Policy Papers

N°02

Juan Carlos Lara, Francisco Vera & Bárbara Soto

Privacidad y nuevas tecnologías, regulación chilena y propuestas de política pública

ONG DERECHOS DIGITALES

Policy Papers

Nº02

ONG Derechos Digitales:
Organización No Gubernamental (ONG) fundada en el año 2005, cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en el entorno digital desde el interés público. Entre sus principales ejes de interés, están la libertad de expresión, los derechos de autor y la privacidad.

Diseño y diagramación: Estudio Navaja
Corrección: Paz Peña

Diagonal Paraguay 458 Piso 2, Santiago de Chile
CP 833003I.
+56 22 6323660
http://derechosdigitales.org
info@derechosdigitales.org

Privacidad y nuevas tecnologías, regulación chilena y propuestas de política pública

Policy paper
ONG Derechos Digitales

Introducción

Atendida la cantidad de información sin precedentes que circula a través de Internet, la importancia de los conceptos de privacidad, vida privada y datos personales ha ido creciendo de manera sostenida. No solo existe la capacidad técnica para acumular información sobre las personas, sino también para ordenarla, sistematizarla e interpretar esa información, con distintos fines. Esto obliga a examinar los riesgos inherentes a la manipulación de datos a través de herramientas tecnológicas y las vías de acción que permitan un adecuado resguardo de los intereses de la comunidad.

I. Privacidad, vida privada y datos personales

El contenido de la idea de "privacidad" ha tenido importante evolución. Entre los primeros esfuerzos por ubicar esa idea, a fines del siglo XIX se definió el derecho a la privacidad como el derecho a estar y permanecer solo[1], en oposición a someterse al escrutinio público, en relación con la invasión a la vida privada. Es decir, el derecho a la privacidad surgió como una forma de hacer frente al hostigamiento por los medios de comunicación social de la época, para guardar reserva respecto de aquel aspecto de la vida personal que legítimamente podía ser excluido de la injerencia de la prensa[2].

Con posterioridad, este primer concepto de privacidad fue gradualmente recogido por la jurisprudencia estadounidense. Desde entonces, con diversos niveles de desarrollo normativo, el derecho a la vida privada está previsto sistemáticamente en los tratados internacionales sobre derechos humanos y, en términos más o menos explícitos, en la Carta Fundamental de los diversos Estados.

Durante las décadas de 1960 y 1970, el interés por asuntos relativos a la privacidad se incrementó con las nuevas tecnologías de la información. El potencial de las herramientas informáticas para recolectar, procesar y analizar información

1 WARREN, Samuel y BRANDEIS, Louis, "The right to privacy", en Harvard Law Review, Vol. IV, núm. 5, 1890. Trad. "El derecho a la vida privada", Ed. Civitas, Madrid, 1995, p. 25.

2 Seguimos en lo sucesivo sobre este punto a CERDA S:, Alberto, "Autodeterminación informativa y leyes sobre protección de datos", en Revista Chilena de Derecho Informático, Núm. 3, Santiago, 2003.

ponía en peligro la vida privada de los individuos, lo que impulsó las demandas por normas específicas que regularan la recolección y el manejo de información personal. Este avance tecnológico dejó en evidencia que no era suficiente el derecho a la privacidad entendido como el derecho a excluir la injerencia de terceros, sino que se hacía necesario ampliar su protección para que el titular pudiera controlar la información personal que le compete. Así, diversos fallos de la Corte Suprema de Estados Unidos extendieron la privacidad (en su ámbito informacional) desde una noción pasiva, que se centraba sólo en la retención de información, a una activa, que releva el control y disposición sobre cuándo, quién y para qué puede acceder a la información que nos concierne.

De esta forma se amplió la concepción de información privada desde un espacio libre de intromisión ajena, a uno donde los titulares de la información pudieran tomar parte en su control, activamente; con la privacidad ya no se aludía a una figura de "espacio reservado" fuera de intromisiones de terceros, sino que a la capacidad del titular de los datos de decidir por sí mismo el control del destino de los mismos.

Estos avances jurisprudenciales y doctrinarios, que tuvieron posteriormente su correlato legal en diversas reformas legales y constitucionales a nivel mundial, dieron lugar a la distinción de una dimensión particular de la privacidad cuyas características la convirtieron en un objeto de estudio y desarrollo separado. Nos referimos a la protección de los datos personales o privacidad informacional en sentido estricto.

Es así que en relación con todos los conceptos individualizados, la protección de los datos personales nace como una derivación del derecho a la privacidad que llega incluso a configurar un nuevo derecho fundamental, reconocido ya en 1983 en la famosa sentencia del tribunal constitucional alemán en el caso de la Ley de Censo de Población: el **derecho a la autodeterminación informativa.** Este derecho confiere a su titular un haz de facultades para controlar la información que respecto de los datos personales que le conciernen puedan ser albergados, procesados o suministrados informáticamente, variando desde el concepto tradicional que manifestaba una faz negativa del derecho.

En suma, la privacidad se vincula a una manifestación jurídica del respeto y protección que se debe a cada persona, protegiendo la dignidad y libertad humana por medio del reconocimiento a su titular de un poder de control sobre su ámbito privado.

Regulación en Chile

En Chile, la doctrina constitucional suele utilizar indistintamente los conceptos de privacidad y vida privada. En la Constitución de 1980, se utiliza el concepto de "vida privada" y no el de "privacidad", porque el concepto de vida privada, según los integrantes de la Comisión encargada de su redacción, se encontraba más desarrollado en el lenguaje común; ya había un reconocimiento por parte de la colectividad de que lo que se respeta es la vida privada, y la privacidad era un término menos conocido[3].

En relación con la dimensión específica de protección de datos personales, ella no está contemplada expresamente en la Constitución Política de la República de Chile, sino que en la Ley sobre Protección de la Vida Privada[4], que define a los datos personales como "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables" (artículo 2 letra f). Se trata de una definición amplia, que abarca cualquier tipo de información que se refiera a un sujeto identificado o susceptible de serlo. El propósito de proteger estos datos es el adecuado amparo de los ciudadanos frente a las eventuales utilizaciones no autorizadas por parte de terceros de su información personal, de manera que el titular de los datos posea el control sobre el destino de los mismos.

II. Diferentes dimensiones de la privacidad y su relación con nuevas tecnologías

Lo señalado en la sección previa se basa en el supuesto que el concepto de privacidad no es unívoco, sino que responde más bien a un fenómeno difuso con diversas dimensiones o acepciones. Esto es producto de la vaguedad del término privacidad, particularmente en su acepción estadounidense de privacy, donde se ha llegado a afirmar que tiene la capacidad "proteica de ser todas las cosas a todos los abogados"[5].

La literatura disponible sobre la materia, proveniente mayormente desde EE. UU., da cuenta de diversas y múltiples definiciones de privacidad. Es más, no solamente existe divergencia entre ellas sino en torno a cuál es el rol que este concepto (y derecho) debe cumplir. Con fines prácticos, y teniendo en mira la relación entre tecnología y privacidad, utilizaremos una clasificación que dis-

3 Acta Oficial Comisión de Estudio de la Nueva Constitución, Sesión 129ª, 1975.

4 Ley N° 19.628, publicada el 28 de agosto de 1999.

5 CAROLAN, Eoin. The Concept of a Right to Privacy (July 19, 2011). Disponible en SSRN: http://ssrn.com/abstract=1889243

tingue entre distintas actividades humanas vinculadas a este derecho[6]:

a. **Privacidad de la información,** también conocida como "protección de datos personales";
b. **Privacidad corporal,** que apunta a la protección física de las personas ante procedimientos invasivos tales como pruebas sanguíneas;
c. **Privacidad comunicacional,** la cual se refiere a la seguridad y privacidad del correo (físico o electrónico), u otras formas de comunicación; y
d. **Privacidad territorial,** que se refiere a la fijación de límites a la intromisión en los medios domésticos y otros tales como el centro laboral o el espacio público.

Todas estas dimensiones presentan grandes desafíos en relación con las nuevas tecnologías e Internet:

a) Respecto de la **privacidad de la información** (privacidad informacional o protección de datos personales), la incidencia de Internet es evidente, puesto que gran parte de las informaciones que circulan, son almacenadas y se procesan en sus redes, revisten la calidad de datos personales al estar relacionados con personas determinadas. De acuerdo a la ley, cualquier página que almacene, procese, indexe o transmita estas informaciones está haciendo tratamiento de datos personales, y por lo tanto conviene analizar si esas conductas afectan o no los derechos fundamentales de los titulares de dicha información, y en qué medida lo hacen.

Esto es particularmente relevante en servicios de Internet tales como redes sociales, muchos de las cuales justamente se basan en la recopilación y tratamiento de esta información, generando perfiles de usuario en los que dicha información se sistematiza y presenta a terceros. Esta información es especialmente valiosa en el mercado y su tratamiento indiscriminado presenta severos riesgos, pues podría permitir conocer o deducir características de la vida de una persona que ella misma preferiría mantener en reserva o lejos del escrutinio público. Los datos recopilados en estos sitios adquieren un gran valor para anunciantes y empresas de estudios de mercado en Internet, y por tanto la legislación debe cautelar que el tratamiento de la misma sea respetuoso de la voluntad de sus usuarios, y especialmente de sus derechos fundamentales.

b) Respecto de la **privacidad corporal,** Internet no juega un rol inmediato, pero la difusión en esta plataforma de los datos obtenidos mediante procedimientos invasivos, tales como los registros de salud o datos biométricos suponen serios

6 La clasificación es tomada de LAURANT, Cedric. Guía de Privacidad para Hispanohablantes, p 17. Disponible en https://www.privacyinternational.org/reports/una-guia-de-privacidad-para-hispanohablantes-0

riesgos por el tratamiento a que puede someterse estos datos. Ahora bien, y teniendo claro que estos riesgos se encuadran mejor dentro de la categoría de protección de datos personales que de privacidad corporal, la irrupción de dispositivos informáticos que pueden implantarse o adosarse en las personas y que pueden conectarse a Internet, puede tornar borrosa la distinción entre ambas clases de privacidad.

c) Respecto de la **privacidad comunicacional,** una plataforma como Internet sirve de soporte a numerosas formas y medios de comunicación, que operan tanto en tiempo real (sistemas de conferencia de voz, vídeo, chat, texto, VNC, etc), como asincrónicamente (foros, tablones de anuncios, correo electrónico, etc).

Tales plataformas de comunicación son susceptibles de ser interceptadas por terceros, conociéndose de esa forma el contenido de las comunicaciones. Es por ello que el respeto a la privacidad de las comunicaciones en Internet presenta enormes desafíos tanto para el sector público como al privado. Este desafío de respeto a la privacidad de las comunicaciones se traduce tanto en que los actores antes señalados aseguren dicha privacidad al interior de sus organizaciones, como también en que sus actuaciones no comprometan la privacidad del resto. En el caso del sector público, que las regulaciones y actuaciones de su parte no afecten de manera indebida o desproporcionada las comunicaciones privadas de las personas, creando reglas y controles que aseguren que solamente se podrá interceptar las mismas en casos justificados y necesarios, de manera proporcional y acotada, todo bajo un debido proceso y control judicial que asegure el pleno respeto de los derechos fundamentales del afectado. En el caso del sector privado, por su parte, deberá asegurarse que quienes tengan acceso a los datos o provean los medios para dicha comunicación no abusen de dicha posición de poder ni afecten la privacidad de los usuarios de los mismos medios, y que respondan a la peticiones de acceso de la autoridad solamente cuando éstas hayan sido hechas de manera legalmente adecuada.

d) Respecto de la **privacidad territorial,** las nuevas tecnologías tienen un gran impacto a través de las tecnologías de registro de información, las que debido al nivel de miniaturización, conectividad y ubicuidad existente, son capaces de inmiscuirse en la esfera privada de las personas, considerando su domicilio, sus conductas en lugares públicos y en su lugar de trabajo, sin filtro ni límites. Ello torna imprescindible el resguardo contra la intromisión indebida en el espacio íntimo de las personas, evitando el registro indiscriminado y abusivo de imágenes, audios, e incluso otros datos como identificadores de redes wi-fi (SSID) de las personas, particularmente cuando no existe claridad en el uso, manipulación y finalidad con la que se recopila la misma información.

III. Estándares internacionales aplicables en materia de privacidad y especialmente en datos personales

A nivel de instrumentos internacionales, el punto de referencia moderno sobre el derecho a la privacidad puede hallarse en la Declaración Universal de Derechos Humanos de 1948, que en su artículo 12 establece: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Por otra parte, la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica) de 1969 establece en su Artículo 11 la protección de la honra, dignidad y vida privada en los siguientes términos: "1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

Por su parte, la Declaración Americana de los Derechos y Deberes del Hombre dispone el derecho a la protección a la honra, la reputación personal y la vida privada y familiar en su Artículo V: "Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar".

Además de las variadas formas de consagración de la privacidad como garantía en materia de derechos humanos, y ya en relación con la protección de datos personales, diversas organizaciones han elaborado estándares mínimos exigibles para implementar esta protección en las normas y prácticas nacionales relacionadas. Entre esos estándares destacan especialmente aquellos elaborados por la OCDE, la Unión Europea y el APEC.

Directrices OCDE[7]

Los Principios de Privacidad de la Organización para la Cooperación y el Desarrollo Económicos se integran en las "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", que fueron desarrolladas a finales de la década de los 70 y adoptadas en 1980. Este instrumento internacional pretende reglamentar el procesamiento de datos personales y flujo internacional de estos datos mediante la adopción de directrices relativas a la protección de la vida privada y de la circulación transfronteriza de datos personales. Estas directrices establecen un estándar mínimo con el objeto de armonizar inter-

7 Texto completo disponible en: http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

nacionalmente las normas relativas al tratamiento manual y automatizado de información personal por los sectores público y privado.

Respecto del flujo transfronterizo de datos personales, a efectos de proteger los derechos humanos, las directrices evitan la adopción de medidas que establezcan obstáculos innecesarios al libre flujo de información, pero, sin embargo, autoriza la restricción del flujo cuando un país no provee un nivel de protección "equivalente". En síntesis, los principios propuestos por la OCDE son los siguientes:

a. **Limitación de recogida:** deberán existir límites para la colecta de datos personales, y ellos deberán obtenerse a través de medios legales y justos.
b. **Calidad de los datos:** Los datos personales deberán ser relevantes para el propósito de su uso además de exactos, completos y actuales.
c. **Especificación del propósito**: El propósito de la recogida de datos se deberá especificar a más tardar en el momento en ésta que se produce.
d. **Limitación de uso**: No se deberá divulgar, poner a disposición o usar los datos personales para propósitos que no cumplan las directrices.
e. **Salvaguardia de la seguridad**: Se aplicarán salvaguardias razonables de seguridad para proteger los datos personales contra riesgos comunes.
f. **Transparencia**: Deberá existir una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales.
g. **Participación individual**: Todo individuo tendrá derecho a que el controlador de datos le confirme tenencia de datos sobre su persona, además de que se le comuniquen los datos relativos a su persona, o la negativa de entrega.
h. **Responsabilidad**: Sobre todo controlador de datos debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

Directiva 95/46/CE[8]

La Unión Europea decidió tomar la iniciativa de adoptar una regulación comunitaria vinculante para los países miembros, iniciativa que adoptó la forma de la Directiva Nº 95/46/CE del Parlamento Europeo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. La Directiva se aplica a los datos tratados por

8 Texto completo disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:ES:PDF

medios automatizados (base de datos informática de clientes, por ejemplo), así como a los datos contenidos en un fichero no automatizado o que vayan a figurar en él (ficheros en papel tradicionales).

La Directiva tiene como objetivo proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento. Dichos principios guardan similitud con los de la OCDE, y son: calidad de los datos, legitimación del tratamiento, resguardo a categorías especiales de tratamiento, información a los afectados por dicho tratamiento, derecho de acceso del interesado a los datos, respeto a excepciones y limitaciones, el derecho del interesado a oponerse al tratamiento, confidencialidad y la seguridad del tratamiento, notificación del tratamiento a la autoridad de control.

En particular, de este instrumento regulador destaca la mención explícita a una autoridad de control de datos personales, lo que ha movido a los países de la Unión Europea a contar con instituciones especiales responsables del control de tráfico de datos personales, con diversas clases pertenencias institucionales y rangos de atribuciones.

Otro aspecto importante es que hace recepción de las directrices OCDE en lo referente a prohibir el flujo cuando un país no provee un nivel de protección equivalente, estableciendo limitaciones en el flujo de datos transfronterizo a países fuera del convenio que no hayan recibido la declaración de "nivel de protección adecuado" de datos personales de acuerdo a los estándares comunitarios.

Marco de Privacidad APEC[9]

El Foro de Cooperación Económica Asia-Pacífico es un foro cuyo principal propósito es facilitar el crecimiento económico, la cooperación técnica y la facilitación y liberalización del comercio y las inversiones en la región Asia-Pacífico. Los lineamientos sobre protección de la privacidad de la APEC fueron aprobados en 2004 y se encuentran orientados principalmente por consideraciones económicas, que reconocen el libre flujo de información como un requisito esencial para el crecimiento económico. Estos principios se basan en los "Principios de Protección de la Privacidad y el Flujo Transfronterizo de Datos" de la OCDE y la Directiva 95/46/CE de la Unión Europea, pero el énfasis en el libre flujo de datos y la escasa tradición de defensa estatal de la privacidad en los miembros de la APEC redunda en el bajo estándar de protección que brinda este instrumento en comparación con los anteriormente reseñados.

Los principios son: la prevención de daño; el aviso previo de políticas de uso;

9 Texto completo disponible en: http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

la limitación de recolección; la limitación de usos de la información personal; la entrega de herramientas de elección al usuario; la integridad de la información; la obligación de mantener medidas de seguridad en los datos; el derecho de acceso y corrección; y la responsabilidad por el tratamiento.

Dado que el marco del APEC se aplica a países con escasa tradición de protección a la privacidad, constituye una buena oportunidad para mejorar los estándares de dichos países, pero al costo de fijar niveles de protección inferiores a los propuestos por OCDE y la Unión Europea[10].

IV. Regulación nacional sobre derecho a la vida privada y datos personales

I. Regulación Constitucional

La Carta Fundamental chilena no cuenta con disposiciones que hagan referencia expresa al derecho a la vida privada o a la autodeterminación informativa; sin embargo, el artículo 19 N°4 de la Constitución asegura el "respeto y protección a la vida privada y a la honra de la persona y su familia", garantía que constituye el punto de partida desde el cual se ha fundamentado la protección de los datos personales por parte de la jurisprudencia y la doctrina nacional[11], entendiendo a la vida privada como el presupuesto del control que el titular de los datos personales tiene sobre su información.

Además de lo anterior, respecto de la privacidad entendida como la protección de las comunicaciones privadas y como protección territorial[12], el artículo 19 N° 5 de la Carta Fundamental consagra "la inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la Ley".

2. Regulación legal

En segundo lugar, el derecho a la vida privada en Chile se encuentra regulado por la Ley N° 19.628 sobre protección de la vida privada, que en realidad se enfoca en regular la protección de datos personales antes que la privacidad

10 Así LAURANT, Cedric. Op. Cit. p.26

11 CERDA S., Alberto, "Legislación sobre protección de las personas frente al tratamiento de datos personales", Centro de Estudios en Derecho Informático, Facultad de Derecho Universidad de Chile, p. 13.

12 Ambas distintas facetas de la privacidad, junto a la privacidad de la información y a la privacidad corporal.

como un fenómeno o derecho omnicomprensivo[13]. Regula el tratamiento que los organismos públicos y particulares efectúen de los datos de carácter personal que se encuentren almacenados en registros o bancos de datos, sean éstos de carácter automatizados o no.

La ley define el concepto de datos de carácter personal o datos personales como "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables" (artículo 2°, letra f), y establece que el tratamiento de datos de carácter personal es posible siempre que se haga de manera concordante con esta ley y para finalidades permitidas por el ordenamiento jurídico.

Sin embargo, la ley parece perder de vista sus propósitos, convirtiéndose en una mera declaración de principios al establecer, por ejemplo, que el tratamiento de los datos personales sólo puede hacerse en virtud de autorización legal o del titular de los datos, ya que del contexto de las normas se desprende que la mayoría de los datos provienen de fuentes de acceso público (por lo que no se requiere autorización para su tratamiento), y además se consagran importantes excepciones, sobre todo en materia de datos personales-patrimoniales[14].

Además de la mencionada ley, también existen reglas sobre la vida privada en el ámbito penal y procesal penal, mediante normas que no entregan suficientes garantías para brindar amparo al derecho a la vida privada frente a la diversidad de ataques a que se encuentra expuesto. De esta forma, el artículo 161-A del Código Penal castiga a quienes por cualquier medio capten, intercepten, reproduzcan, capten, graben, filmen o fotografíen, o difundan, hechos de carácter privado que se produzcan en recintos particulares o lugares que no sean de libre acceso al público. Sin embargo, la protección que ofrece este artículo contiene una confusa redacción que denota imprecisiones de política legislativa y que generan dificultades interpretativas en su aplicación.

Por su parte, el artículo 36 letra b) de la Ley General de Telecomunicaciones sanciona a quien maliciosamente interfiera, intercepte o interrumpa un servicio de telecomunicaciones, y el comiso de los equipos e instalaciones. Sin embargo, esta ley no considera a Internet como un servicio de telecomunicaciones propiamente tal, por lo que su aplicación es difícilmente plausible en ese caso.

En relación con la autorización legal al estado para intervenir comunicaciones privadas de personas, los artículos 218 y 222 del Código Procesal Penal fijan los requisitos para esta actividad. El primer artículo (218) se refiera a la retención e incautación de correspondencia (postal, telegráfica o de otra clase) cuando existan motivos fundados de que fuere previsible su utilidad para la investigación, mientras el segundo (222), dice relación con la interceptación de comuni-

13 De hecho, esta ley lleva un segundo título, cual es "Ley sobre Protección de Datos de Carácter Personal".

14 JIJENA, Renato, "Actualidad de la protección de datos personales en América Latina. El caso de Chile",

caciones telefónicas o de otras formas de telecomunicación, cuando existieren fundadas sospechas de que una persona hubiere cometido o participado en la preparación o comisión de un hecho punible que mereciere pena de crimen, y la investigación lo hiciere imprescindible.

Junto con lo anterior, en el mismo artículo 222 del Código Procesal Penal se norma la obligación de retención de datos personales (datos sobre direcciones IP de conexión a internet de usuarios) por parte de los prestadores de servicio de Internet y la obligación de poner dichos datos a disposición del Ministerio Público. Sin embargo, esta disposición resulta imprecisa y por lo tanto riesgosa a la hora de cautelar los derechos de los usuarios de Internet, ya que no se conoce bien el alcance de la norma, que obliga a los Prestadores de Servicio de Internet a poner a disposición del Ministerio Público esta información que se retiene, sin precisar un estándar legal para que se verifique este acceso.

Dado que los datos sobre direcciones IP de usuarios son propiamente datos personales, consistentes con los conceptos contenidos en la Ley 19.628 y por ende parte de la esfera de protección del derecho fundamental a la vida privada, consagrado en el artículo 19 N°4 de la Constitución Política de la República de Chile, cabe concluir que cualquier acceso del Ministerio Público a estos antecedentes debe llevarse a cabo con el estándar fijado en el artículo 9° del Código Procesal Penal, donde se establece que "Toda actuación del procedimiento que privare al imputado o a un tercero del ejercicio de los derechos que la Constitución asegura, o lo restringiere o perturbare, requerirá de **autorización judicial previa**".

3. Críticas a la regulación

La legislación chilena sobre privacidad, especialmente la Ley de Protección de la Vida Privada chilena, tiene varios vacíos que permiten la afectación grave de derechos fundamentales asociados a la privacidad en nuestro país. En la práctica, la Ley de Protección de la Vida Privada configura un sistema que no garantiza los derechos de las personas, sino que solamente establece un marco legal para el tráfico indiscriminado de datos personales.

Esto se produce porque en la práctica existen nulos incentivos e inexistentes sanciones para que los administradores de sistemas de tratamiento de datos personales resguarden la información tratada.

Por una parte, la Ley de protección de la vida privada regula de manera incompleta e insuficiente los principios rectores en torno al tratamiento de datos personales, a diferencia de lo que ocurre en el escenario internacional, donde cuerpos normativos tales como las recomendaciones de la OCDE contemplan expresamente un número de principios que regirán la aplicación de las normas respectivas.

En Chile en tanto, varios principios, como el de la libertad en el tratamiento de datos personales, de la información y **consentimiento del titular** de los datos,

de finalidad, de calidad de los datos, de protección especial de datos sensibles y de seguridad de los datos, se obtienen solamente después de un proceso de inducción que toma a la actual regulación apenas como punto de partida. La inexistente consagración positiva de estos principios, y su falta de definición autoritativa, crea múltiples dificultades a la hora de interpretar y aplicar la legislación de datos personales.

Por otra parte, la Ley, tras señalar que el tratamiento de datos personales sólo puede efectuarse con autorización legal o el consentimiento del titular (artículo 4°), agrega una excepción de alcance general a esa disposición que termina por desnaturalizar el sistema de protección de datos personales chileno. La disposición (incisos V y VI del artículo 4°) señala que no es necesaria la autorización para el tratamiento de datos personales que provengan o se recolecten de fuentes accesibles al público, bajo una serie de hipótesis que debilitan el tratamiento de datos al prescindir de la finalidad de los mismos. Es decir, se torna más relevante el origen público de los datos que el uso para el cual son recolectados[15].

Otro aspecto cuestionable de la Ley de Protección de la Vida Privada se vincula a la extensión que adquiere el principio de consentimiento a la luz de lo dispuesto en el artículo 10 de la mentada ley, que señala que "No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares". En este escenario, bastaría el mero consentimiento por escrito del titular de los datos para tratar sus datos sensibles, sin obligaciones especiales de cautela o garantía para quienes hacen tratamiento de estos datos, ni consideraciones especiales respecto de las condiciones en que se presta el consentimiento antes indicado.

Con todo lo anterior, la crítica más grave que se le puede efectuar a esta ley radica en la casi completa ausencia de mecanismos especiales de enforcement (observancia forzada) de los derechos allí consagrados, como sí existen en otros sistemas legales. Una de las razones para explicar esta falencia es que el mecanismo contemplado en la misma Ley opera a través de la justicia ordinaria y

15 Ley N°19.628, Artículo 4°, incisos quinto y sexto: "No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al público, uando sean de carácter económico, financiero, bancario o comercial, se contengan en listados relativos a una categoría de personas que se limiten a indicar antecedentes tales como la pertenencia del individuo a ese grupo, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento, o sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios.
"Tampoco requerirá de esta autorización el tratamiento de datos personales que realicen personas jurídicas privadas para el uso exclusivo suyo, de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquéllos."

de forma reactiva, y no a través de un órgano especializado (como se exige en el sistema europeo) con capacidad para fiscalizar, lo que crea serios problemas de especialización, demora en la tramitación de causas y dificultades en el acceso a la justicia. En suma, lo anterior se traduce en un bajo nivel de respeto y consideración a los intereses de las personas en resguardo de su privacidad.

Muchos de los derechos involucrados en la protección de datos personales, partiendo por la revisión de los principios que sustentan estas normas, contemplan la posibilidad de conocer ciertos datos almacenados en bases de datos de entes públicos o privados y entregando la opción de reclamar acceso, modificación o borrado de los mismos por parte de sus titulares, en casos determinados. Este tipo de prácticas envuelven situaciones cotidianas donde una de las partes (el titular de datos) está en una situación de debilidad frente al responsable del tratamiento, debido a diferencias económicas, de información y de poder entre ambos. Ello se hace patente en casos en donde quien colecta y maneja datos es el aparato estatal, o empresas con la capacidad de hacer transitar los datos fuera de las fronteras nacionales. A esto se suman las constantemente expansivas capacidades de almacenar y tratar datos de distinta naturaleza y de la transversalidad de las consideraciones sobre privacidad en distintos ámbitos.

Lo anterior fue considerado en el estudio previo al Convenio 108 del Consejo de Europa de 1981 y su Protocolo Adicional de 2011, como asimismo en la Directiva 95/46/EC sobre Protección de Datos Personales de la Unión Europea, como justificación para la instalación de autoridades estatales de control de datos personales, destinadas a resguardar la privacidad y el tratamiento adecuado de la información de las personas. De este modo se fijó la entrega a agencias públicas e independientes de la competencia sobre esa información[16].

Por cierto, es vital que tales agencias mantengan atribuciones y presupuestos adecuados a su función, pero es aún más crucial que mantengan un nivel de independencia tal que permita un resguardo de intereses fundamentales, incluso contra iniciativas de la autoridad estatal[17].

Razones de eficiencia y especialización, han justificado asimismo la existencia de registros de bases de datos en poder de terceros. Allí donde existen asimismo órganos especializados para el control de los datos personales, son ellos los llamados a mantener y actualizar registros de estas bases de datos, así como a controlar la legalidad de su utilización.

16 Véase al respecto el informe de EU Agency for Fundamental Rights (FRA), Data Protection in the European Union: the role of National Data Protection Authorities. European Union Agency for Fundamental Rights, 2010, p. 14-18.

17 OUZIEL, Pablo, Protecting Privacy or Justifying Surveillance: A Critique of the Data Protection Authority Model. Disponible en: http://www.pabloouziel.com/Academic%20Essay/Protecting%20Privacy%20or%20Justifying%20Surveillance.pdf

Respecto al resto de regulación en materia de privacidad, si bien no son merecedoras de críticas tan severas como las formuladas a la Ley de protección de la vida privada, las leyes chilenas sí suponen problemas para el ejercicio de los derechos fundamentales vinculados a este concepto, como pasamos a señalar.

En materia criminal podemos constatar que delitos cuyo objetivo declarado es la protección de la privacidad, en particular el contemplado en el artículo 161-A del Código Penal[18], sirve de desincentivo a la labor periodística, toda vez que mediante este mecanismo es posible limitar la libertad de expresión inherente a la actividad informativa.

La obligación que impone el artículo 222 del Código Procesal Penal, que ordena que las empresas telefónicas y de comunicaciones mantengan "en carácter reservado, a disposición del Ministerio Público, un listado actualizado de sus rangos autorizados de direcciones IP y un registro, no inferior a un año, de los números IP de las conexiones que realicen sus abonados", carece de la precisión necesaria para identificar en qué casos y bajo qué circunstancias puede ser utilizado por el Ministerio Público, lo que a nuestro juicio es imprescindible para resguardar los derechos fundamentales de los abonados a Internet[19].

La Ley de Transparencia Pública, al otorgar al Consejo para la Transparencia la facultad de "Velar por el adecuado cumplimiento de la Ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado" en su artículo 33 letra m), crea una incómoda situación para la labor de un órgano cuya misión primordial es cautelar la transparencia de las actuaciones del Estado, al darle el rol de velar por el cumplimiento de una Ley que busca fines esencialmente diferentes y casi antagónicos con los vinculados a la transparencia pública.

I. PROPUESTAS DE MODIFICACIÓN LEGAL PROMOVIDAS EN LOS ÚLTIMOS AÑOS

Como hemos visto, en nuestro país la privacidad es percibida de manera dispersa por el legislado, en oposición a un tratamiento integral y sistemático de este

18 El artículo 161-A del Código Penal castiga con penas de reclusión menor y multas a quienes por cualquier medio (ej.: capten, intercepten, reproduzcan, graben, filmen o fotografíen, incluida la difusión de estos registros) registren hechos de carácter privado que se produzcan en recintos particulares o lugares que no sean de libre acceso al público.

19 En Europa, la Directiva 2006/24/CE de retención de datos, que además permite a policías y autoridades obtener datos de telecomunicaciones previa solicitud a un tribunal, ha sido fuente de gran polémica y no ha concluido su transposición. Establece un plazo mínimo de seis meses y uno máximo de dos años para la retención, entregando amplio margen para las finalidades. Países como EE. UU. y Australia actualmente buscan fórmulas para regular obligaciones de retención de datos.

derecho, resultando la creación de leyes que constituyen arreglos temporales a problemas que se van dando en la realidad nacional.

Los proyectos de ley enunciados en el cuadro a continuación representan las iniciativas de reforma legal vinculadas a la vida privada, al manejo de datos personales, o ambos, que demuestren cierta relación con el uso de tecnologías de comunicación e información, y que han sido presentados de manera reciente (esto es, a contar del año 2005) para discusión en el Congreso. Ellos dan muestra de diversos intentos por modificar diversos aspectos del derecho a la vida privada durante los últimos años, con lo que puede apreciarse la fragmentación existente en la regulación de este derecho.

Proyectos de Ley presentados:

Boletín	Año	Título	Resumen	Etapa de tramitación
N° 3796-07	2005	Modifica la ley N° 19.628 de protección de la vida privada, con el fin de evitar el uso abusivo de datos personales o de empresas y de resguardar a los usuarios de correos electrónicos de la propaganda comercial no solicitada.	La propuesta contaba con una ampliación en el ámbito de aplicación de la ley, extendiéndolo a las personas jurídicas; y con una modificación en la definición de "dato sensible" y "fuentes accesibles al público", entre otras.	Archivado sin discusión en sala.
N° 4466-03	2006	Modifica la ley N° 19.628 con el objeto de ampliar los mecanismos de protección de los datos de carácter personal.	Incluye cambios en el concepto de fuente accesible al público, una clasificación de infracciones y sus sanciones, entre otras modificaciones.	Proyecto presentado, en discusión en comisión de cámara de origen
N° 7178-07	2007	Impide acogerse a la eliminación de las anotaciones penales en caso de delitos sexuales contra menores.	Incorpora el siguiente inciso tercero, nuevo, al artículo 1 del Decreto Ley N° 409: "Los beneficios contemplados en este artículo no se concederán a quienes hayan sido condenados por alguno de los delitos contemplados en los párrafos quinto, sexto, séptimo y octavo del título VII del Libro Segundo del Código Penal, contra menores de edad".	Proyecto presentado, en discusión en comisión de cámara de origen

Nº 6120-07	2008	Modifica la ley Nº 19.628 sobre protección de la vida privada y la ley Nº 20.285 sobre acceso a la información pública.	La propuesta incluye el reconocimiento explícito de derechos, la ampliación del margen de sujetos protegidos, el establecimiento de una autoridad de control, la distinción entre "encargado" y "responsable" de la base de datos, el fortalecimiento de los derechos de información, la regulación del flujo transfronterizo de datos, el aumento en las condiciones de seguridad en el tratamiento de datos, el reforzamiento del deber de rectificación y corrección de datos, la regulación de infracciones y sanciones, el perfeccionamiento del sistema de responsabilidad civil y la creación de un registro de bases de datos.	Proyecto presentado, en discusión en comisión técnica previo a discusión en comisión de cámara de origen

Nº 5662-13	2008	Regula el uso de medios informáticos en el trabajo.	Incorporaba los incisos 2º, 3º, 4° y 5° al artículo 154 bis del Código del Trabajo: "En todas aquellas funciones que involucren el uso de medios informáticos o virtuales para el intercambio de información, sean o no propiedad del empleador, éste no podrá interceptar o acceder a las comunicaciones privadas enviadas o recibidas por los trabajadores."; "Asimismo, no podrá almacenar datos personales obtenidos a partir de las anteriores herramientas, sin su consentimiento."; "Lo establecido en el inciso anterior, se entenderá, sin perjuicio de su facultad para limitar o restringir el uso de los anteriores medios para aquellos ámbitos que excedan las funciones prestadas por el trabajador."; "El empleador deberá informar oportunamente al trabajador de las restricciones al uso de los medios señalados.".	Archivado sin discusión en sala

N° 6495-07	2009	Modifica el artículo 19 N° 4 de la Constitución Política, con el objeto de consagrar la protección y resguardo de los datos personales.	Modificaba el artículo 19 N° 4 de la Constitución Política de la República, agregando los siguientes incisos segundo y tercero: "Toda persona tiene derecho a controlar la información que le concierne, de modo de obtener un adecuado resguardo a sus derechos fundamentales. En ejercicio de este derecho, toda persona podrá conocer sus datos personales y los que le afecten personalmente o a su familia, y obtener su rectificación, complementación y su cancelación, si estos fueren erróneos o afectaren sus derechos constitucionales, de acuerdo con las regulaciones establecidas por la ley".	Archivado sin discusión en sala
N° 6594-07	2009	Reforma constitucional que crea una Agencia de Protección de Datos Personales.	Incorpora en el artículo 19°, numeral 4° de la Constitución Política de la República, a continuación de la expresión "familia" un punto seguido y la oración "Habrá una Agencia, autónoma y con personalidad jurídica, encargada de velar por la adecuada de los datos de carácter personal, resguardar la aplicación de las leyes y los derechos de los ciudadanos en la materia y los responsables de los registros privados o públicos".	Proyecto presentado, en discusión en comisión de cámara de origen

N° 7026-07	2010	Modifica la ley N° 19.628 sobre protección de la vida privada, con el objeto de resguardar en mejor forma los datos de carácter personal y sancionar penalmente su tratamiento y cesión indebida.	Modifica la ley N° 19.628, sobre protección de la vida privada, en la siguiente forma: 1.- En la letra i) de su artículo 1°, agrega después del punto aparte (.), que se reemplaza por una coma(,), la siguiente frase: "todo ello, de acuerdo a las regulaciones establecidas por la ley". 2.- En su artículo 5°, agrega al final de su inciso cuarto, después del punto aparte (.) que pasa a ser punto seguido, la siguiente frase: "las infracciones a esta norma, serán penadas conforme a la ley." 3.- En su artículo 7°, agrega un inciso segundo del siguiente tenor: "Quienes comercialicen, faciliten o cedan a cualquier título, los datos personales o bases de ellos, que les corresponda conocer, por razón de su trabajo, serán sancionados con la pena de presidio menor en su grado mínimo." 4.- En su artículo 11, agrega un inciso final, del siguiente tenor:" Para tal efecto, los responsables de dichas bases o registros de datos personales deberán adoptar las medidas de seguridad máxima, que impidan la extracción indebida o sustracción de los mismos".	Proyecto presentado, en discusión en comisión de cámara de origen

N° 7282-07	2010	Deroga la letra A del artículo 161 del Código Penal.	Deroga la letra A del artículo 161 del Código Penal: "Se castigará con la pena de reclusión menor en cualquiera de sus grados y multa de 50 a 500 unidades tributarias mensuales, al que, en recintos particulares o lugares que no sean de libre acceso al público, sin autorización del afectado y por cualquier medio, capte, intercepte, grabe o reproduzca conversaciones o comunicaciones de carácter privado; sustraiga, fotografíe fotocopie, o reproduzca documentos o instrumentos de carácter privado; o capte, grave, filme o fotografíe imágenes o hechos de carácter privado que se produzcan, realicen, ocurran o existan en recintos particulares o lugares que no sean de libre acceso al público".	Primer trámite constitucional
N° 6939-03	2010	Prohíbe el monopolio de la información comercial de carácter personal.	"Ninguna empresa, gremio, asociación o agrupación de cualquier naturaleza podrá tener el monopolio sobre el tratamiento de la información comercial. Por consiguiente, las entidades comerciales, tales como Bancos, compañías de seguros, financieras, casas comerciales y las notarías, tratándose de protestos de cheques, letras o pagarés, podrán remitir la información comercial que produzcan a cualquier empresa, sea persona natural o jurídica que como giro tenga el tratamiento de información comercial."	Proyecto presentado, en discusión en comisión de cámara de origen

Nº 6994-07	2010	Restringe el uso de determinados datos personales existentes en Internet.	Incorpora a la Ley 19.628 sobre protección de la vida privada el artículo 2 bis nuevo: "Los datos personales de carácter sensible de una persona, según lo prescrito en la letra g) del artículo 2 de esta Ley, disponibles en redes sociales en Internet, no podrán ser utilizados por terceras personas, para otros fines, más que para aquellos, que dentro del contexto doméstico o socializador de la red social, sean utilizados o estén disponibles, a menos que cuente con el consentimiento expreso del su titular según lo prescrito en el artículo 4 de la presente ley. Así, los datos que un empleador recabe de sus trabajadores de una red social, no podrá utilizarlos como causal de despido, ni los datos sobre la salud de una persona ser utilizados para ofrecer planes de salud por parte de una empresa. La inobservancia de lo dispuesto en este artículo hará aplicable las sanciones previstas, en el artículo V de esta ley.	Proyecto presentado, en discusión en comisión de cámara de origen

N° 7158-05	2010	Modifica el DFL N° 3 de 1997, de Hacienda, con el objeto de eliminar la información comercial en todo registro o base de datos, transcurridos 5 años desde que la obligación se hizo exigible.	Agrega en el artículo 14 del DFL N° 3 del año 1997 de la Ley General de Bancos, lo siguiente: "En ningún caso pueden comunicarse los datos que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible, de acuerdo a lo señalado en el artículo 18 de la ley N° 19.628."	Proyecto presentado, en discusión en comisión de cámara de origen
N° 7732-07	2011	Modifica el Art. 14 de la ley N° 19.628 sobre protección de la vida privada, prohibiendo y sancionando el envío de comunicaciones comerciales no autorizadas a teléfonos celulares.	Incorpora un nuevo inciso 2°y 3° en el artículo 14 de la Ley N° 19.628 sobre protección a la vida privada: "Prohíbase el envío de comunicaciones comerciales a través de mensajes de texto a teléfonos celulares (SMS) que no hayan sido previamente autorizados por el destinatario. "La infracción a lo preceptuado en el inciso precedente será sancionada con multa de 50 Unidades Tributarias Mensuales."	Proyecto presentado, en discusión en comisión de cámara de origen

N° 7776-03	2011	Sobre eliminación en registros o bancos de datos personales de clientes cuyas deudas se hayan repactado unilateralmente.	Se propone modificar la Ley N° 19.628 incorporando un nuevo inciso final en el artículo 17, en los siguientes términos: "Las empresas que hayan repactado sin autorización o de manera unilateral las deudas de sus clientes, deberán retirar de los registros o bancos de datos personales a los deudores que hayan sido incluidos en dichos registros en el plazo de 30 días. En el caso que exista reclamo administrativo pendiente ante el SERNAC, o demanda ante los tribunales de justicia derivados de este tema, las entidades responsables que administren bancos de datos personales no podrán publicar o comunicar la información referida en el presente artículo, cuando éstas se hayan originado producto de repactaciones sin autorización o unilaterales durante el plazo de un año".	Proyecto presentado, en discusión en comisión de cámara de origen

N° 7886-03	2011	Regula el tratamiento de la información sobre obligaciones de carácter crediticio o financiero.	La propuesta incluye una ampliación en la noción de titulares de los datos, una extensión del concepto de información comercial, la creación de un Sistema de Obligaciones Económicas (SOE), el fortalecimiento de los derechos de los titulares de los datos, la regulación de los requisitos de entrada y de salida del mercado de las distribuidoras de información, la regulación de las obligaciones de todos los aportantes de datos de obligaciones económicas, entre otras modificaciones.	En discusión en segunda comisión de cámara de origen, con urgencia simple
N° 8208-07	2012	Establece la facultad de los usuarios de Internet de exigir a portales y redes sociales que eliminen sus datos personales.	Incorpora un nuevo inciso 3"y 4° en el artículo 15 de la ley 19.628 sobre protección de datos personales: "Toda persona podrá solicitar, de forma explícita, la eliminación de sus datos personales de cualquier especie, a las compañías que administren tales datos cuando no exista razón legítima para retenerlos. La solicitud deberá ser planteada a la subsecretaría de telecomunicaciones y publicada en su sitio web". Cumplidos los requisitos mencionados en el inciso anterior la compañía requerida para la eliminación de tales datos tendrá un plazo de 15 días para eliminar definitiva e irrevocablemente la información so pena de multa ascendente a 100 UTM a beneficio fiscal".	Proyecto presentado, en discusión en comisión de cámara de origen

Nº 8143-03	2012	Reforma la Ley Nº 19.628 de protección de la vida privada. Tiene el objeto de hacer una reforma integral a la ley de protección de la vida privada, con el objeto de adecuarla a los estándares de la OCDE, y buscando reforzar la protección de estos datos.	En la propuesta se cuentan las siguientes modificaciones: precisión del objeto de protección de la Ley Nº 19.628, la introducción del concepto de consentimiento previo, la incorporación de principios en materia de protección de datos, el reforzamiento del derecho a la información por parte de los titulares de datos personales y la definición de las obligaciones del responsable del registro o base de datos y del encargado de todo o parte del tratamiento de datos personales, el establecimiento de la obligación de informar en comunicaciones comerciales y publicitarias el origen de los datos que permitieron su envío al titular y el derecho para este último de excluirse de la recepción de tales comunicaciones, la regulación del flujo transfronterizo de datos, el deber de informar registros o bases de datos, la protección especial respecto de los datos personales de niños, niñas y adolescentes, el establecimiento de procedimientos de reclamo más expeditos y equilibrados para los titulares de datos respecto de los responsables y encargados del tratamiento.	Proyecto presentado, en discusión en comisión de cámara de origen

Leyes recientemente aprobadas:

De entre los esfuerzos por regular los datos personales de los últimos años, se han integrado a la legislación las leyes listadas a continuación:

Ley	Año	Descripción
Ley N° 20.526	2011	La ley se denomina "Ley N° 20.526 que sanciona el acoso sexual de menores, la pornografía infantil virtual y la posesión de material pornográfico infantil". El proyecto de ley original contemplaba la creación de registros de usuarios de cibercafés, lo cual fue rechazado por el Tribunal Constitucional por constituir una infracción al derecho de privacidad.
Ley N° 20.575	2012	La ley se denomina "Ley N° 20.575 que establece el principio de finalidad en el tratamiento de datos personales". Este cuerpo normativo afecta sólo a la información comercial, en circunstancias en que el derecho de información que ella establece (que obliga a que los bancos de datos informen gratuita y periódicamente a los titulares sobre la información que almacenan, y la obligación de declarar la finalidad con la cual se accede a los datos personales) podía ser incorporado a la Ley N°19.628, como una obligación a todos los responsables de tratamiento de datos personales.
Ley N° 20.594	2012	La ley se denomina "Ley N° 20.594 que crea inhabilidades para condenados por delitos sexuales contra menores y establece registro de dichas inhabilidades". La iniciativa introdujo modificaciones al Código Penal y al Decreto Ley N° 645 sobre Registro Nacional de Condenas. En primer lugar, se establece la sanción de inhabilidad perpetua cuando la víctima es menor de 14 años. En segundo lugar, en orden a corregir los actuales vacíos de la ley, se extiende la inhabilidad a la difusión de material pornográfico en cuya elaboración se han empleado a menores (artículo 374 bis inciso 1°) y se aclara que se extiende también a la sustracción de menores con violación, y a los casos violación con homicidio y robo con violación en los que las víctimas sean menores de edad. De igual manera, se elimina la mención a las personas del artículo 371, manteniéndose la referencia sólo para el caso de la sodomía libremente consentida con un menor mayor de 14 años (artículo 365) y solicitación de servicios sexuales a un menor mayor de 14 años a cambio de una prestación de cualquier naturaleza (artículo 367 ter). Como consecuencia de establecer casos de inhabilitación perpetua, la cual es pena de crimen, algunos delitos que hoy no lo son -según sus penas corporales- pasan a serlo por la inhabilidad. Ejemplo de ello son la corrupción de menores de 14 años (artículo 366 quáter), la elaboración de material pornográfico con menores de 14 años (artículo 366 quinquies), los delitos de los artículos 367 y 367 bis con menores de 14 años. El principal efecto de esta nueva calificación de las conductas antes descritas es que se aumenta el plazo de prescripción de la acción penal de 5 a 10 años, lo que es coherente con la gravedad de los delitos indicados. En su artículo segundo el proyecto crea una sección especial dentro del Registro General de Condenas, caracterizada por el principio de publicidad. A partir de esta norma, será la administración que hoy día realiza el Registro Civil de dicho Registro, la encargada de implementar y gestionar esta sección, como asimismo, de establecer los medios tendientes a su adecuada publicidad, uso y control.

II. RECOMENDACIONES DE POLÍTICA PÚBLICA

Con base en lo expuesto, queda claro que a la fecha el marco legal chileno no responde de manera adecuada al desafío de proteger la privacidad de las personas, en particular considerando algunos fenómenos específicos como el manejo de la información personal en línea.

De lo anterior se desprende la necesidad de una nueva regulación en materia de protección de datos de carácter personal, que en resguardo del interés público y de los derechos fundamentales, recoja las propuestas siguientes:

I) Adecuación de las normas sustantivas sobre protección de la vida privada

- Se recomienda **fijar un estándar de protección de datos personales a tono con el de la Unión Europea,** que al día de hoy es el que mejor defiende los derechos humanos e intereses públicos asociados a la protección de datos personales, además de requerir del mismo nivel de protección a países con los que exista tráfico transfronterizo de datos personales.
- Se recomienda **concentrar la regulación en materia de datos personales dentro de la ley de protección de datos personales** (N° 19.628), con el objeto de evitar la dispersión normativa y falta de sistematicidad en la materia.
- La ley de protección de datos personales debe contener una **consagración positiva** de los principios rectores en torno al tratamiento de datos personales, mediante la adecuación del ordenamiento jurídico a las recomendaciones de la OCDE en materia de protección de datos personales. Lo anterior se logra por medio de la **introducción en el texto de la ley de los principios estudiados**, como marco regulatorio a partir del cual se estructuran todas las reglas en materia de protección de datos, sirviendo estos principios de elementos de interpretación que actuarán como una bisagra entre la norma jurídica vigente y el valor imperante en una situación determinada. Estos principios, cuando corresponda, deberán ser desarrollados dentro de la ley con el objeto de permitir el ejercicio de los derechos correspondientes.
- La ley de protección de datos personales debe incluir **definiciones rigurosas** de los derechos consagrados y sus márgenes de protección, así como también las **excepciones a la autorización previa para el uso**, dentro de un marco de equilibrio. El propósito es que no se generen abusos a partir de definiciones insuficientes de conceptos como "fuente accesible al público", lo que desnaturaliza el sistema de protección de datos personales chilenos, al prescindir de la finalidad de los datos, como ocurre hoy.

- La ley de protección de datos personales debe establecer **obligaciones especiales de cautela y garantía** para quienes realizan el tratamiento de datos sensibles, en vista de que en la actualidad el tratamiento de este tipo de datos sólo requiere el consentimiento del titular de ellos, no quedando establecido ningún tipo de garantía que proporcione la seguridad que este tratamiento requiere.
- La ley de protección de datos **debe entregar a los titulares de datos la mayor cantidad de control posible sobre los mismos**, permitiendo a los mismos no solamente el acceso, rectificación o eliminación de sus datos cuando corresponda, sino también obligando a los responsables de las bases de datos a proveer toda la información de manera consolidada y compatible con otros sistemas, con el objeto de asegurar la portabilidad de estos datos a otras bases de datos.
- En general, las leyes que afecten el derecho a la vida privada deben incluir **obligaciones claras y específicas respecto de la tenencia y manejo de datos personales por parte de los responsables de las bases de datos**. Por ejemplo, debe delimitar claramente la obligación de retención de datos de telecomunicaciones y los mecanismos para solicitarlos por parte de las instituciones públicas de persecución criminal, en el caso de las leyes que regulan los procedimientos criminales.
- Se recomienda **retirar resguardos desmedidos de privacidad que impiden el ejercicio de otros derechos y libertades**, como el delito del artículo 161-A del Código Penal, que sanciona ampliamente la grabación o registro gráfico o audiovisual en sitios particulares, en desmedro de la libertad de expresión e información.
- **Las leyes que afecten el derecho a la protección de la privacidad deben establecer sanciones apropiadas por la infracción de sus normas**. Estas no deben limitarse a la imposición de multas o penas corporales, sino que también deben existir sanciones que obliguen a la adopción de ciertas medidas e impidan que persista la conducta infractora, como por ejemplo: la cancelación del registro de datos personales, la suspensión del tratamiento o cesión de datos, la suspensión o remoción del encargado o responsable del tratamiento de los datos, etc.

2) Creación de una agencia de protección de datos personales

- Con el objeto de ajustar la realidad chilena a una tendencia internacional creciente en materia de protección de datos y elevar los estándares de protección de los mismos, **proponemos la institución de una agencia de protección de datos, esto es, una autoridad pública, autónoma e independiente**, dotada de las competencias y

herramientas eficaces para velar por el adecuado cumplimiento de las normas relativas al tratamiento de datos, de forma constante y activa.

- Este organismo debe encontrarse facultado para llevar a cabo diversas labores de manera especializada, asegurando el acceso a la justicia, facilitando la tramitación de litigios y la correcta preparación para enfrentar las problemáticas especiales que presenta la protección de datos personales. Debe participar con voz en instancias deliberativas en el seno de los poderes ejecutivo y legislativo en los temas de su competencia, en defensa de los intereses vinculados a la privacidad, y no como un órgano de gobierno más.
- Dentro de las atribuciones que necesita una agencia de protección de datos, se contarían:
  - la supervigilancia de entidades privadas y públicas que administren bases de datos
  - la fiscalización del cumplimiento de las disposiciones sobre tratamiento de datos personales
  - la facultad para dictar instrucciones de carácter general o particular, respecto de las condiciones de legitimidad de un tratamiento de datos (potestad normativa)
  - la facultad de conocer de las reclamaciones de particulares relacionadas con el ejercicio de sus derechos
  - la aplicación de sanciones administrativas a los responsables de los bancos de datos que infrinjan la normativa sobre protección de datos (potestad sancionadora)
  - la facultad de aprobar mecanismos de autorregulación; la comparecencia ante tribunales ordinarios de justicia por infracción grave de la legislación
  - el ejercicio de acciones en beneficio directo de las personas, tales como informar sobre los derechos en materia de tratamiento de datos de carácter personal y promover el respeto de los mismos.

3) Instauración de mecanismos adecuados de enforcement

- Se requiere la existencia de mecanismos que **garanticen la observancia de la ley**, tanto en la fiscalización en el sector público (función que hoy en día se encuentra radicada en el Consejo para la Transparencia), como en el sector privado, donde en la actualidad sólo existe la acción judicial conocida como habeas data.
- Debe asegurarse la implementación de **procedimientos de reclamación expeditos, fácilmente accesibles y de bajo costo**. Allí donde sea la iniciativa de un particular la que impulse la acción del órgano de control, este debe contar con la capacidad de responder con

celeridad. En términos de costos y beneficios, esto no ocurre con la reclamación judicial hoy procedente.

- Los procedimientos de reclamación deben ser llevados a cabo por **organismos especializados**, y no por organismos que ya poseen sus propias labores y ámbitos de competencia (como el Servicio Nacional del Consumidor). En tal sentido, resulta más eficiente (siempre que existan atribuciones suficientes) radicar el control de la observancia de la ley en una **agencia independiente, como ya indicamos, con atribuciones fiscalizadoras y sancionatorias**, a diferencia de las atribuciones que hoy poseen organismos como el Servicio Nacional del Consumidor, cuyas facultades no están orientadas a resolver conflictos sino a solamente acompañar y eventualmente denunciar los mismos.
- El organismo encargado de asegurar la observancia de la ley debe contar con **facultades fiscalizadoras y sancionadoras**, en casos de infracción a la ley, con lo que se equipararía a otras autoridades de protección de datos del mundo, adecuando a la legislación chilena a los mejores estándares internacionales disponibles. La fiscalización, como proceso activo de control sobre el manejo de datos personales, es una herramienta hoy ausente de la legislación, que es capaz de revertir la actual situación en que es necesariamente de iniciativa de los particulares la reacción frente a un uso inadecuado de sus datos.
- Debe existir una **regulación pormenorizada de un procedimiento sancionatorio, el que puede ser iniciado de oficio o por denuncia**. El órgano ante el cual se seguiría este procedimiento es el organismo de protección de datos (autoridad de control), que estará facultado para aplicar las sanciones correspondientes.

Google

Este trabajo es parcialmente resultado de un proyecto de investigación financiado por Google Inc.