Australian Communications and Media Authority (2013): "Privacy and personal data – Emerging issues in media and communications – Occasional paper 4", en: https://www.acma.gov.au/~/media/Regulatory%20Frameworks%20and%20International%20Engagement/Information/pdf/Privacy%20and%20digital%20data%20protection%20Occasional%20paper%204.pdf.

Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report N° 108 (2008).

Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era*, Final Report N° 123 (2014).

Barrera, Isabel (2013): *Estado Situacional de la Protección de Datos Personales en Chile, Regulación Jurídica y Alcances* (tesis de maestría, Universidad de Chile, 2013), en: http://www.repositorio.uchile.cl/handle/2250/115456.

Davara, Miguel Ángel (2015). *Manual de Derecho Informático* (Pamplona, Aranzadi).

De la Maza, Iñigo y Momberg, Rodrigo (2017). "Términos y condiciones: Acerca del supuesto carácter contractual de las autorizaciones para el tratamiento de datos personales en sitios web", *Revista Chilena de Derecho y Tecnología*, N° 2, Vol. 6.

European Commission (2010): "Europeans' Privacy will be big challenge in next decade, says EU Commissioner", en: europa.eu/rapid/press-release_IP-10-63_en.htm

García-Alfaro, Joaquín *et. al.* (eds.) (2016). *Data Privacy Management, and Security Assurance: 10th International Workshop, DPM 2015 and 4th International Workshop, QASA 2015, Vienna, Austria, September 21-22, 2015: Revised Selected Papers* (Vienna, Springer).

Financial System Inquiry (2014): "Interim Report", en: fsi.gov.au/files/2014/07/FSI_Report_Final_Reduced20140715.pdf.

Goldberg, Paul W. y Guo, Mingyu (eds.) (2012). *Internet and Network Economics: 8th International Workshop, WINE 2012, Liverpool, UK, December 10 - 12, 2012 ; Proceedings* (Berlin, Springer).

Guasch, Vicente (2012). "La Transferencia Internacional De Datos De Carácter Personal", *Revista de Derecho UNED,* N° 11, p. 413.

Jackson, Margaret y Hughes, Gordon L. (2015). *Private Life in a Digital World* (Pyrmont, Thomson Reuters).

Jay, Rosemary y Hamilton, Angus (2003). *Data Protection: Law and Practice* (London, Sweet & Maxwell).

Johnson, Bobbie (2010): *"Privacy no longer a social norm, says Facebook founder"*, en: www.theguardian.com/technology/2010/jan/11/facebook-privacy.

Koltay, András (ed.) (2014), *Media Freedom and Regulation in the New Media World* (Budapest, Wolters Kluwer Ltd. CompLex Kiadó).

Lerman, Jonas (2013): "Big Data and Its Exclusions", *Stanford Law Review Online,* Vol. 66, pp. 55, en https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/66_stanlrevonline_55_lerman.pdf.

Matus, Jessica y Montecinos, Alejandro (2006). *El deber de información y el consentimiento para la cesión de datos personales* (Santiago, Lexis Nexis).

Momberg, Rodrigo (2017). "Acciones colectivas y ley N° 19.628 sobre protección de la vida privada y de datos de carácter personal", *Revista Chilena de Derecho Privado*, N° 28, pp. 357-363.

Office of the Australian Information Commissioner (2015): "Annual Report 2014-15", en: www.oaic.gov.au/resources/about-us/corporate-information/annual-reports/oaic-annual-report-201415/oaic-annual-report-2014-15.pdf.

Office of the Australian Information Commissioner (2015): "Australian Privacy Principles guidelines", en: https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/APP_guidelines_complete_version_2_March_2018.pdf.

Office of the Australian Information Commissioner (2015): "Guide to securing personal information – 'Reasonable steps' to protect personal information", en: https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-securing-personal-information.pdf.

Office of the Australian Information Commissioner, (fecha desconocida): "Rights and responsibilities", en: www.oaic.gov.au/privacy-law/rights-and-responsibilities.

Ow, Jack (2012): "The Trans-Pacific Partnership's take on personal data", en: united-kingdom.taylorwessing.com/globaldatahub/article-the-tpp-take-on-personal-data.html.

Palmer, Michael (2006): "Data is the New Oil", en: ana.blogs.com/maestros/2006/11/data_is_the_new.html.

Pew Research Center (2013): "Anonymity, Privacy, and Security Online", en: www.pewinternet.org/files/old-media/Files/Reports/2013/PIP_AnonymityOnline_090513.pdf.

Shirky, Clay (2013): "How very wrong David Simon is about the NSA's capabilities", en: www.theguardian.com/commentisfree/2013/jun/12/david-simon-wrong-nsa-capabilities.

Silva, Paulina (2015): "The regulatory framework for data protection in Chile and Future Challenges", en: united-kingdom.taylorwessing.com/globaldatahub/article_dp_cyber_chile.html.

Sloan, Luke y Quan-Haase, Anabel (eds) (2017), *The SAGE Handbook of Social Media Research Methods* (Londres, SAGE reference).

Smith, Catharine (2010): "7,500 Online Shoppers Accidentally Sold Their Souls To Gamestation", en: http://www.huffingtonpost.com.au/entry/gamestation-grabs-souls-o_n_541549.

Viollier, Pablo (2017). *El estado de la protección de datos personales en Chile* (Derechos Digitales).

Wagstaff, Keith (2012): "How Target Knew a High School Girl Was Pregnant Before Her Parents Did", en: techland.time.com/2012/02/17/how-target-knew-a-high-school-girl-was-pregnant-before-her-parents.

Zax, David (2011): "Is Personal Data the New Currency?" en: www.technologyreview.com/s/426235/is-personal-data-the-new-currency.

NORMAS CITADAS

Australia:

Privacy Act 1998 (Ley de Privacidad) (Cth).

Chile:

Boletín N° 8143-03 del 11 de enero de 2013, que modifica la ley N° 19.628 sobre protección de la vida privada.

Boletín N° 10608-07 del 7 de abril de 2016, que modifica la ley N° 19.628, sobre protección de la vida privada, para efectos de garantizar, al titular de los datos personales, el derecho al olvido.

Boletín N° 10819-07 del 2 de agosto de 2016, que modifica la ley N° 19.628, sobre protección de la vida privada, para sancionar el tratamiento irregular de datos personales.

Boletines N° 11144-07 y N° 11092-07 refundidos en enero y marzo de 2017.

Ley N° 19.733 del 4 de junio de 2001, sobre las libertades de opinion e información y ejercicio del periodismo.

Ley N° 19.628 del 28 de agosto de 1999, sobre Protección de la Vida Privada.

Ley N° 21.096 del 16 de junio de 2018, que consagra el derecho a protección de los datos personales.

Unión Europea:

Consejo de Europa: Convención para la Protección de los Derechos Humanos y las Libertades Fundamentales, abierto para firma el 4 de noviembre de 1950, en vigencia desde el 3 de septiembre de 1953).

Comunidad Europea: Directiva 95/46/CE del Parlamento Europeo y el Consejo del 24 de octubre de 1995 sobre la protección de individuos respecto al procesamiento de datos personales y sobre el libre movimiento de dichos datos.

Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo del 27 de abril de 2016 sobre la protección de individuos respecto al procesamiento de datos personales y sobre el libre movimiento de dichos actos, que deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

Tratados internacionales:

Acuerdo Transpacífico de Cooperación Económica, firmado el 4 de febrero de 2015, no todavía en vigencia.

Convención Internacional de Derechos Económicos, Sociales y Culturales, abierta para firma el 16 de diciembre de 1966, vigente desde el 3 de enero de 1976.

Naciones Unidas:

Declaración Universal de los Derechos Humanos, 10 de diciembre de 1948.

JURISPRUDENCIA CITADA

Australia:

'HW' and Freelancer International Pty Limited, AICmr 86 (2015). Office of the Australian Information Commissioner, 18 de diciembre de 2015.

Chile:

Servicio Nacional del Consumidor con Créditos Organización y Finanzas S.A. (2015). Corte Suprema, 11 de octubre de 2016, Rol N° 4903-2015 (cláusulas abusivas en acuerdos formales, estándar entre proveedores y consumidores)

Servicio Nacional del Consumidor con Ticketmaster (2015). Corte Suprema, 7 de julio de 2016, Rol N°1533-2015 (cláusulas abusivas en acuerdos formales, estándar entre proveedores y consumidores).

Servicio Nacional del Consumidor con Ticketek (2015). Corte Suprema, 6 de diciembre de 2016, Rol N°26932-2015 (cláusulas abusivas en acuerdos formales, estándar entre proveedores y consumidores).

Unión Europea:

Google Spain SL, Google Inc. con Agencia Española de Protección de Datos (AEPD), Mario Costeja González (2014). Corte Europea de Justicia, 13 de mayo de 2014, Caso N° C-131/12, *identificador ECLI: ECLI:EU:C:2014:317.*