UNIVERSIDAD FINIS TERRAE
FACULTAD DE DERECHO
MAGÍSTER EN DERECHO PÚBLICO: TRANSPARENCIA, REGULACIONES Y CONTROL

NUEVO MARCO REGULATORIO DE LA PROTECCIÓN DE DATOS PERSONALES Y PROTECCIÓN DE LA VIDA PRIVADA EN CHILE.

MACARENA NOGUERA OSORIO

ARTÍCULO ACADÉMICO PRESENTADO A LA FACULTAD DE DERECHO DE LA UNIVERSIDAD FINIS TERRAE, PARA OPTAR AL GRADO DE MAGISTER EN DERECHO PÚBLICO: TRANSPARENCIA, REGULACIONES Y CONTROL.

PROFESOR GUÍA: IGNACIO COVARRUBIAS CUEVAS

SANTIAGO, CHILE
2020

NUEVO MARCO REGULATORIO DE LA PROTECCIÓN DE DATOS PERSONALES Y PROTECCIÓN DE LA VIDA PRIVADA EN CHILE.

MACARENA NOGUERA OSORIO
Universidad Finis Terrae
macanoguer@hotmail.com

Profesor guía: Ignacio Covarrubias.

Resumen

El año 2018, se incorporó el derecho a la protección de datos personales al catálogo de los derechos constitucionales, sin embargo, aún no se modifica la Ley N°19.628 sobre protección de la vida privada, existiendo múltiples iniciativas para su modificación debido a sus carencias y deficiencias, impidiendo que se garantice plenamente este nuevo derecho de rango constitucional. Ante la contingencia actual, cobra aún más sentido contar con las herramientas necesarias que impidan su vulneración, por tanto, urge una legislación que este a la altura de las circunstancias actuales.

Palabras clave: Protección de datos personales, datos sensibles, autodeterminación informativa, habeas data, transparencia, acceso a la información.

Abtract

In 2018, the right to the protection of personal data was incorporated into the catalog of constitutional rights, however, Law 19.628 on protection of privacy has not yet been amended, and there are multiple initiatives for its modification due to its deficiencies and deficiencies preventing this new right of constitutional rank to be fully guaranteed. Given the current contingency, it makes even more sense to have the necessary tools to prevent its violation, therefore, there is an urgent need for legislation that is up to the current circumstances.

Key words: Protection of personal data, sensitive data, advertising, transparency, access to information.

Introducción

La incorporación del derecho a la protección de los datos personales a la Constitución, lo consagra como un derecho autónomo, cuyo tratamiento y protección se debe efectuar en la forma y condiciones que señale la ley, en este caso la ley N°19.628, sobre protección a la vida privada, pero ésta ley dictada en 1999 ya no es suficiente para garantizar en la práctica, el ejercicio de este nuevo derecho constitucional, debido a la falta de un órgano fiscalizador, la inexistencia de un procedimiento de reclamo idóneo, la ausencia de infracciones y sanciones efectivas, la inexistente regulación para la transferencia internacional de datos, entre otros.

Por lo anterior, se está discutiendo actualmente la modificación de la Ley N°19.628, Boletines N°11144-07 y N°11.092-07, refundidos, que pretende ser una solución a estos y otros cuestionamientos, pero ¿esta modificación será efectiva para garantizar un derecho tan importante en la actualidad?

En el presente trabajo se analizará brevemente el proyecto de ley mencionado, de modo de establecer si efectivamente mejorará el estándar de protección de datos personales, si logra corregir las falencias actuales y si realmente recoge los estándares internacionales, para lo cual se revisará la forma en que otras legislaciones han regulado el tema.
Se estudiará la situación actual de Chile con la normativa vigente en materia de datos personales y otras normas vinculadas a la materia y se abordarán algunos casos contingentes a modo de ejemplificar como se evidencian estas falencias y como podrían eventualmente solucionarse, considerando la gran relevancia que ha adquirido este derecho en la actualidad y la importancia de regularlo de la mejor forma.

El derecho a la protección de los datos personales ha ido ganando importancia debido a la revolución de datos que estamos viviendo gracias a la transformación digital. Hoy por hoy, nuestros datos personales son catalogados como una gran fuente de riqueza, pero en Chile y el mundo no están suficientemente protegidos, debido a que los ordenamientos no logran seguir la rapidez y la velocidad con la que se van actualizando las tecnologías y la modernidad.

Antes, al pensar en nuestros datos personales solo los asociábamos a aquellos relativos a nuestra identificación como ciudadano, otros relativos a nuestra salud, a nuestra familia o economía. Pero en la actualidad, debemos ampliar lo anterior a nuestros datos biométricos, de georreferenciación y aquellos que se recopilan a partir del uso de las plataformas tecnológicas que permiten saber nuestros gustos o preferencias en determinados mercados, los que incluso pueden ser comercializados sin nuestra autorización.

Las bases de datos en la actualidad constituyen grandes fuentes de información de las que todos somos parte sin saber su verdadero uso.

Según lo señalado en un reportaje del periódico The New York Times sobre el valor de los datos personales, un estudio de la consultoría de Shapiro "calculó que el beneficio corporativo que produjo la recolección de datos personales de los estadounidenses en línea —principalmente para las grandes empresas tecnológicas— fue de 76.000 millones de dólares en 2018 y esa cantidad aumentará de forma drástica en el futuro… La gente encargada de formular políticas está haciendo lo posible para encontrar la manera de que las acciones del gobierno y las fuerzas del mercado se empleen para controlar el poder de los gigantes tecnológicos que se alimentan de los datos"[1].

Claro está, que el problema para abordar el tratamiento de los datos personales no es algo que afecte solo a nuestro país, sino del mundo en general considerando la globalización en el uso de las tecnologías. Es más, este año podemos sumar otro tema común que nos ha hecho preguntarnos si nuestros datos personales están efectivamente garantizados y se ha evidenciado lo fácil que es su vulneración, pues con la pandemia del coronavirus, muchos países han debido recurrir a diversos medios para controlar su expansión y contagio ¿recurriendo a qué? Al uso de **los datos personales**.

[1] LOHR (2019), página única.

1. Contexto general de la protección de datos personales

El derecho a la protección de datos personales nace al alero del derecho a la protección de la intimidad y la vida privada, con el pasar de los años este derecho fue cobrando un carácter autónomo debido a la importancia que fueron adquiriendo los datos personales, pero ¿Qué son los datos personales? Según la Red Iberoamericana de Protección de Datos, es cualquier información de personas físicas identificadas o identificables, en forma numérica, alfabética, gráfica, fotográfica, alfanumérica, acústica o de otro tipo[2].

De este modo se hizo necesario garantizar este derecho en forma independiente regulando todos los ámbitos vinculados a los datos personales como su utilización, tratamiento, recopilación y almacenamiento.

El derecho de la protección de datos personales es considerado como un derecho de cuarta generación para algunos autores, otros prefieren enmarcarlo aún en los de tercera generación, "en la mayor parte de los casos de esta nueva generación, se trata de nuevos derechos, pero en otros se trata de derechos ya enunciados y regulados anteriormente, pero redefinidos por las nuevas condiciones de la sociedad, la tecnología y la globalización"[3]

1.1 Marco normativo a nivel internacional; breve historia

Para comprender de modo general la evolución de este derecho, se recopila brevemente el marco jurídico internacional.

Como se mencionó anteriormente, el derecho a la protección de datos personales surge primeramente asociado al derecho a la intimidad, pero de a poco se fue transformado en un derecho autónomo, con el avance tecnológico de la sociedad se evidenció la necesidad de regularlo y garantizarlo de forma particular.

Una primera aproximación de protección en la esfera íntima de la persona se encuentra enunciada en el ámbito internacional dentro de la Declaración Universal de los Derechos Humanos de 1948, cuyo artículo 12 señala: "Nadie será objeto de injerencias arbitrarias

[2]Consultado en https://www.bcn.cl/observatorio/americas/noticias/instituciones-y-proteccion-de-datos-personales-experiencia-en-iberoamerica
[3]BAILÓN, p.114.

en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques"[4].

Europa

En el ámbito internacional, Europa ha llevado la delantera en cuanto a la basta protección que ha otorgado a los datos personales, es así como se rescatan los hitos más importantes en este sentido:

- El Tratado de Funcionamiento de la Unión Europea (TFUE) de 1957, en su artículo 16 establece:
  1. "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
  2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes.

     Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea."[5]
- Convenio 108 Para la Protección de las Personas con respecto al Tratamiento automatizado de datos personales, de 1981 y su Protocolo Adicional, conocido como Convenio 108+ de 2001, Constituye el primer instrumento internacional jurídicamente vinculante en materia de protección de datos personales, fue elaborado por el Consejo de Europa, sin embargo países que no pertenecen a la

[4] GARCÍA (2007) Consultado en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332007000300003

[5] Tratado de Funcionamiento de la Unión Europea. Consultado en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN

región pueden adherirse, en Latinoamérica solo han adherido México, Uruguay y Argentina[6].

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, 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[7]
- Carta de los Derechos Fundamentales de la Unión Europea del año 2000, que reconoce en su artículo N°8 el Derecho a la Protección de Datos de carácter personal, señalando lo siguiente:

  1. "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

  2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

  3. El respeto de estas normas quedarán sujeto al control de una autoridad independiente[8].
- Reglamento General de Protección de Datos de 2016, pero que entró en vigor en 2018 y que sustituyo a la Directiva 95/46. Este reglamento garantiza la privacidad de todos los ciudadanos de la Unión Europea en sus actividades on line. Regula a las empresas en el ámbito del tratamiento de datos personales, estableciendo requisitos mínimos y sanciones ante el incumplimiento de la normativa, con multas de hasta 20.000.000 de euros o hasta un 4% de la facturación de la empresa.

España

Particularmente en España, la Constitución de 1978 no consagra explícitamente el derecho a la protección de datos personales, pero señala en su artículo 18.4 "La ley

[6] Convenio para la Protección de las Personas con respecto al Tratamiento Automático de Datos Personales. Consultado en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[7] Directiva 95/46/CE del Parlamento Europeo y del Consejo. Consultado en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

[8] Carta de Derechos Fundamentales de la Unión Europea. Consultado en https://www.europarl.europa.eu/charter/pdf/text_es.pdf

limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".[9]

Luego a través de la LORTAD (Ley Orgánica 5/1992 de 29 de Octubre de 1992, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal) se da cumplimiento a lo mandatado en el artículo 18.4 de la Constitución[10] (Sin embargo, esta ley no incluyo los datos no automatizados como aquellos datos manuales, por lo que en 1999 se dicta la Ley Orgánica **Protección de Datos de Carácter Personal,** LOPD, con el objetivo de dar cumplimiento a la Directiva 95/46 que exigía la extensión a ficheros manuales. Esta ley es reemplazada por la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales, cuyo objeto señalado en su artículo N°1 es: "a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones. El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución"[11].

Finalmente hay que señalar que España creo en 1992 la Agencia de Protección de Datos que "constituye *la autoridad de control* que el Reglamento General de Protección de Datos determina que establecerán los Estados miembros a efectos de supervisar su aplicación, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión"[12].

[9] Constitución Española de 1978. Consultado en https://app.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=18&tipo=2
[10] Ley Orgánica 5/1992 de España. Consultada en https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189
[11] Ley Orgánica 3/2018 de España. Consultada en https://www.boe.es/eli/es/lo/2018/12/05/3
[12] Agencia Española de Protección de Datos. Consultado en https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/historia

Estados Unidos

En el caso norteamericano, no se considera la protección de datos personales como un derecho fundamental, sino que se enmarca dentro de la protección de derechos del consumidor[13], además no dispone una norma a nivel federal que regule los datos personales, existiendo distintas normativas que varían según cada estado y no posee un ente de control.[14]

Ante la exigencia de la legislación europea para el tratamiento de datos fuera de la Unión Europea se firmó en 2016 un acuerdo denominado *Privacy Shield* o Escudo de Privacidad entre la UE y los EE. UU. Este acuerdo permite que los datos personales se transfieran de una empresa de la UE a otra de los Estados Unidos, únicamente si dicha empresa procesa (es decir, usa, almacena y transfiere posteriormente) los datos personales con arreglo a una serie de normas de protección y salvaguardias bien definidas. La protección conferida a los datos personales se aplica con independencia de si se es o no ciudadano de la Unión Europea[15].

Sin embargo, recientemente el Tribunal Europeo declaro invalido el Acuerdo debido a que no garantiza una protección de datos conforme al RPGD[16].

Tratamiento de datos personales en Latinoamérica[17].

En cuanto a nuestra región, el derecho a la protección de datos en general ha sido reconocido constitucionalmente ya sea de forma directa o a través del derecho a la

[13] INAI (2015) pag.19. Consultado en http://metabase.uaem.mx/bitstream/handle/123456789/2534/12%20Consecuencias%20por%20el%20uso%20indebido%20de%20datos%20personales.pdf?sequence=1
[14] Consultado en http://www.mundolopd.com/lopd/diferencias-europa-eeuu-proteccion-de-datos/
[15] Guía Acerca del Escudo de Privacidad UE-EE.UU. Consultado en https://www.aepd.es/sites/default/files/2019-09/guia-acerca-del-escudo-de-privacidad.pdf
[16] Sentencia C-311/18 del Tribunal de Justicia de la Unión Europea. Consultado en http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=10478869
[17] BOJALIL Y VELA (2019) Consultado en https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/

privacidad, tal el caso de las constituciones de Argentina, Brasil, Colombia, México, Perú, Venezuela y Chile.[18]

Breve recopilación de la normativa sobre protección de datos personales en la región:

Argentina: cuenta desde el año 2000 con la Ley N°25.326[19] de protección de datos personales y en 2018 se propuso un proyecto de ley para su reemplazo y adecuación a los estándares del GDPR.

Brasil: Desde 2018 cuenta con una ley general de protección de datos personales (Lei Nº 13.709, de 14 de agosto de 2018)[20] estableciendo un régimen único (pues antes existían diversas leyes sectoriales que trataban de forma general la protección de daros personales)

Colombia: cuenta con dos leyes que regulan y protegen los datos personales, la Ley N°1581[21] de 2012, por la cual se dictan disposiciones generales para la protección de datos personales y la Ley N°1.266[22] de 2008, por la cual se dictan disposiciones generales del Habeas Data y regula el manejo de la información contenida en bases de datos personales. También existe un proyecto para modernizar sus leyes al estándar GDPR.

México: cuenta desde el año 2010 con la Ley Federal de Protección de Datos Personales en posesión de los particulares[23]. La autoridad de protección de datos mexicana, denominada INAI, es considerada una de las más activas de Latinoamérica debido a la cantidad de procedimientos que ha revisado y las sanciones impuestas.

1.2 El Derecho de protección de datos personales en Chile actualmente.

La Ley N°21.096 de 2018, consagró el derecho a la protección de los datos personales, modificando el artículo 19 N°4 de la Constitución Política de la Republica, elevando este derecho a rango constitucional. Se estableció que la forma y condiciones bajo las cuales se pueden tratar dichos datos estaría regulada por la aún vigente Ley N°19.628 sobre protección de la vida privada, que data del año 1999. Sin embargo, se ha evidenciado que

[18] MILANES (2017), pág. 21. Consultado en https://www.consejotransparencia.cl/wp-content/uploads/2018/04/v_milanes__1_.pdf
[19] Consultado en https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto
[20] Consultado en https://legis.senado.leg.br/norma/27457334/publicacao/27457731
[21] Consultado en http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html
[22] Consultado en http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html
[23] Consultado en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

esta ley posee vacíos legales que en la práctica no permiten gozar plenamente de este derecho, lo que se justifica por diversas razones como el paso del tiempo, el avance de la sociedad y "también debemos considerar la evidente y rápida evolución en materia tecnológica que deja con mucha rapidez desfasada la legislación dictada en una época determinada".[24]

Debido a lo anterior, se ha intentado modificar dicha ley con diversas iniciativas, la última de ellas y que actualmente se encuentra en tramitación en el Senado, los proyectos contenidos en los Boletines N°11092-07 y N°11144-07, refundidos en este último.

Antes de la modificación constitucional, el artículo 19 N°4 solo garantizaba el respeto a la vida privada y a la honra de la persona y su familia, y a través de la Ley N°19.628, se otorgaba protección a los datos personales bajo una ley denominada sobre protección de la vida privada.

Lo anterior, dificultaba la protección de este derecho a nivel constitucional, y cuando un titular de un dato personal recurría de protección por la vulneración de su derecho, debía invocar la amenaza al derecho a la vida privada y el resultado era frustrante, un ejemplo de ello es el recurso de protección Rol Nº 19.154-2015. En este caso, se dedujo la acción en contra de una empresa que publicó en una página web los Rut de las personas bastando solo con indicar su nombre o viceversa para que la página entregue la información de estos datos, por ello, las recurrentes indican que la empresa vulnera su derecho a la protección a la vida privada, ya que el acceso abierto y sin ningún control del dato personal, RUT, obtenido de fuentes indeterminadas les priva, perturba y amenaza el legítimo derecho a la intimidad, y en particular, a los datos personales que forman parte de ella, derecho que es reconocido en el artículo 19 Nº 4 de la Constitución Política de la República. La Corte de Apelaciones rechazo el recurso y la Corte suprema lo confirmo fundamentalmente y en lo que nos importa en su punto *"**Noveno:** Que, además, en la especie **no existe un derecho constitucional que haya sido afectado** en su legítimo ejercicio, requisito esencial para la procedencia de esta acción cautelar, pues no se ha logrado demostrar que con el tratamiento de datos realizado por el recurrido se haya amenazado la vida privada de las recurrentes, accediendo por su intermedio u operación*

[24] VERGARA (2017), p. 136.

a otros de carácter sensible o de carácter personal de las mismas, cuyo tratamiento hubiese requerido su autorización, situación fáctica que impide dar a las recurrentes la protección constitucional solicitada[25].

Como se puede evidenciar, el recurso fue rechazado por considerarse que no existía un derecho constitucional afectado, pues a la fecha de la sentencia aún no se encontraba constitucionalmente protegido el derecho al resguardo de los datos personales y debía acreditarse que con su divulgación se afectaba la vida privada de las personas.

Ahora, con su reconocimiento constitucional el derecho a la protección de los datos personales es un derecho autónomo e independiente, no obstante y según sostiene Víctor Bazán "Es conveniente independizar conceptualmente el derecho de autodeterminación informativa, como bien jurídico protegido por el hábeas data, de derechos personalísimos tales como el de intimidad, al honor o a la imagen, y aun a la identidad, sin desconocer que tienen puntos de confluencia…"[26]El problema es que bajo la legislación actual la institución del Habeas Data no es efectivamente garante del derecho a la protección de datos personales.

"La normativa sobre protección de los datos personales más que pretender resguardar la intimidad de las personas, aquel ámbito de nuestro quehacer cotidiano respecto del cual excluimos a los demás, procura brindar amparo a un nuevo bien jurídico: la autodeterminación informativa"[27], que consiste en la facultad de las personas a decidir por sí mismas cuando y dentro de que limites revelar información de su vida privada, permitiéndoles tener el control de sus datos. Este concepto fue recogido por primera vez a nivel jurisprudencial por el Tribunal Constitucional Federal Alemán, a través de una sentencia dictada el 15 de diciembre de 1983, relativa a la Ley de Censo de la Población, en la que se consideró que varios de sus preceptos vulneraban el derecho general de la personalidad, estableciendo que los individuos tienen un derecho de autodeterminación informativa que consiste en decidir por sí mismos, cuando y dentro de que limites los

[25] Corte Suprema de Justicia. Sentencia Rol N°5243-2015.
[26] BAZÁN (2005), pp. 110 y 111.
[27] Consultado en http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_simple/0,1493,SCID%253D14341%2526ISID%253D507%2526PRT%253D14331,00.html

asuntos de su vida personal habrán de ser públicos, pero esto no es ilimitado si no que tiene como restricción el interés general vinculado con el principio de proporcionalidad[28].

La Ley 19.628 reconoce algunos derechos que los titulares de los datos tienen para su resguardo y además dispone de un procedimiento para su cautela, la acción judicial es conocida comúnmente como "Habeas Data".

La ley otorga a los titulares de los datos los siguientes derechos, contenidos en su artículo 13:

• **El derecho de acceso a la información:** es aquel que tiene el titular de datos personales de solicitar y obtener del responsable de un registro o banco de datos, toda la información sobre su persona, su procedencia y su destino y el propósito de su almacenamiento.

• **El derecho de modificación o rectificación:** es la facultad que tiene el titular del dato personal para que se modifiquen aquellos datos erróneos, inexactos, equívocos o incompletos.

• **El derecho de eliminación:** consiste en solicitar la eliminación de los datos personales cuando su almacenamiento carezca de fundamento legal o los datos estuvieran caducos.

• **El derecho de bloqueo:** es la facultad que tiene el titular de un dato personal que voluntariamente entrego sus datos personales y no desea continuar figurando en los registros.

Para el ejercicio de estos derechos la ley faculta a sus titulares a solicitar judicialmente la exhibición de sus datos almacenados en algún banco o registro de datos, solicitar su rectificación, eliminación o cancelación, aunque el ejercicio de esta acción no impide que se utilicen otras vías judiciales como el recurso de protección, el de amparo económico y las acciones de indemnización de perjuicios por los daños causados por el tratamiento de datos. En efecto, titular de los datos personales podrá interponer en conjunto con la acción de habeas data, la indemnización de perjuicios causados por el tratamiento indebido de los datos personales, según lo establecido en el artículo 23 de la ley, sin perjuicio de que se establezca que el responsable de los datos deba eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal. Sin embargo, estas garantías establecidas en la ley tienen poca eficacia en la práctica debido

[28] SCHWABE (2009), pp. 94 y ss.

a lo lento que resulta su tramitación en sede civil y los costos asociados a ello, sumado a la falta de sanciones ejemplares para los infractores.

Por lo mismo, no es de extrañar de que este procedimiento haya sido utilizado muy pocas veces, dando pie a la impunidad sobre el tratamiento ilegítimo de los datos personales de las personas chilenas; no porque la privacidad no importe, sino que se ha transformado en un privilegio defenderla[29].

1.3 Tratamiento de datos en el sector público chileno

Según lo establecido en el articulo 20 de la Ley 19.628, los organismos públicos podrán efectuar el tratamiento de datos personales solo respecto de las materias de su competencia y con sujeción a las reglas de la ley, para lo cual no necesitarán del consentimiento del titular.

En relación con lo anterior, los organismos públicos tienen la obligación de proporcionar los bancos de datos que dispongan al Servicio de Registro Civil, cuando inicien las actividades y deben comunicar sus cambios dentro de un plazo de 15 días, según lo establecido en el articulo 6° del Reglamento de la Ley N°16.628 (Decreto 779 del año 2000).

La norma establece que es el Registro Civil el organismo que debe llevar un registro de los datos personales a cargo de organismos públicos, sin embargo, el Registro Civil carece de poder fiscalizador y sancionador para hacer que los organismos públicos cumplan la ley.

Por otra parte, la Ley N°20.285, en su artículo 33, encomendó al Consejo para la Transparencia, velar por el cumplimiento de la Ley N°19.628, por parte de los órganos de la Administración del Estado, pero tampoco se le otorgaron facultades concretas de fiscalización y sanción.

Finalmente, dentro del contexto actual, nuestro país tiene una variedad de normas que en su conjunto constituyen un marco regulatorio en materia de datos personales y la forma en que se garantiza la seguridad de los mismos ya sean datos automatizados o no, pero otorgando mayor énfasis a los primeros, debido a la era moderna en que vivimos en que

[29] CANALES y VIOLLIER (2019). Consultado en https://www.derechosdigitales.org/13443/proteccion-de-datos-con-dientes/

todo se realiza en línea, debiendo para ello regularse inclusive la forma en que nuestros datos circulan por el ciberespacio. Chile se está preparando jurídicamente para ello y se recopilan a continuación las principales normas vinculadas a la seguridad de los datos personales:

- Constitución Política de la Republica, artículo 19 N°4.
- Ley N°19.628 y su Reglamento, en proceso de modificación.
- Ley N°20.285, sobre acceso a la información pública.
- D.S. 83/2005, que aprueba norma técnica para los órganos de la administración del estado, sobre seguridad y confidencialidad de los documentos electrónicos.
- D.S. 533/2015, que crea el Comité Interministerial sobre Ciberseguridad.
- Política Nacional de Ciberseguridad
- Compromiso N°10: Política de Datos Abiertos y Protección de Datos
- Ley 21.180 Transformación Digital del Estado, actualmente se prepara su reglamento.

Además, Chile forma parte y tiene un equipo C SIRT funcionando (Equipo de respuesta ante incidentes de seguridad informática).

2. La importancia de avanzar en la modificación de la Ley N°19.628.

Como ya se dijo, la actual ley que regula el tratamiento de los datos personales en Chile tiene más de 20 años y aunque no pareciera ser una ley muy antigua, sí ha quedado desactualizada ya que el derecho de protección de datos personales tiene un carácter dinámico, que va día a día va cambiando conforme cambia la sociedad. Prueba de ello, es la situación actual que vive el mundo en relación con la Pandemia del coronavirus, pues en varios países se ha recurrido a diversos medios para controlar el contagio, en países asiáticos, por ejemplo, se han utilizado datos de geolocalización de los ciudadanos para controlar el cumplimiento del aislamiento social y enviar advertencias a quienes estuvieron en contacto con alguien contagiado. El problema es que esta información podría servir para vigilar a las personas y los lugares que frecuentan.

En Chile el problema no ha sido menor, ello por cuanto se ha dado la discusión sobre la entrega de los datos de las personas contagiadas con el COVID-19 a las policías y Fuerzas Armadas para hacer el control de quienes debían cumplir con un periodo de cuarentena, así como también, las Municipalidades solicitaron tener acceso a los datos para poder

llevar un control de los contagios y ofrecer beneficios a los habitantes contagiados de sus comunas. Pero, bajo el imperio de la actual ley ¿es posible que los órganos de salud entreguen este tipo de datos a terceros? Al respecto la Contraloría General de la República se refirió al tema, puntualmente referente a los municipios, mediante el dictamen **N°8113N20**[30], indicando que los terceros no pueden acceder a la información en el marco de la ley vigente, debido a que el artículo 12 de la Ley N°20.584 define la ficha clínica como un instrumento de registro de un conjunto de antecedentes relativos a la salud de las personas, señalando que estos datos son calificados como **dato sensible** de conformidad con lo previsto en la Ley N°19.628. A su vez, el artículo 13 de la Ley N°20.584 establece que los terceros que no estén directamente relacionados con la atención de salud de la persona no tendrán acceso a la información contenida en la respectiva ficha clínica, lo que se extiende, incluso, al personal de salud y administrativo del mismo prestador que no esté vinculado a su atención, además establece que se podrá entregar la información contenida en la ficha clínica, copia de la misma o parte de ella, total o parcialmente, en la forma y condiciones específicas que señala y a solicitud expresa de las personas y organismos que taxativamente indica, esto es, al respectivo titular; su representante legal; sus herederos; los tribunales de justicia -en las causas a las que se alude-, y los fiscales del Ministerio Público y los abogados -previa autorización del juez competente en el caso que se enuncia-.

Finalmente la Contraloría General de la Republica concluye que considerando que ni la referida Ley Nº 20.584 -que no admite otras excepciones que las descritas- ni otro texto legal vigente, autorizan expresamente a las municipalidades o sus respectivos alcaldes para realizar el tratamiento de datos sensibles, no resulta procedente la entrega a tales entidades o autoridades de información de salud relativa a los pacientes que hayan sido diagnosticados con el denominado COVID-19, sin su consentimiento. Cualquier medida en contrario requerirá de la aprobación de la correspondiente ley modificatoria que así lo permita.

Por tanto, estos datos no pueden ser objeto de tratamiento, excepto si el titular consiente en ello, la ley lo autoriza o si es necesario para la determinación u otorgamiento de un beneficio de salud para su titular. En este caso, se puede evidenciar los vacíos de la actual ley, por una situación extrema que quizás no se pensaba que podría ocurrir, pero ocurrió

[30] Dictamen N°8113N20 de la Contraloría General de la Republica.

y tal como es urgente establecer medidas para detener el contagio de la enfermedad, es urgente tener una ley que pueda prever situaciones como esta.

Este tipo de situaciones ya se encuentra regulada en otras partes del mundo como el Reglamento General de Protección de Datos de la Unión Europea que autoriza a tratar este tipo de información personal sin consentimiento de su titular, cuando sea *"necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios"* (art. 9.2.i).[31] Como se señaló anteriormente a propósito de la legislación internacional en la materia, este Reglamento fue dictado para adecuarse a los cambios de la era digital, publicado en 2016, pero vigente desde 2018, introduciendo cambios importantes no solo para los estados miembros "sino también para todas aquellas naciones que mantienen negocios comerciales con los países miembros, o que utilizan información del comportamiento de ciudadanos pertenecientes a la Unión (OCDE, 2017)".[32]

La referida norma autoriza este tipo de tratamiento, lo sujeta al cumplimiento de una serie de requisitos que tienen por objeto asegurar que el mismo sea llevado a cabo de una manera ética, legal y segura. Estos principales mecanismos de resguardo se traducen en la obligación de utilizar estos datos únicamente para fines de salud, observar medidas específicas y adecuadas para proteger los derechos fundamentales y no debe dar lugar a que terceros, como empresarios o compañías de seguros o entidades bancarias, traten estos datos con otros fines[33].

Chile necesita una regulación de esta calidad para no arriesgar que se transfieran, comuniquen o cedan bases de datos sin control y garantías, porque estos vacíos se ven de forma práctica, como ya vimos en cuanto a quienes tendrán acceso a la información de datos sensibles y a como éstos son resguardados, pues en abril de este año se filtraron los datos de personas contagiadas por Covid-19, levantando una vez más la alerta y evidenciando "la fragilidad del ecosistema normativo que protege la información personal

[31] Reglamento General de Protección de Datos de la Unión Europea (p. L119/38) https://www.boe.es/doue/2016/119/L00001-00088.pdf
[32] CLAPES UC. Informe: Privacidad y Protección de datos personales. (p.8)
[33] Considerandos 52, 53 y 54 del Reglamento General de Protección de Datos de la Unión Europea.

en nuestro país. Bajo normas más estrictas, situaciones como estas deberían ser de más difícil ocurrencia"[34]. Lo anterior, solo demuestra lo necesario de contar con una norma robusta en esta materia.

Por lo anterior, el Consejo para la Transparencia, organismo que cuenta de acuerdo a la normativa vigente con la facultad de supervigilar el cumplimiento de la ley en organismos del Estado en materia de protección de datos personales, ha manifestado la posibilidad de tramitar una ley corta que permita hacer frente a las diversas situaciones que hemos debido enfrentar como sociedad a raíz de la pandemia y que afectan nuestros datos personales, además de las situaciones ya señaladas, se debe garantizar los datos que circulan a raíz del teletrabajo, "de esta manera se busca, cerrar brechas de seguridad para proteger información personal y sensible, como es el estado de salud, de la ciudadanía que está entregando gran cantidad de datos no sólo para ser diagnosticado, también para trámites en línea como solicitar un permiso en territorios en cuarentena o teletrabajar",[35]así lo señalo el Presidente del Consejo, Jorge Jaraquemada.

Otro caso que dejó en evidencia las carencias de la actual legislación es el convenio suscrito entre dos órganos públicos, la Agencia Nacional de Inteligencia (ANI) y el Servicio Nacional de Menores (SENAME), el que tiene por objeto transferir datos que están en poder del Sename, o sea, datos de niños, niñas y adolescentes, datos que son considerados como esencialmente sensibles. Junto con lo anterior, se evidenció que este convenio es de carácter amplio, esto, pues no señala que datos serán los transferidos, como serán utilizados o para qué. Según lo expresado por el Consejo para la Transparencia "dicho acuerdo sobrepasa la garantía constitucional de la protección de datos en niños, niñas y adolescentes ya que requiere consentimiento de titulares, una ley que lo autorice o ser objetos de beneficios de salud".[36]

El Presidente del Consejo para la Transparencia recordó que, en la jurisprudencia y pronunciamientos reiterados del Consejo para la Transparencia, los datos de niños, niñas

[34] CONTRERAS Y BORDACHAR (2020) https://ciperchile.cl/2020/03/25/pandemia-y-datos-sensibles/
[35] Consejo para la Transparencia (20.04.2020) https://www.consejotransparencia.cl/en-el-marco-de-la-pandemia-cplt-plantea-ley-corta-para-resguardar-datos-personales/
[36] Consejo para la Transparencia (22.04.2020) https://www.consejotransparencia.cl/cplt-el-convenio-entre-sename-y-la-agencia-nacional-de-inteligencia-no-se-ajusta-a-la-garantia-constitucional-de-proteccion-de-datos-en-ninos-ninas-y-adolescentes/

y adolescentes son de características especialmente sensibles, "por cuanto éstos pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de los mismos". Lo anterior aparece reforzado -agregó- "si consideramos la circunstancia de que se trata de menores de edad que se encuentran en condiciones de especial vulnerabilidad".[37]

Por todo lo expuesto, se considera de suma importancia avanzar en la modificación de la Ley N°19.628, de manera que todos los ciudadanos podamos efectivamente gozar este derecho, principalmente tener mecanismos que impidan su vulneración.

Quizás, 20 años atrás no se consideraba tan importante este derecho, pero hoy podemos ver lo valioso que son los datos personales y lo amplio de estos, que van desde los datos que nos identifican como individuos en la sociedad hasta nuestros datos biométricos que permiten identificarnos a través de equipos modernos que son capaces de identificar nuestras huellas, rostro, etc.

En 2016, el Departamento de Evaluación de la Ley de la Cámara de Diputados realizo una evaluación de la Ley 19.628 con el objetivo de entregar un informe que sirva de insumo para robustecer la norma, en este trabajo participaron expertos en la materia de protección de datos, de diferentes sectores y organizaciones públicas y privadas (Consejo para la Transparencia, abogados y fundaciones expertas en protección de datos personales, CEDI, SERNAC, entro otros) En resumen, detectaron algunos de los siguientes problemas de la Ley 19.628[38]:

- Excepciones que se convierten en la regla general
- Concepto de dato personal es insuficiente
- Fuentes accesibles al público: definición poco clara y escaso control sobre su finalidad
- Falta de un ente de fiscalización y control.
- La norma carece de sanciones efectivas en caso de infracción
- Procedimiento de amparo: indefensión del afectado por infracciones a la ley
- Ausencia de límites en el tratamiento de datos por organismos públicos

[37] Consejo para la Transparencia (22.04.2020) https://www.consejotransparencia.cl/cplt-el-convenio-entre-sename-y-la-agencia-nacional-de-inteligencia-no-se-ajusta-a-la-garantia-constitucional-de-proteccion-de-datos-en-ninos-ninas-y-adolescentes/

[38] Cámara de Diputados de Chile (2016). Consultado en http://www.evaluaciondelaley.cl/wp-content/uploads/2019/07/informe_final_ley_19628_con_portada.pdf

- Utilización abusiva de datos sensibles
- Regulación del consentimiento no contempla nuevas tecnologías.

Como se puede evidenciar la Ley N°19628 necesita urgente una modificación que contenga en parte una solución a los problemas que se han visto en la práctica, porque si bien una legislación más robusta en la materia no es garantía de que el derecho a la protección de datos personales no será vulnerado, pero al menos sus titulares tendrán más herramientas para su pleno ejercicio.

2.2 Análisis del proyecto de ley, Boletín N°11144-07

Durante la discusión se han actualizado las definiciones de conceptos, se establecen los principios rectores de la norma, y se regulan las sanciones para los infractores, etc. Además, se establece un ente fiscalizador y sancionador, en principio se buscaba seguir el modelo internacional de una Agencia de Protección de Datos, independiente y con facultades de control y sanción en caso de incumplimiento de la nueva normativa, tanto por parte de privados o entes públicos, sin embargo, se optó por otorgar esta función al Consejo para la Trasparencia, pasando a denominarse Consejo para la Transparencia y Protección de Datos Personales.[39]

Diversas criticas surgen al traspasar esta importante función al referido Consejo, si bien, este órgano cuenta con altos niveles de independencia y autonomía, desde su creación su labor ha estado enfocada en materializar los principios de acceso a la información pública y la transparencia en la actuación del Estado. Entendiendo que el derecho al acceso a la información pública y el derecho a la protección de datos personales no son materias necesariamente excluyentes, se trata de áreas del derecho que tienen sus propios principios y particularidades.

Por lo demás, cabe preguntarse ¿qué sucedería en la situación hipotética en que una persona requiera acceso al Registro de Datos que estará a cargo del Consejo para la Transparencia, y éste denegara la información, procedería reclamar ante este mismo organismo? Actualmente existe el derecho a solicitar información a los organismos

[39] Diario Constitucional (2019). Consultado en https://www.diarioconstitucional.cl/noticias/asuntos-de-interes-publico/2019/05/07/opinion-tratamiento-de-datos-personales-estado-actual-de-la-legislacion-nacional/

públicos y en caso de no recibir respuesta dentro de 20 días hábiles o la respuesta entregada no le satisface, las personas tienen el derecho a reclamar ante el Consejo para la Transparencia. En el caso hipotético, ¿será el mismo órgano el que resuelva un reclamo en su contra?

El proyecto de modificación de la Ley N°19.628, recoge ciertas materias que quedaron ignoradas en la legislación actual, el objetivo general es actualizar y modernizar el marco normativo e institucional, adecuar el ordenamiento al estándar internacional (Unión Europea y OCDE), definir estándares regulatorios, contar con una autoridad de control de carácter técnico y una institucionalidad pública que asuma los desafíos regulatorios y de fiscalización en materia de protección de las personas y tratamiento de los datos personales.
Se incorporan un conjunto de principios que han sido recogidos también del ámbito internacional como: la licitud del tratamiento, finalidad, proporcionalidad, calidad, seguridad, responsabilidad, transferencia y confidencialidad.

Cabe hacer presente, que el proyecto de ley "no innova respecto de la regulación específica y actualmente vigente, referida al tratamiento de los datos personales relativos a obligaciones de carácter económico, financiero, bancario o comercial, manteniendo íntegramente las normas contenidas en el Título III de la ley, salvo adecuaciones formales y de referencia"[40].

De todas maneras, se debe resaltar que la norma si se hace cargo de las nuevas tecnologías e incorpora la regulación de los datos personales relativos al perfil biométrico tales como la huella digital, el iris, los rasgos de las manos o faciales y la voz. Los datos del perfil biológico humano como datos genéticos, proteómicos o metabólicos. Además, incorpora los datos personales de geolocalización y la forma en que estos deben tratarse.

Adicionalmente, se incorpora el derecho a la portabilidad de datos personales el que consiste en la facultad del titular de datos a solicitar y obtener del responsable, una copia de sus datos personales en un formato electrónico estructurado, genérico y común, que

[40] Boletín N°11144-07. Consultado en https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07

permita ser operado por distintos sistemas, y poder comunicarlos o transferirlos a otro responsable de datos.

El proyecto de ley ha reforzado el tema de la seguridad de los datos, especialmente de los llamados sensibles y lo que sucederá al momento de hacer tratamiento de datos, la forma, el procedimiento y la persona encargada quién cargará con un deber especial de resguardo.

En síntesis, la nueva norma podría entregar mayor cobertura y hacer más eficaz el ejercicio del derecho a la protección de los datos personales pero aún quedan situaciones a mejorar, por ejemplo, se mantiene vigente que la autorización para el tratamiento de datos es la regla general, que arranca del consentimiento que otorgan las personas para ello, considerando que en nuestro sistema la protección de datos personales está vinculado a la privacidad y ésta es un ámbito del que las personas pueden disponer. Sin embargo, en el marco regulatorio de la Unión Europea se parte de la base en que el tratamiento de los datos personales está prohibido y establece 10 reglas que lo autorizan.

Como se analizó, el derecho a la protección de datos personales es un derecho autónomo y no queda suficientemente resguardado con esta posición, en que la regla general es su tratamiento, me parece mas adecuada la postura europea.

Conclusión

En la actualidad, más allá de ser titulares de nuestros datos personales tenemos un derecho de propiedad sobre los mismos, de incalculable valor, que quizás cada uno por separado pareciera no tenerlo, pero al procesarlos y efectuar un tratamiento de los datos personales de una persona se pueden obtener diversos insumos de utilidad en distintas áreas, ya sea políticas, económicas, publicitarias, etc. Por lo que la legislación debe avanzar hacia ese punto, considerando que todos somos dueños de nuestros datos personales y en principio no debería permitirse espacio para que personas naturales o jurídicas, públicas o privadas puedan lucrar con ellos, sin un consentimiento expreso, pero actualmente el consentimiento ya no aparece como una garantía suficiente debido a que la información y los datos se multiplican de manera extraordinariamente rápida y el manejo de su difusión se hace realmente complejo, en una sociedad en que el usuario no tiene la noción de los datos que entrega y cuál es el tratamiento que se hace de ellos.

En relación con lo anterior, debemos tener presente que el derecho a la autodeterminación informativa no puede ser un obstáculo para el desarrollo de las nuevas tecnologías y herramientas que contribuyan a su mejoramiento, considerando que se hace difícil recoger el consentimiento de los usuarios en las distintas materias. Por ello se hace necesario establecer un equilibrio que permita el avance tecnológico, pero con la debida protección de los datos personales, con un tratamiento licito y transparente de los datos y un sistema integral que permita tener datos de calidad.

Entonces ¿el proyecto de ley que modifica la Ley N°19.628, es suficiente para garantizar nuestro derecho a la protección de datos personales?, a mi juicio avanza bastante, pero hubiera preferido un ente dedicado solo a la protección de datos personales dejando al Consejo para la Transparencia cumpliendo su actual función. Si bien se acerca a los estándares internacionales, ya que se tuvo como ejemplo el modelo europeo, será en definitiva el marco jurídico general de Chile el que podrá dejar al país en un nivel aceptable en materia de tratamiento de datos para cumplir con sus compromisos con la Organización para la Cooperación y el Desarrollo Económico (OCDE) pero también para poder mantener relaciones comerciales con Europa.

Sin embargo, se hace complejo tener en consideración cada una de las normas que conforman un sistema de protección de datos y ciberseguridad en Chile debido a la diversidad de normas relativas a la materia, deberíamos avanzar hacia un sistema integral sobre todo considerando los grandes desafíos tecnológicos que como país queremos afrontar, como el Bigdata, el 5G, la transformación digital del Estado, por nombrar algunos y a su vez para estar bien preparados ante situaciones imprevistas como la vivida durante este año a raíz de la pandemia.

Una de las grandes dificultades en cuanto a la protección de datos es la rapidez en que se desarrollan las nuevas tecnologías, por tanto, se requiere de una constante actualización, evidencia de ello, es que al realizar este artículo varias normas dictadas hace no muchos años ya se encontraban derogadas (en otros países) o en vías de modificación así como también los textos, ensayos y artículos relativos a los datos personales, quizás en un par de años este artículo también este obsoleto y deba ser actualizado.

Bibliografía

1)Lohr, Steve (2019): "¿Cuánto valen tus datos digitales? Saberlo puede darte más control sobre ellos", artículo del New York Times, disponible en: https://www.nytimes.com/es/2019/07/29/espanol/proteccion-datos-facebook-google.html

2)BCN (2017) "Órganos de control de protección de datos personales: la experiencia en América Latina" Consultado en https://www.bcn.cl/observatorio/americas/noticias/instituciones-y-proteccion-de-datos-personales-experiencia-en-iberoamerica

3)Bailón, Moisés. "Derechos humanos, generaciones de derechos, derechos de minorías y derechos de los pueblos indígenas; algunas consideraciones generales" Disponible en https://www.corteidh.or.cr/tablas/r28614.pdf

4) García, Aristeo. (2007) "La Protección de Datos Personales: derecho fundamental del siglo XXI, Un estudio comparado". Disponible en http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0041-86332007000300003

5)Versión Consolidada del Tratado de Funcionamiento de la Unión Europea (2012) Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN

6)Convenio para la Protección de las Personas con respecto al Tratamiento Automático de Datos Personales. Disponible en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

7)Directiva 95/46/CE del Parlamento Europeo y del Consejo (1995). Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN

8)Carta de Derechos Fundamentales de la Unión Europea (2000). Disponible en https://www.europarl.europa.eu/charter/pdf/text_es.pdf

9)Constitución Española de 1978. Disponible en https://app.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=18&tipo=2

10)Ley Orgánica 5/1992 de España. (1992). Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189

11)Ley Orgánica 3/2018 de España. Disponible en https://www.boe.es/eli/es/lo/2018/12/05/3

12)Agencia Española de Protección de Datos. Disponible en https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/historia

13)INAI (2015). "Consecuencias por el uso indebido de datos personales". Disponible en http://metabase.uaem.mx/bitstream/handle/123456789/2534/12%20Consecuencias%20por%20el%20uso%20indebido%20de%20datos%20personales.pdf?sequence=1

14)Conversia (2017). "Diferencias entre Europa y Estados Unidos en materia de privacidad y protección de datos (I)". Disponible en http://www.mundolopd.com/lopd/diferencias-europa-eeuu-proteccion-de-datos/

15)Comisión Europea Dirección General de Justicia y Consumidores (2016) "Guía Acerca del Escudo de Privacidad UE-EE.UU.". Disponible en https://www.aepd.es/sites/default/files/2019-09/guia-acerca-del-escudo-de-privacidad.pdf

16)Sentencia C-311/18 del Tribunal de Justicia de la Unión Europea (2020). Disponible en http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=ES&mode=req&dir=&occ=first&part=1&cid=10478869

17)Bojalil, Paulina y Vela, Carlos. (2019). "Despuntan las reformas en materia de protección de datos en América Latina". Disponible en https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/

18)Milanes, Valeria (2017), "Desafíos en el Debate de la Protección de Datos para Latinoamérica." Disponible en https://www.consejotransparencia.cl/wp-content/uploads/2018/04/v_milanes__1_.pdf

19)Ley N°25.326 de Argentina, sobre Protección de los datos personales. (2000). Disponible en https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

20)Lei N°13.709, de Brasil, sobre Protección de datos personales. (2018). Disponible en https://legis.senado.leg.br/norma/27457334/publicacao/27457731

21)Ley Estatutaria N°1581, de Colombia, por la cual se dictan disposiciones generales para la protección de datos personales. (2012). Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

22)Ley Estatutaria N°1266, de Colombia, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. (2008). Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

23)Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de México. (2010). Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

24)Vergara Rojas, Manuel. Chile. "Comentarios preliminares al proyecto de ley que regula la protección y tratamiento de datos personales y crea la Agencia de Protección de Datos Personales"**.** Rev. chil. derecho tecnol. [online]. 2017, vol.6, n.2, pp.135-152. ISSN 0719-2584. Disponible en https://scielo.conicyt.cl/pdf/rchdt/v6n2/0719-2584-rchdt-6-02-00135.pdf

25)Corte Suprema de Justicia. Sentencia Rol N°5243-2015.

26)Bazán, Víctor. Estudios Constitucionales, Año 3 N°2, ISSN 0718-0195, Universidad de Talca, 2005. *El hábeas data y el derecho de autodeterminación informativa en perspectiva de derecho comparado.*

27)Revista Chilena de Derecho Informático (2003) "Autodeterminación informativa y leyes sobre protección de datos". Disponible en http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_simple/0,1493,SCID%253D14341%2526ISID%253D507%2526PRT%253D14331,00.html

28)Schwabe, Jürgen,comp. (2009) *Jurisprudencia del Tribunal Constitucional Federal Alemán: extractos de las sentencias más relevantes compiladas por Jürgen Schwabe.*

29)Canales, María Paz y Viollier, Pablo. (2019) “Chile necesita una regulación de protección de datos con dientes.” Disponible en https://www.derechosdigitales.org/13443/proteccion-de-datos-con-dientes/

30)Dictamen N°8113N20 de la Contraloría General de la Republica (2020).

31)Reglamento General de Protección de Datos de la Unión Europea, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. (2016) Disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf

32)Informe: Privacidad y Protección de datos personales, Centro Latinoamericano de Políticas Económicas y Sociales, CLAPES UC. Disponible en: https://clapesuc.cl/assets/uploads/2019/05/informe-privacidad-y-proteccin-de-datos-personales.pdf

33)Reglamento General de Protección de Datos de la Unión Europea, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. (2016) Disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf

34)Contreras, Pablo y Bordachar, Michelle. (25.03.2020). “Pandemia y datos sensibles”. Ciper Académico, Chile. Disponible en https://ciperchile.cl/2020/03/25/pandemia-y-datos-sensibles/

35)Consejo para la Transparencia (2020). “En el marco de la pandemia CPLT plantea ley corta para resguardar datos personales.” Disponible en https://www.consejotransparencia.cl/en-el-marco-de-la-pandemia-cplt-plantea-ley-corta-para-resguardar-datos-personales/

36)Consejo para la Transparencia (2020). “CPLT: El convenio entre Sename y la Agencia Nacional de Inteligencia no se ajusta a la garantía constitucional de protección de datos en niños, niñas y adolescentes.” Disponible en https://www.consejotransparencia.cl/cplt-el-convenio-entre-sename-y-la-agencia-nacional-de-inteligencia-no-se-ajusta-a-la-garantia-constitucional-de-proteccion-de-datos-en-ninos-ninas-y-adolescentes/

37)Consejo para la Transparencia (2020). “CPLT: El convenio entre Sename y la Agencia Nacional de Inteligencia no se ajusta a la garantía constitucional de protección de datos en niños, niñas y adolescentes.” Disponible en https://www.consejotransparencia.cl/cplt-el-convenio-entre-sename-y-la-agencia-nacional-de-inteligencia-no-se-ajusta-a-la-garantia-constitucional-de-proteccion-de-datos-en-ninos-ninas-y-adolescentes/

38)Cámara de Diputados de Chile (2016). “Evaluación de la Ley N°19.628. Protección de la Vida Privada.” Consultado en http://www.evaluaciondelaley.cl/wp-content/uploads/2019/07/informe_final_ley_19628_con_portada.pdf

39) Diario Constitucional (2019). “Opinión: Tratamiento de datos personales. Estado actual de la legislación nacional.” Consultado en https://www.diarioconstitucional.cl/noticias/asuntos-de-interes-publico/2019/05/07/opinion-tratamiento-de-datos-personales-estado-actual-de-la-legislacion-nacional/

40)Boletín N°11144-07, Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. Disponible en https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07