REVISTA
CES DERECHO

ARTÍCULO DE INVESTIGACIÓN

Desafíos para la modernización de la Ley Protección de Datos Chilena, de cara al alcance extraterritorial del GDPR de la Unión Europea*

Challenges for the modernization of the Chilean Data Protection Law, in the face of the extraterritorial scope of the GDPR of the European Union

Francisco Javier Sanz Salguero [1] ✉

* Este trabajo es parte del proyecto Fondecyt de Iniciación Nº 11221089, "Desafíos para la modernización de la Ley Nº 19.628 de 1999, de cara al alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea GDPR", financiado por la Agencia Nacional de Investigación y Desarrollo ANID (Chile).

[1] Doctor en Derecho, Pontificia Universidad Católica de Valparaíso. Abogado, Universidad Externado de Colombia. Profesor Derecho Constitucional, Universidad Católica de Norte. Director Magíster en Derecho, Universidad Católica de Norte.

Forma de citar: Sanz, Francisco. "Desafíos para la modernización de la Ley Protección de Datos Chilena, de cara al alcance extraterritorial del GDPR de la Unión Europea" En: *Revista CES Derecho*. Vol. 14. No. 1, enero a abril de 2023. pp. 3-16. https://dx.doi.org/10.21615/cesder.6806

Resumen

Con base en el estudio sistemático de la doctrina, la normativa y la jurisprudencia, tanto en el ámbito del derecho chileno como del derecho comparado, temas vertebrados en una única línea central, es posible apoyar el trabajo de perfeccionamiento del actual régimen jurídico de protección de la información personal, formulando recomendaciones a partir de la identificación de los efectos extraterritoriales del Reglamento General de Protección de Datos de la Unión Europa GDPR.

Palabras claves: información personal; Ley Nº 19.628; Reglamento General de Protección de Datos de la Unión Europa; efectos extraterritoriales.

Abstract

Based on the systematic study of the doctrine, regulations and jurisprudence, both in the field of Chilean law and comparative law, topics structured in a single central line, it is possible to support the work of improving the current legal regime for the protection of personal information, formulating recommendations based on the identification of the extraterritorial effects of the General Data Protection Regulation.

Keywords: personal information; Law Nº 19.628; General Data Protection Regulation; extraterritorial effects.

Introducción

A nivel universal, ha sido permanente la preocupación por la tutela de la información personal. La protección de los datos personales debe examinarse, simultáneamente, con los avances alcanzados dentro de la esfera de las telecomunicaciones y el mundo digital, elementos que en conjunto han tenido un impacto en el desarrollo de las prácticas negociales, en los cambios organizacionales del Estado, y en la modificación de la conducta de los individuos dentro del espectro del Internet. La sumatoria de estos factores, determina la importancia del rol de la tutela de la información personal en el contexto actual, circunstancia reconocida por el Derecho Europeo con

Fecha correspondencia:
Recibido: 22 de junio de 2022.
Revisado: 19 de diciembre de 2022.
Aceptado: 30 de enero de 2023.

DOI: 10.21615/cesder.6806
ISSNe: 2145-7719
https://revistas.ces.edu.co/index.php/derecho

la aprobación y reciente aplicación (2018) del Reglamento General de Protección de Datos de la Unión Europa (en adelante GDPR, por sus siglas en inglés), legislación más avanzada en este contexto (Milanés, 2017, p. 20). En el caso chileno, el interés por el resguardo de la vida privada o privacidad y, consecuentemente, la protección de los datos personales, se ha manifestado a través de la continua regulación normativa, regulación que en sus inicios se remonta al Reglamento Constitucional Provisorio de 1812 (desde la perspectiva de la esfera privada de las personas), hasta llegar a la Ley 19.628 de 1999 (en adelante LPD) [estatuto que en su trámite parlamentario surgió bajo la pretensión de tutelar la vida privada, pero que luego de un complejo trámite legislativo terminó limitándose a la protección de los datos personales (Sanz, 2017, p. 136)] (Sanz, 2017, p. 324).

La preocupación por la tutela de la información personal en el ámbito interno ha llegado incluso hasta su reconocimiento como derecho fundamental, garantía consagrada expresamente en el artículo 19 numeral 4 de la Constitución Política (por virtud de la reforma constitucional generada con la Ley 21.096 de 2018). Al momento de escribir estas líneas y en pleno proceso de redacción de una nueva Carta Política, es visible el interés por refrendar el resguardo de la información personal. En efecto, a propósito del debate sobre la dimensión digital de los derechos fundamentales, se ha subrayado en la necesidad de actualizar las normas legales sobre esta temática, preocupación asociada a la exigencia de incorporación de los derechos digitales en la nueva Carta, propósito que, de concretarse, se convertiría en un "significativo avance para el ordenamiento político del país", permitiendo "reconfigurar derechos ya existentes desde la perspectiva de la tecnología de la información, tales como el respeto y protección a la vida privada y a la libertad de expresión" (Universidad Central, s.d).

En el contexto anterior, a pesar de ese permanente interés, actualmente se reconoce el carácter insuficiente del tratamiento normativo de la protección de los datos de carácter personal, ya que solo regula el tratamiento de datos y no el derecho de los titulares a controlarlos. En efecto, la LPD puso énfasis en el derecho a tratar datos de carácter personal para las empresas y entidades gremiales y no reconoció, como primer derecho, el de los titulares a controlar los mismos, en asocio con la falta de anonimato que posibilite un registro y del apoyo administrativo de un órgano *ad hoc*, (Jijena, 2009, pp. 70-71). Igualmente (y no obstante algunos avances alcanzados en los últimos años[1]), otras falencias que subsisten dentro de este marco legal incluyen la ausencia de sanciones efectivas, la falta de regulación del flujo transfronterizo de datos personales, la autorización del uso de datos para marketing directo sin consentimiento del titular, y las amplias excepciones al consentimiento para el tratamiento de datos (Jijena, 2001, p. 22-24).

Las fallas atribuidas a la principal norma chilena en materia de protección de los datos personales, determinan su rezago al momento de contrastarla con leyes análogas aprobadas en otros países de la región, cuyos modelos jurídicos cuentan con organismos especializados en la protección de la información personal, o con normas más modernas, como ocurre en los casos de Argentina, Colombia, México, Perú y Uruguay (Brian, 2018). Superar este rezago adquiere la mayor relevancia, al examinar el modelo interno y su relación con los efectos extraterritoriales atribuidos al GDPR. En este punto de la extraterritorialidad, pese a que estamos haciendo referencia a un reglamento que se aplica directamente a los países miembros de la Unión Europea, el GDPR está dirigido no solo a las organizaciones públicas y privadas establecidas en esta comunidad (artículo 3, GDPR). En efecto, su alcance involucra el tratamiento de datos llevados a cabo por organizaciones, identificadas como "Responsables" y "Encargados" por el Reglamento, sin importar si estas actividades se llevan a cabo dentro o fuera de la Unión. Igualmente, el GDPR sería aplicable a "Responsables" y "Encargados" localizados fuera de la comunidad de países, respecto a actividades como la oferta de bienes o servicios a personas físicas localizadas

[1] Entre estos avances normativos, tenemos la Ley 19.812, publicada el 13 de junio de 2002, la cual modificó a la Ley 19.628 y el Código del Trabajo, con el objeto de que los datos personales de carácter económico, financiero, bancario y comercial dejaran de ser utilizados para discriminar a quienes postulan un puesto de trabajo; la Ley 20.463, publicada el 25 de octubre de 2010, que prohíbe a los administradores de bases de datos personales de carácter financiero tratar datos relativos a deudas de personas físicas, cuando éstas se hubieran producido en el período en que la persona se encontraba sin empleo; la Ley 20.521, publicada el 23 de julio de 2011, la cual prohíbe cualquier tipo de evaluación de riesgo comercial que no esté basada en información objetiva relacionada con la situación financiera de las personas; y la Ley 20.575, promulgada el 14 de febrero de 2012, que consagra el principio de finalidad en la toma de datos personales.

dentro de la Unión Europea (ya sea a título gratuito u oneroso), y al monitoreo del comportamiento de las personas físicas (en la medida en que este tenga lugar en la Unión), entre otros casos (Gómez, 2019, p. 16)[2]. Adicionalmente, el impacto de la vocación extraterritorial del GDPR exige el examen delas propuestas formuladas por la institucionalidad de la Unión Europea con miras al perfeccionamiento de dicha vocación, lo que incluye el estudio de instrumentos como las "Directrices 3/2018 relativas al ámbito territorial del GDPR (artículo 3), Versión 2.1" y las "Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, Versión 2.0".

Con base en los argumentos presentados, la posibilidad de perfeccionar el actual régimen jurídico chileno de protección de la información personal, exige la identificación de los alcances que tiene la vocación de eficacia del GDPR más allá del territorio de los Estados de la Unión Europea. A partir de esta premisa, y como punto de partida de una investigación más profunda, en el presente artículo hacemos un estudio preliminar en el que abordamos el estado de la cuestión en la relación entre el GDPR y la LPD, examinamos los avances en la identificación de deficiencias dentro de la esfera de la normativa de protección de información personal, y nos aproximamos a la vocación de eficacia extraterritorial del GDPR. Al finalizar el texto y dentro del marco de investigación planteado, a modo de conclusión formulamos los pasos o etapas de estudio que deben ser desarrollados, a fin establecer los alcances de la vocación de eficacia del GDPR, y su impacto en la modernización y perfeccionamiento del ordenamiento jurídico chileno de protección de los datos personales.

1. Estado de la cuestión en la relación entre el GDPR y la LPD

A nivel nacional, ya existe una discusión sobre la necesidad de implementar la regulación europea como un estándar más completo que la legislación interna. Simultáneamente, cursa en el Congreso chileno un proyecto de ley con inspiración en el reglamento europeo, contenido en el Boletín N°11.144-07[3], iniciativa que constituye un aporte con miras a la modernización del tratamiento de datos pero que, aun sin estar aprobado, ya ha sido objeto de comentarios por parte de la doctrina, en materias como la situación del encargado de tratamiento de datos (Vergara, 2017, pp. 145-146). Pese a estos avances, se observa una ausencia de trabajos especializados en el carácter transnacional del GDPR y su impacto en el tratamiento de la información personal dentro del escenario interno, impacto que no solo se limita a la esfera de lo jurídico, dadas las potenciales consecuencias sociales y económicas que involucra el uso (o mal uso) de esta información privilegiada. Desde la perspectiva chilena, un estudio en este sentido permitiría resolver diversos interrogantes: ¿qué ocurre cuando una persona que haga parte de la Unión Europea, realiza un tratamientode la información personal fuera esta comunidad de naciones?, ¿en qué situaciones el GDPR se aplica a personas establecidas fuera de la Unión Europea?, ¿en qué casos definitivamente no se aplica el alcance extraterritorial del GDPR?

Paralelamente y en la órbita de lo económico (siempre dentro del tratamiento de la información personal), la identificación de los efectos del GDPR tendría incidencia al momento de precisar los alcances del Acuerdo de Asociación Chile-Unión Europea (en adelante AAE Chile-UE), suscrito el 2002[4]. A este respecto, no obstante en el AAE Chile-UE las partes concertaron "*cooperar en la protección de los datos personales"* (artículo 30), poner en práctica esta directriz exige establecer de forma clara el rango de acción del GDPR en los términos explicados. La necesidad de esta labor, adquiere mayor relevancia teniendo en cuenta que desde el año 2015 se constituyó un Grupo de Trabajo para avanzar en la profundización del Acuerdo, Grupo que, en el contexto de una eventual renegociación del AAE Chile-UE, ya ha tenido que afrontar una serie de controversias[5].

Desde otra perspectiva geográfica y concentrándonos en la región Asia-Pacífico (entendida como la ribera

[2] En efecto, otra hipótesis en la que se reconoce el carácter extraterritorial del GDPR, determina la aplicación del Estatuto a los "Responsables" que no se encuentren en la Unión Europea sino en un lugar en el que aplique el derecho de un Estado miembro de la Unión, en virtud a un tratado de derecho internacional.

[3] Proyecto de ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales.

[4] Suscrito el 8 de noviembre de 2002, y promulgado en el Decreto 28 del 28 de enero del 2003.

[5] Para destacar, tenemos las protestas generadas en Chile contra los perjuicios ambientales que el pacto puede traer. [Contenido en: https://www.dw.com/es/ue-chile-libre-comercio-gran-controversia/a-44985496].

opuesta del Pacífico, desde Rusia y Japón por el norte hasta Nueva Zelandia por el sur), teniendo en cuenta la pertenencia de Chile al Foro de Cooperación Económica Asia-Pacífico APEC desde el año de 1994 (Wilhelmy, 2010, pp. 125 y 130), otra temática que puede examinarse son los probables efectos del GDPR en su relación con el Sistema de Reglas de Privacidad Transfronteriza del APEC (o CBPR, por sus siglas en inglés), uno de los instrumentos que promueve el Marco de Privacidad de APEC, el cual se aprobó en el 2004 con el fin de adoptar principios de protección a la privacidad y al mismo tiempo evitar la creación de barreras para los flujos de información (Galves, 2019).

Superar el desafío de adecuar la LPD a los estándares establecidos por el GDPR, implica inicialmente llevar a cabo un trabajo que involucre la revisión del estado del arte en la relación entre el GDPR y la LPD, establecer los avances en la identificación de deficiencias dentro del marco de la normativa de protección de información personal, y definir los alcances de la vocación de eficacia extraterritorial del GDPR.

2. Avances en la identificación de deficiencias, dentro del marco de la normativa de protección de información personal

Desde el punto de vista doctrinal, son diversas las observaciones que se han formulado al contenido de la LPD. De hecho, de toda la producción normativa en Chile relativa al espectro informático, el estatuto sobre protección de datos personales ha sido el más criticado, al punto que en el Congreso Nacional se registran numerosos intentos de modificación (Vergara, 2017, p. 135). En este sentido, la sistematización de la discusión sobre las fallas detectadas en la citada Ley, exige examinar áreas que transcurren entre la posibilidad del titular de disponer de su propia información, la dificultad por establecer el concepto de "fuente accesible al público", los desafíos que conlleva el establecimiento de los "intereses legítimos" para dar tratamiento a los datos personales, la necesidad de establecer una autoridad con la potestad de controlar el tratamiento de esta información especialmente protegida, y las variables propias de una falta de regulación del flujo transfronterizo de estos datos.

Adicionalmente, otros asuntos que han sido objeto de crítica (o al menos de algún comentario) dentro del escenario de la normativa sobre tratamiento de la información personal, incluyen temas como la ausencia de sanciones efectivas, y la presencia de excepciones amplias al consentimiento para el tratamiento de datos (Jijena, 2001, pp. 22 – 24).

Igualmente, tenemos el impacto de la normativa vigente y su relación con el tratamiento de los datos personales en el Poder Judicial, en donde la doctrina plantea que el artículo 2, letra c) inciso tercero de la Ley de Tramitación Electrónica (Ley 20.886 de 2015) deja la puerta abierta para una desregulación de los datos personales que se encuentran en las bases de datos del Poder Judicial[6].

En este orden de ideas, incluso observamos la discusión originada en temas coyunturales, como lo es el impacto de la pandemia por el Covid 19, y su relación con la tutela de la información personal. En el debate, se reconoce que en el ámbito del derecho comparado, puntualmente en algunos ordenamientos jurídicos, las autoridades de control han servido de contrapeso o limitado las pretensiones de ciertas autoridades de incrementar los niveles de control y vigilancia de las personas (con la excusa de controlar la propagación del Covid-19); promover el uso de aplicaciones que atentan contra la privacidad de los usuarios y desproporcionadas en la recolección de datos personales; o solicitar accesos indebidos a datos de fichas clínicas de personas contagiadas (Álvarez, 2020, p. 1).

[6] La norma en comento, al regular el "principio de publicidad", estipula que "*Se prohíbe el tratamiento masivo de los datos personales contenidos en el sistema de tramitación electrónica del Poder Judicial, sin su autorización previa. La infracción cometida por entes públicos y privados a lo dispuesto en este inciso será sancionada conforme a la ley Nº 19.6282*". La crítica aparejada a esta norma, tiene que ver con la amplitud y la poca claridad de la naturaleza de la autorización necesaria, junto con la aparente cesión de los datos forzosa al momento de ingresar información a la base de datos del Poder Judicial, y la consecuente desprotección del titular de estos datos frente a la Administración de Justicia (Bustos, 2018, p. 43).

Vol. 14 No. 1 / enero - abril de 2023

2.1. Limitado poder de disposición que tienen los titulares respecto a sus datos personales

Inicialmente, uno de los temas que ha sido objeto de mayor cuestionamiento lo constituye el limitado poder de disposición que tienen los titulares respecto a sus datos personales. Esta falencia, viene desde el origen de la aprobación de la Ley, ya que la norma prefiere el tratamiento de datos, relegando el derecho que tienen los titulares de la información personal a controlar los mismos (Jijena, 2009, pp. 70-71). Como consecuencia, en la praxis se privilegia el tratamiento de los datos por parte de las empresas (Jijena, 2009, pp. 70-71), tal como ocurre con las empresas de marketing que conocen la información de los ciudadanos, negocio atribuido a las sociedades responsables de las bases de datos. El origen de esta anomalía se remonta al proceso de incorporación del Estado chileno a la Organización para la Cooperación y el Desarrollo Económicos OECD, proceso en el cual se estimó que las deficiencias de la legislación nacional eran una barrera de entrada para el ingreso de Chile a este organismo internacional. Para superar esta dificultad, la solución adoptada por el Gobierno consistió en presentarse ante los evaluadores europeos promoviendo e impulsando los cambios en materia de políticas públicas y las normas chilenas relacionadas, y comprometiendo formalmente ante la señalada organización, la posterior aprobación en el Parlamento de las modificaciones legales necesarias para la estandarización o adecuación normativa a las directrices y políticas del órgano europeo. Este compromiso, aún se encuentra en mora de cumplimiento.

Retornando al privilegio en el tratamiento de los datos por parte de las empresas, consultores del sector empresarial advierten del impacto que el GDPR puede ocasionar a este tipo de sociedades, formulando diversas recomendaciones a fin de enfrentar este nuevo escenario, propuestas que sugieren identificar áreas de relevancia (equipos, procesos y labores que involucran el tratamiento de datos personales), conocer y revisar las bases para el tratamiento lícito de datos, limitar el tratamiento de datos (y, de paso, uniformar su procedimiento), y designar un encargado de cumplimiento (es decir, contar con una persona o equipo dedicado y especializado en el tratamiento adecuado de la información personal) (Lluch, 2020, pp. 12-13).

Continuando con el negocio llevado a cabo por las sociedades responsables de las bases de datos, para el individuo común resulta difícil restringir el tratamiento de la información personal que se encuentra depositada en estas, restricción que se hace más compleja cuando hablamos de la información inserta en las redes sociales *on line,* independientemente de la definición que le otorguemos a esta manifestación de la interacción humana[7] (sugerimos, para lograr una mejor aproximación al tema, tener en cuenta la siguiente:

> "las Redes son formas de interacción social, definida como un intercambio dinámico entre personas, grupos e instituciones en contextos de complejidad. Un sistema abierto y en construcción permanente que involucra a conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos"[8]).

En el contexto anterior, entre los elementos que configuran una red social de los cuales surgen las principales transgresiones hacia la vida privada de las personas (junto con los elementos "comunicación" y la "interconectividad"), al concentrarnos en la información personal debemos destacar el elemento "identidad", teniendo en cuenta que los datos personales que conforman nuestra personalidad son el medio de cambio para poder ingresar y participar en estos servicios: el exceso de contenido vertido en este tipo de plataformas, hace posible obtener una perspectiva general de la personalidad de determinado individuo, personalidad que está protegida como una proyección de su privacidad (Herrera, 2016, pp. 93-95). Ciertamente, pese a la amplitud en cuanto a las clasificaciones de las redes sociales que operan en la actualidad (Burgueño, s.d.), las más utilizadas

[7] A este respecto, el Grupo de Estudios del artículo 29 del Consejo de Europa, las identifica como aquellas plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes (Dictamen del Consejo de Europa 05/2009 sobre redes sociales en línea). Entre tanto, la Agencia Española de Protección de Datos (AEPD) las define como los "servicios prestados a través de internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al ser publicados".

[8] Esta definición, se propuso durante las Jornadas sobre Gestión en Organizaciones del Tercer Sector, llevadas a cabo en la Universidad Di Tella de Buenos Aires, Argentina, en noviembre de 2001 (Caldevilla, 2010, p. 46).

(Facebook, Twitter, entre otras) generan mayor amenaza a la vida privada y, por ende, al debido resguardo de la información personal. De todas formas, no se puede otorgar un carácter perverso *per se* a estas formas de interacción, ya que buena parte de las desventajas que observamos en ellas dependen de las intenciones y los criterios ético-morales del usuario. En este sentido, no podemos concluir que las redes en sí son culpables de los comportamientos de éstos, ni de las consecuencias de sus actos (Caldevilla, 2010, p. 66).

Junto con la problemática que plantea el fenómeno de las redes sociales, un nuevo desafío lo representa el internet de las cosas (IoT, en su acrónimo en inglés), tecnología basada en la interconexión de objetos cotidianos, y que consiste en la comunicación que se establece entre las "cosas" de uso diario, a través de una conexión a Internet, con la pretensión de mejorar la vida del individuo. A este respecto, la doctrina reconoce con el desarrollo del IoT una serie de amenazas que se concretan en vulneraciones a la privacidad y, en particular, a la protección de datos personales, amenazas representadas en la asimetría de la información, la ausencia de control sobre la información personal, el consentimiento inexistente o ineficaz, y las malas prácticas de los actores del IoT (Jervis, 2015, pp. 28-31).

Finalmente, en contraste, dentro del marco del GDPR el escenario es diferente: la Unión Europea quiere dar a las personas más control sobre cómo se utilizan sus datos personales, teniendo en cuenta que muchas empresas como Facebook y Google intercambian el acceso a los datos de las personas para el uso de sus servicios (Power Data, 2018).

2.2. Carácter ambiguo de la definición de "fuente accesible al público"

Actualmente, la regla general en Chile es que, para tratar un dato personal, se requiere el permiso de su titular (artículo 20, LPD). Sinembargo, como excepción a esa regla general, es posible acceder a esa información cuando el dato se encuentra en una "*fuente accesible al público*" (artículo 4º inciso 5º, LPD). El problema identificado, surge a partir de la definición que la Ley otorga a esta fuente. En efecto, la norma define como fuentes accesibles al público "*los registros o recopilaciones de datos personales públicos o privados, de acceso no restringido o reservado a los solicitantes*" [artículo 2 letra i) Ley Nº 19.628]. La ambigüedad de este concepto (Anguita, 2007, pp. 295-296) determina como, a menos que el titular de la información permita su divulgación, o a menos que la ley prohíba expresamente esa divulgación, cualquiera puede dar tratamiento a la información que se encuentra en esta "fuente". Por tanto, y aplicando las definiciones y excepciones de la normativa chilena vigente, las redes sociales y, en general, la información contenida en "internet", es considerada una información accesible al público. Estamos aquí ante una excepción tan amplia que termina transformando la desprotección en la regla general: de ahí la proliferación de sitios web que exponen los datos de los ciudadanos, o de empresas que los utilizan para entregar inteligencia de negocio a campañas políticas (Kraus y Sanz, 2018).

En este contexto, con base en el concepto de "fuente accesible al público" consagrado en la LPD, otra duda que se plantea es la de establecer si las bases o bancos de datos personales que mantienen los servicios públicos deben ser consideradas legalmente como fuentes de acceso público, o como fuentes de acceso reservado o secreto. A este respecto, para la doctrina la respuesta a este interrogante sólo puede determinarse considerando la especial naturaleza del dato personal tratado, anotando que por regla general los sistemas de tratamiento de datos personales del sector público no deben ser considerados fuentes accesibles al público, o fuentes públicas de información personal, pese a la amplitud de la definición legal (Jijena, 2009, p. 37).

2.3. Falta de establecimiento de "intereses legítimos" para dar tratamiento a los datos personales

En la práctica, una persona natural o jurídica puede tener la legítima necesidad de dar tratamiento a la información personal. Esto ocurre cuando el tratamiento de datos persigue exclusivamente fines históricos, estadísticos, científicos y de estudios o investigaciones. Una situación análoga se presenta, cuando las bases de datos de una empresa que trabaja en el de marketing están a punto de caducar. Frente a estas necesidades

legítimas de información, la actual normativa chilena falla al no contemplar un conjunto de "intereses legítimos" que el interesado pueda argumentar, anomalía vinculada estrechamente con el carácter indeterminado de esta noción jurídica (Guasch y Soler, 2015, p. 438), concepto que incluso puede resultar vago y ambiguo (Ferretti, 2014).

No obstante que el proyecto de ley más adelantado que cursa en el Congreso Nacional abarca esta materia (proponiendo avanzar hacia un sistema más complejo de títulos habilitantes para el tratamiento de datos personales)[9], la misma iniciativa determina que el interés legítimo del responsable del tratamiento o un tercero aparezca como un elemento de balance que, caracterizado por su formulación a partir de conceptos abiertos o indeterminados, vendría a dotar de cierta flexibilidad al nuevo modelo. En consecuencia, este rasgo otorgado en el proyecto a los "intereses legítimos", determinaría la necesidad de un desarrollo hermenéutico que complete su contenido (Contreras y Trigo, 2020, p. 203). Esta labor de interpretación, exigirá el examen de los recursos disponibles en el derecho comparado, principalmente las distintas fuentes del derecho de la Unión Europea, partiendo por el GDPR (en especial sus artículos 6 y 7), sin olvidar el rol jugado por la derogada Directiva 95/46/CE [en su momento, objeto de críticas en el ámbito del interés legítimo[10]], e incorporando el estudio de la jurisprudencia del Tribunal de Justicia de la Unión Europea y los fallos de los Tribunales en cada Estado (Contreras y Trigo, 2019, pp. 77-94). Esta revisión comparada, debe también tener en cuenta el tratamiento otorgado al interés legítimo por diversas legislaciones a nivel regional, como fuente habilitante para el tratamiento de datos personales, trabajo que incluye los casos del Perú (artículo 14, Ley 29.733 de Protección de Datos Personales de 2011), Brasil (artículo 7, numeral 9, Ley General de Protección de Datos Personales de 2018[11]) y Argentina (con su proyecto de ley que tiene por finalidad reemplazar su actual normativa sobre protección de datos, contenida principalmente en la Ley 25.326 del 2000[12]).

2.4. Ausencia de una autoridad con la potestad de controlar el tratamiento de los datos personales

Desde la perspectiva del tratamiento de los datos personales, en el plano doctrinal se reconoce la falta de un órgano *ad hoc* con la capacidad de ejercer un control en este sentido (Jijena, 2009, pp. 70–71). En efecto, para el caso chileno no existe un organismo con características de imparcialidad e independencia, dotado de facultades de oficio y técnicas en la resolución de conflictos surgidos en materia de privacidad y protección de datos personales. La consecuente situación de desprotección, determina que los propios titulares de los datos sean quienes deban velar por el resguardo de su información, mediante la presentación de una demanda ante la jurisdicción civil, con todas las vicisitudes en materia de tiempo y costos que esto implica para el afectado (Kraus y Sanz, 2018).

Frente al escenario anterior, hay que reconocer el avance que supone la iniciativa legislativa contenida en el Boletín N°11.144-07, proyecto en el que se crea una "Agencia de Protección de Datos", organismo de carácter especializado y diferente de otros, superando la intención presente en otros proyectos de ley por radicar la función de tutela de la información personal en organismo como la Contraloría General de la República (Anguita, 2007, pp. 283-284), el Servicio Nacional del Consumidor[13], el Consejo para la Transparencia (Álvarez, 2016, pp. 68-73), o el Servicio de Registro Civil (Anguita, 2007, p. 284).

Son diversas las ventajas que implicaría el establecimiento de este organismo (siempre que se adopte lo contenido en el proyecto), teniendo en cuenta ámbitos como la naturaleza administrativa de la entidad, el mecanismo de selección del jefe superior a través del sistema de la Alta Dirección Pública de la Ley 19.882

[9] Contenido, recordemos, en el Boletín N°11.144-07.

[10] Se entendía que el interés legítimo, por su naturaleza, brindaba a los Estados miembros de la Unión Europea un amplio margen para establecer los elementos que permitiesen determinar su existencia y alcances (al dictar la respectiva normativa de transposición), lo que fue reconocido por la Comisión Europea en sus diversas evaluaciones sobre la implementación de la Directiva (Baldoni y otros, 2013, p. 245).

[11] Vigente desde el 18 de septiembre del 2018.

[12] Publicado en el Boletín Nacional del 2 de noviembre del 2000.

[13] Boletín 8.143-03, artículo segundo, que modifica varias disposiciones de la ley del consumidor.

(aunque se ha discutido sobre el uso poco eficiente del lenguaje para designar al superior como «director o directora»), la entrega de normas sobre coordinación entre la Agencia y el Consejo para la Transparencia, el régimen estricto de incompatibilidades (salvo para los casos de docencia y participación en entidades internacionales), y el tratamiento del personal y el patrimonio (llamando la atención que la iniciativa desiste de lo estipulado en otras entidades de reciente creación, en cuanto a recurrir a las normas de derecho privado para su personal[14]), entre otras materias (Vergara, 2017, pp. 141-142).

2.5. Falta de regulación del flujo transfronterizo de los datos personales

La regulación sobre los datos, ya sea sobre su uso nacional o sobre su flujo transfronterizo, busca el balance entre dos intereses que se anteponen. En este escenario, por un parte las empresas tienen necesidad de información de tal manera que, entre más facilidad posean para la recopilación de los datos, su almacenamiento, su transferencia, su análisis y comercio, mayores serán sus beneficios económicos. Por otro lado, las personas (y comunidades) tienen necesidad de protección de su información (Oficina de Información científica y Tecnológica para el Congreso de la Unión, 2019, p. 1).

El creciente flujo transfronterizo de datos personales, confirma la necesidad de adoptar una aproximación a la normativa internacional, a efectos de garantizar el apropiado nivel de resguardo para las personas concernidas por la información. Esta aproximación, debe alcanzarse evitando la adopción de barreras innecesarias al libre movimiento de los datos, con sus nocivos efectos para una economía global e interconectada (Cerda, 2011, p. 353).

Una hipótesis en la que se conspiraría contra la mencionada libertad en el movimiento de datos, podría ser la aplicación no coordinada entre las leyes sobre protección de datos personales y los tratados multilaterales que establecen las reglas que gobiernan el comercio internacional (las cuales son hechas cumplir por la Organización Mundial de Comercio OMC). A este respecto, tenemos el caso del Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT) de 1948, y el Acuerdo General sobre el Comercio de Servicios (GATS) de 1995. Con relación al GATS y su propósito de asegurar un justo y equitativo trato entre todos los partícipes del comercio internacional, este acuerdo establece dos obligaciones cuya aplicación podría colisionar con las normas que resguardan la información personal. En primer lugar, tenemos el "principio de trato nacional", el cual exige que cada miembro no adopte medidas discriminatorias entre servicios nacionales y extranjeros[15]. En segundo lugar, tenemos el "principio de la nación más favorecida"[16], obligación que estipula que cada miembro dará inmediata e incondicionalmente a cualquier otro miembro un tratamiento no menos favorable que aquél provisto a cualquier otro miembro (Cerda, 2011, 347). De todas formas, y dentro de la labor de resguardo de los datos personales, para evitar situaciones en las cuales un Estado adopte medidas discriminatorias entre los servicios provistos por sus propios nacionales y aquéllos suministrados por extranjeros, o realice tal tipo de distinción entre los servicios prestados por nacionales de otros países, el GATS plantea algunas excepciones que permiten adoptar medidas de política pública inconsistentes con las obligaciones del mismo Acuerdo comercial, una de ellas vinculada con la protección de la privacidad de las personas en relación con el procesamiento y diseminación de sus datos personales[17] (Cerda, 2011, pp. 347-348). Es pertinente aclarar, que la señalada excepción está limitada (Swire y Litan, 1998, p. 191) y sometida a las exigencias del artículo XIV del GATS, a fin de evitar el abuso de las excepciones[18].

[14] En efecto, el proyecto de ley desiste de lo establecido en otros organismos, en cuanto a recurrir a las normas de derecho privado para su personal (Código del Trabajo), haciendo aplicación del Estatuto Administrativo.
[15] Puntualmente, el artículo XVII numeral 1º del GATS estipula que "*En los sectores inscritos en su Lista y con las condiciones y salvedades que en ella puedan consignarse, cada Miembro otorgará a los servicios y a los proveedores de servicios de cualquier otro Miembro, con respecto a todas las medidas que afecten al suministro de servicios, un trato no menos favorable que el que dispense a sus propios servicios similares o proveedores de servicios similares*".
[16] Artículo, numeral 1º, GATS.
[17] Al respecto, el artículo XIV letra c) (ii) del GATS estipula como excepción "*la protección de la intimidad de los particulares en relación con el tratamiento y la difusión de datos personales y la protección del carácter confidencial de los registros y cuentas individuales*".
[18] Sobre el particular y para tener en cuenta, *Work Programme on Electronic Commerce, Progress Report to the General Council*, adoptado por el Consejo del Comercio de Servicios el 19 de julio de 1999, *WTO document S/L/74, 27 July 1999*, párrafo 14.

Teniendo en cuenta que la actual norma chilena no ordena una prohibición de transferencia internacional de datos personales a países carentes de un adecuado sistema de protección [falencia que se detectó desde el inicio de la aplicación de la Ley 19.628, (Jijena, 2001, pp. 22–24)], su modernización implica el establecimiento de disposiciones que permitan, por un lado, una tutela efectiva de la información personal y, por otro lado, la generación de escenarios que no obstaculicen el tráfico normal de esta información dentro del marco de las relaciones negociales. Una de las virtudes del proyecto de ley contenido en el Boletín N°11.144-07, en el evento de que se apruebe, consiste en la distinción entre países que poseen niveles adecuados de protección y los que no lo tienen, en el contexto de la transferencia internacional de la información personal.

3. Vocación de eficacia extraterritorial del GDPR: comentarios y perspectivas

Apuntando a la mejor comprensión de la vocación de eficacia extrateriotorial atribuido al GDPR, en esta parte de la investigación revisamos el contenido de este Reglamento enfatizando en el ámbito de su aplicación territorial, asociado al estudio de las propuestas formuladas por la institucionalidad de la Unión Europea con miras al perfeccionamiento de dicha vocación.

4. Comentarios sobre la vocación de eficacia extraterritorial del GDPR

El GDPR y la Directiva 95/46/CE que deroga, comparten un principio: "las personas físicas deben tener el control de sus datos personales". No obstante esta coincidencia, el Reglamento Europeo supone un cambio sustancial de enfoque hacia una verdadera cultura de la prevención y protección de los datos personales en la Unión (Fuensanta, 2018, p. 190).

Al sistematizar las principales novedades del GDPR, y teniendo como criterios de clasificación las materias más afectadas, podemos establecer la siguiente categorización (FUNDACIÓN ESYS, 2016): (1) novedades que afectan a la gobernanza empresarial y cumplimiento normativo (*compliance*); (2) fortalecimiento y nuevos derechos de los ciudadanos y (3) novedades que afectan al control y supervisión del cumplimiento normativo. En la esfera de la última categoría, el nuevo escenario para el control y supervisión del cumplimiento normativo involucra cambios en diversas áreas. En primer lugar, tenemos la creación de un organismo con capacidad decisora y consultiva, como es el caso del Comité Europeo de Protección de Datos CEPD; en segundo lugar, observamos el endurecimiento de las sanciones administrativas [unificando los criterios comunitarios para la imposición de sanciones, y aumentando su cuantía para garantizar la mayor protección de un derecho fundamental como la privacidad (Ortega y Gonzalo, 2018, p. 11)]; finalmente, tenemos la ampliación del concepto de dato personal (Fuensanta, 2018, pp. 191-192). Precisamente, uno de los temas que deberá ser objeto de estudio, lo constituye la identificación de los alcances de la competencia del CEPD. A este respecto, hay que tener en cuenta que este Comité no solo emite directrices sobre la interpretación de los conceptos básicos del GDPR, sino que también se pronuncia para adoptar decisiones vinculantes sobre disputas relacionadas con las actividades de tratamiento transfronterizo, garantizando así una aplicación uniforme de las normas de la UE para evitar que el mismo caso pueda ser tratado de manera diferente en distintos territorios.

Avanzando en la temática propuesta, observamos que el ámbito de aplicación territorial del GDPR determina su vocación de eficacia más allá de los límites de la comunidad de países. Este "Ámbito territorial", está consagrado en el artículo 3 del Reglamento, norma que incorpora al derecho positivo la doctrina expansiva del Tribunal de Justicia de la Unión Europea [particularmente, las sentencias del Tribunal C-131/12 del 13 de mayo de 2014 (asunto Google Spain), y C-230/14 del 1 de octubre de 2015, (asunto Weltimmo)][19] y que, en consecuencia, se

[19] Dichas sentencias del Tribunal de Justicia de la Unión Europea, estipulan que "*De lo anterior se deriva, como señaló en esencia el Abogado General en los puntos 28 y 32 a 34 de sus conclusiones, una concepción flexible de la noción de establecimiento, que rechaza cualquier enfoque formalista según el cual una empresa estaría establecida únicamente en el lugar en que se encontrase registrada. Por lo tanto, para determinar si una sociedad, responsable de un tratamiento de datos, dispone de un establecimiento, en el sentido de la Directiva 95/46, en un Estado miembro distinto del Estado miembro o del tercer país en el que está registrada, procede interpretar tanto el grado de estabilidad de la instalación como la efectividad del desarrollo de las actividades*

aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del "responsable" o del "encargado" en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no. La misma norma (artículo 3.3), considera aplicable al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión, sino en un lugar en que el Derecho de los Estados miembros resulte de aplicación, situación que determina como el GDPR no es ajeno a las normas de Derecho internacional público (Bauzá, 2019, p. 126).

Continuando con el "Ámbito territorial" y poco tiempo después de la aprobación del GDPR, el propio CEPD, mediante las "Directrices 3/2018 relativas al ámbito territorial del GDPR (artículo 3), Versión 2.1"[20] (en adelante "Directrices"), reconoció como materias de la mayor importancia el que, por un lado, el artículo 4 de la Directiva tiene como objetivo definir qué legislación nacional de un Estado miembro es de aplicación, mientras que el artículo 3 del GDPR define el ámbito territorial de un texto directamente aplicable. Simultáneamente, el CEPD aclara en las "Directrices" que "si bien el artículo 4 de la Directiva hacía referencia al hecho de «recurrir a medios» situados en el territorio de la Unión como base para llevar a los responsables del tratamiento que no «estaban establecidos en el territorio de la Comunidad» al ámbito de la legislación en materia de protección de datos de la Unión Europea, esta referencia no aparece en el artículo 3 del GDPR". Finalmente, las "Directrices" señalan que el artículo 3 del GDPR define el ámbito territorial del Reglamento sobre la base de dos criterios principales: el criterio del «establecimiento»[21], y el criterio de la «selección de destinatarios»[22], agregando el organismo que, cuando se cumpla uno de estos dos criterios, las disposiciones pertinentes del GDPR se aplicarán al tratamiento correspondiente de los datos personales por parte del responsable o del encargado del tratamiento en cuestión.

5. Perspectivas sobre la vocación de eficacia extraterritorial del GDPR

Concentrados en la vocación de eficacia extraterritorial del GDPR, el estudio de las propuestas formuladas por la institucionalidad de la Unión Europea a fin perfeccionar esta vocación, se configura en un insumo clave dentro de la pretensión por construir un régimen jurídico de protección de la información personal adecuado para el ámbito chileno. En este contexto, un instrumento a tener en cuenta son las "Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, Versión 2.0" (en adelante "Recomendaciones")[23].

El Acto anterior, a pesar de no tener un carácter vinculante y fundamentado en el doble propósito de creación del GDPR (consistente en facilitar la libre circulación de datos personales dentro de la Unión Europea, sin abandonar el debido resguardo de esta información), reconoce en el capítulo V del GDPR encargado de regular las transferencias de datos personales a "terceros países"[24] una condición necesaria: la transferencia no debe

en ese otro Estado miembro tomando en consideración la naturaleza específica de las actividades económicas y de las prestaciones de servicios en cuestión. Esto es válido concretamente para las empresas que se dedican a ofrecer servicios exclusivamente a través de Internet".

[20] A través de una interpretación común por parte de las autoridades de protección de datos en la Unión Europea, la pretensión principal de estas directrices (adoptadas inicialmente por el CEPD el 16 de noviembre, y que fueron objeto de una consulta pública realizada entre el 23 de noviembre de 2018 y el 18 de enero de 2019 y se han actualizado teniendo en cuenta las contribuciones y observaciones recibidas) es la de garantizar una aplicación coherente del GDPR, a la hora de evaluar si el tratamiento concreto por parte de un responsable o encargado se corresponde con el ámbito de aplicación del nuevo marco legal de la Comunidad de Estados Europeos.

[21] De conformidad con el artículo 3, apartado 1 del GDPR.

[22] Con arreglo al artículo 3, apartado 2 del GDPR.

[23] Estas "Recomendaciones", tienen su origen en la sentencia del Tribunal de Justicia de la Unión Europea en el asunto Schrems II (C-311/18), originada en un proceso cuyas partes principales fueron la *Data Protection Commissioner* (en calidad de demandante) y Maximillian Schrems/*Facebook Ireland* (en calidad de demandados). En la sentencia, el Tribunal de Justicia invalidó la Decisión 2016/1250 sobre la adecuación de la protección conferida por el Escudo de la privacidad Unión Europea-EE. UU, declarando en cambio que la Decisión 2010/87 de la Comisión Europea, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, es válida [contenido en https://www.iustel.com/diario_del_derecho/noticia.asp?ref_iustel=1201034].

[24] Es decir, cualquier país que no sea un Estado miembro Espacio Económico Europeo, que incluye a los Estados miembros de la Unión Europea y a Islandia, Noruega y Liechtenstein. Véase: ANEXO 1: DEFINICIONES, Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, Versión 2.0. [contenido en: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_es.pdf].

menoscabar el nivel de protección de las personas físicas garantizado por el GDPR[25]. Bajo esta premisa, y con el objetivo de apoyar a los responsables y encargados del tratamiento que actúan como exportadores de datos con su deber de aplicar las medidas para garantizar un nivel adecuado de protección a las transferencias de información personal, las "Recomendaciones" acuden a un plan de trabajo que establece en seis pasos la aplicación en la práctica del principio de responsabilidad proactiva a las transferencias de datos: (1) catalogar las transferencias, (2) verificar el instrumento en el que se basa la transferencia, (3) evaluar si hay algo en la legislación o la práctica del tercer país que pueda afectar a la eficacia de las garantías adecuadas de los instrumentos de transferencia en los que se basa, (4) determinar y adoptar las medidas complementarias necesarias para que el nivel de protección de los datos transferidos se ajuste a la norma de equivalencia esencial de la Unión Europea, (5) adoptar cualquier fase de procedimiento formal que pueda requerir su medida complementaria, y (6) volver a evaluar el nivel de protección de los datos transferidos a terceros países (Legal Army, (2021).

Finalmente, retomando lo expresado en el proyecto de ley contenido en el Boletín N°11.144-07, y no obstante que la iniciativa incorpora los principios rectores en materia de protección y tratamiento de los datos personales que han sido reconocidos en las directrices de la OCDE y en el derecho comparado (licitud del tratamiento, finalidad, proporcionalidad, calidad, seguridad, responsabilidad e información), en sintonía con lo estipulado en el artículo 3 de GDPR (Bauzá, 2019, p. 126), insistimos en la necesidad de desarrollar un trabajo que mida los efectos del carácter transnacional del GDPR en su relación con el tratamiento de la información personal en el escenario interno, pretensión en la que el examen de las "Directrices" y las "Recomendaciones" abordadas en la parte final de la presente investigación adquieren relevancia.

Conclusiones

Desde la perspectiva chilena, se ha venido reconociendo la insuficiencia del tratamiento normativo de la protección de los datos de carácter personal. Superar esta falencia adquiere la mayor relevancia, previendo los efectos extraterritoriales en el marco de aplicación del GDPR, en relación con la tutela de la información personal en el ámbito interno. En el actual contexto de discusión sobre la necesidad de implementar la regulación europea como un estándar más completo que la legislación interna, se observa una ausencia de trabajos especializados en el carácter transnacional del GDPR y sus potenciales efectos en el tratamiento de la información personal en diversas áreas: la esfera normativa, frente a la exigencia de modernización de la legislación interna; la esfera social, por ejemplo, en relación con las amenazas a la privacidad originadas con el auge de las redes sociales; y la esfera económica, como ocurre con el necesario establecimiento de los alcances del AAE Chile-UE en el ámbito de los datos personales.

En este orden de ideas, nuestra propuesta apunta al desarrollo de una investigación que aborde puntualmente los efectos de la vocación de extraterritorialidad del GDPR, en relación con la tutela de la información personal en el contexto nacional, trabajo cuyos resultados tendrán un impacto en los ámbitos normativo, social y económico descritos. El producto de la investigación entonces, será de utilidad tanto para las autoridades del Estado (incluyendo legisladores y demás funcionarios), como para los investigadores y académicos chilenos y extranjeros, y al público en general.

Finalmente, y desde el punto de vista de su sistematización, el estudio abordado exige el desarrollo de diferentes pasos, que transcurren en las siguientes etapas (las cuales pueden ser identificadas como los objetivos específicos de la investigación):

1. Identificación de las falencias que puedan generar un impacto (jurídico, social o económico) en la protección de los datos personales, al momento de hacer efectivo el carácter extraterritorial del GDPR.

[25] Artículo 44, GDPR.

2. Identificación de la tendencia jurisprudencial chilena, vinculada a casos que involucren la vocación de eficacia transfronteriza del GDPR y el tratamiento de la información personal.

3. Identificación de la tendencia doctrinal chilena, respecto a la opinión sobre casos que involucren la vocación de eficacia transfronteriza del GDPR y el tratamiento de la información personal.

4. Identificación de las ventajas, fallas y temas pendientes del Proyecto de ley contenido en el Boletín N°11.144-07, respecto al cumplimiento de los estándares establecidos por el GDPR.

5. Identificación de la tendencia doctrinal de la Unión Europea vinculada a los alcances de las normas del GDPR que determinan su vocación extraterritorial, en asocio con el estudio de los instrumentos más recientes formulados por la institucionalidad de la Unión Europea con miras al perfeccionamiento de dicha vocación.

6. Identificación de la tendencia de la jurisprudencia comunitaria, vinculada a los alcances de las normas del GDPR que determinan su vocación extraterritorial.

Referencias

Anguita, P. (2007). *La protección de datos personales y el derecho a la vida privada*, *régimen jurídico*, *jurisprudencia y derecho comparado.* Santiago, Editorial Jurídica de Chile.

Álvarez, D. (2016). Acceso a la información pública y protección de datos personales. ¿Puede el Consejo para la Transparencia ser la autoridad de control en materia de protección de datos? Revista de Derecho. 23 (1), 51-79.

Álvarez, D. (2020). La protección de datos personales en contextos de pandemia y la constitucionalización del derecho a la autodeterminación informativa (Editorial). Revista Chilena de Derecho y Tecnología. 9 (1), 1-4.

Baldoni, P. y otros (2013). *Legitimate interest of the data controller: New data protection paradigm: legitimacy grounded on appropriate protection. International Data Privacy Law.* 3, 244-261.

Bauzá, F. (2019). El modelo europeo de protección de datos. Experiencias para la regulación chilena presente y futura. Ars Boni et Aequi. 15 (1), 121-148.

Brian, A. (2018), La protección de datos personales en América Latina: entre la Unión Europea y los Estados Unidos de Norteamérica, ponencia dentro del "Seminario Internacional de Protección de Datos Personales 2018 en conmemoración del Día Internacional de Protección de Datos Personales del INFODF". México D.F., 26 de enero de 2018. Obtenido en http://www.infodf.org.mx/seminariodatos2018/presentaciones/Ana_Brian.pdf. Consultado el 20 de junio del 2021.

Burgueño, P. Clasificación de redes sociales. Obtenido en: https://www.pablofb.com/2009/03/clasificacion-de-redes-sociales/#:~:text=Redes%20sociales%20Verticales%20De%20Ocio,%2C%20Last.FM%20y%20Moterus. Consultado el 30 de mayo del 2022.

Bustos, S. (2018). Tratamiento de datos personales en el Poder Judicial de Chile: ¿El Gran Hermano jurisdiccional? Revista Chilena de Derecho y Tecnología. 7 (2), 27-44.

Caldevilla, D. (2010). Las Redes Sociales. Tipología, uso y consumo de las redes 2.0 en la sociedad digital actual. Documentación de las Ciencias de la Información. 33, 45-68

Cerda, A. (2011). El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea. Revista de Derecho de la Pontificia Universidad Católica de Valparaíso. 36 (1), 327-356.

Contreras, P. y Trigo, P. (2019). Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile. Revista Chilena de Derecho y Tecnología. 8 (1), 69-106.

Contreras, P. y Trigo, P. (2020). ¿Abriendo la caja de Pandora? El interés legítimo en la reforma a la Ley 19.628 sobre Protección de la Vida Privada. Revista Chilena de Derecho y Tecnología. 9 (1), 185-206.

Ferretti, F. (2014). *Data protection and the legitimate interest of data con-trollers: Much ado about nothing or the winter of rights?* Common Law Market Review. 51 (3) 843-868. Obtenido en http://bit.ly/2WIa1Dy. Consultado el 30 de noviembre 2021.

Fuensanta, D. (2018). Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones. Revista Profesional de la Información. 27 (1), 185-194.

Fundación ESYS (2016). El Reglamento general de protección de datos de la UE: una perspectiva empresarial. 0ctubre. Contenido en https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/63285/38571. Consultado 15 agosto del 2021.

Galves, P. (2019). CBPR y la búsqueda del equilibrio en la protección de datos personales. Obtenido en: https://niubox.legal/cbpr-y-la-busqueda-del-equilibrio-en-la-proteccion-internacional-de-datos-personales/. Consultado el 23 de enero del 2023.

Gómez, A. (2019). *La aplicación extraterritorial del nuevo Reglamento Europeo de Protección De Datos Personales y su incidencia en Colombia.* Tesis Especialización de derecho comercial. Bogotá, Pontificia Universidad Javeriana.

Guasch, V. y Soler, J. (2015). El interés legítimo en la protección de datos. Revista de Derecho UNED. 16, 417-438.

Herrera, P. (2016). El derecho a la vida privada y las redes sociales en Chile. Revista Chilena de Derecho y Tecnología. 5 (1), 87-112.

Jervis, P. (2015). Internet de las cosas y protección de datos personales. Revista Chilena de Derecho y Tecnología 4 (2), 9-51.

Jijena, R. (2001). Sobre la no protección de la intimidad en Chile. Análisis de la Ley 19.628, de agosto de 1999. Revista Electrónica de Derecho Informático, 39, 1-27.

Jijena, R. (2009). *Tratamiento de datos personales al interior de la Administración del Estado como restricción a la Ley 20.285 sobre Transparencia y acceso a la información de los Servicios Públicos*, informe en Derecho elaborado a petición del Consejo para la Transparencia en diciembre del 2009, texto no publicado.

Kraus, P. y Sanz, F., (2018). Conclusiones de la Conferencia "Protección de datos: cuando el derecho enfrenta problemas tecnológicos", celebrada por la Escuela de Derecho y Escuela de Ingeniería Informática de la Pontificia Universidad Católica de Valparaíso. Santiago de Chile, 12 de septiembre del 2018.

Legal Army (2021): Publicadas las Recomendaciones sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales. Obtenido en: https://www.legalarmy.net/publicadas-las-recomendaciones-sobre-medidas-que-complementan-los-instrumentos-de-transferencia-para-garantizar-el-cumplimiento-del-nivel-de-proteccion-de-los-datos-personales/. Consultado el 24 de enero del 2022.

Lluch, P. (2020). Más vale prevenir que curar: GDPR y reforma a la protección de datos en Chile. Revista Gerencia. Primera quincena, septiembre, 2020, 1-58.

Milanés, V. (2017). Desafíos en el debate de la protección de datos para Latinoamérica. Revista Transparencia & Sociedad del Consejo para la Transparencia, (5), 13-31.

Oficina de Información científica y Tecnológica para el Congreso de la Unión (2019). El flujo transfronterizo de datos. Informe 003 octubre. México. Obtenido en https://foroconsultivo.org.mx/INCyTU/documentos/informes/INCYTU_19-003.pdf. Consultado el 10 de junio del 2022.

Ortega, A. y Gonzalo, J. (2018). Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea. Revista de la Facultad de Derecho. 44 (1), 1-35.

Power Data (2018). GDPR: Lo que debes saber sobre el reglamento general de protección de datos. Obtenido en https://www.powerdata.es/gdpr-proteccion-datos. Consultado el 10 de agosto del 2021.

Sanz, F. (2017). Grado de equivalencia entre la protección de los datos personales y el derecho de acceso a la información pública. Revista de Derecho de la Pontificia Universidad Católica de Valparaíso, 48 (1), 135 – 163.

Swire, P. y Litan, R. (1998). *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive.* Washington, D.C., The Brookings Institution.

Universidad Central. Diálogos Unión Europea - Chile: La dimensión digital de los derechos fundamentales. Miércoles 9 de marzo del 2022. Obtenido en https://www.youtube.com/watch?v=MLQ5ZhvzrEk. Consultado el 20 de mayo del 2022.

Vergara, M. (2017). 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. Revista Chilena de Derecho y Tecnología. 6 (2), 135-152.

Wilhelmy, M. (2010). La trayectoria de Chile frente a la región Asia-Pacífico. Estudios Internacionales, 167, 125-141.

NORMAS JURÍDICAS

Unión Europea

Directiva 95/46/CE del Parlamento Europeo y del Consejo.

General Data Protection Regulation UE (2016).

Directrices 3/2018 relativas al ámbito territorial del GDPR (artículo 3), Versión 2.1.

Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE, Versión 2.0".

América Latina

Ley 25.326 de Protección de los Datos Personales de 2000 (Argentina).

Ley 29.733 de Protección de Datos Personales de 2011 (Perú).

Ley General de Protección de Datos Personales de 2018 (Brasil).

Chile

Constitution Política de Chile

Ley 19.628 de 1999

Ley 19.812 de 2002

Ley 20.463 de 2010

Ley 20.521 de 2011

Ley 20.575 de 2012

Ley 20.886 de 2015

Ley 21.096 de 2018