Internet y la importancia de un órgano de control para la protección de datos personales

Internet and the importance of a control body for the protection of personal data

Fecha recepción: octubre 2019 / fecha aceptación: diciembre 2019

Emilio Oñate Vera[1]

Resumen

Internet constituye una plataforma virtual que permite interconectar a las personas desde distintas partes del mundo, que ha cambiado las formas de interactuar y comunicarse entre sí, incorporando datos personales que se alojan en la red, dando paso a una sociedad digital. El objetivo de este artículo es contribuir al análisis acerca de las adaptaciones e innovaciones normativas que son necesarias para conjugar la privacidad personal y el acceso público a la información, cautelando de manera equilibrada los derechos involucrados en cada una de estas esferas.

Este artículo revisa distintos mecanismos utilizados para resguardar estos derechos y los órganos de control que se requerirían en Chile para proteger los datos sensibles de los usuarios de la web, atendiendo a sus ventajas y desventajas.

Palabras claves: Internet, redes sociales, protección de datos, órganos de control

Abstract

The Internet is a virtual platform that allows people to be interconnected from different parts of the world, which has changed the ways of how people interact and communicate between each other, incorporating personal data that are hosted on the network creating to a digital society, The aim of this article is to contribute to the analysis about the adaptations and regulatory innovations that are necessary to combine personal privacy and public access to information, while protecting in a balanced way the rights involved in each of these areas.

This paper reviews different mechanisms used to protect these rights and the control bodies that would be required in Chile to protect sensitive data of web users, taking into account their advantages and disadvantages.

Keywords: Internet, social networks, data protection, control body

1 Profesor de Derecho Administrativo Carrera de Derecho de la Universidad Central de Chile; Decano de la Facultad de Derecho y Humanidades de la Universidad Central de Chile; Abogado Licenciado en Ciencias Jurídicas y Sociales de la Universidad Central de Chile; Magister en Gerencia y Políticas Públicas de la Universidad Adolfo Ibáñez; Magister en Derecho Administrativo de la Pontificia Universidad Católica de Valparaíso. Dirección postal: Lord Cochrane 417, CP: 7940460, Santiago, CHILE.. Email: emilio.onate@ucentral.cl

Introducción

Resulta indiscutible la reconfiguración que Internet ha producido en la interacción de los seres humanos, ya que si en antaño las relaciones humanas se desarrollaban de manera principalmente presencial, en la actualidad la comunicación es concretada por medio de las redes sociales virtuales.

En efecto, Internet no solo ha transformado de manera sideral la forma de trabajar, de estudiar, de hacer negocios, transferir dinero, hacer trámites de distinto tipo, sino también ha cambiado la forma de relacionarnos y comunicarnos. Utilizando Internet como plataforma, surge la *World Wide Web* (WWW) o red informática mundial que es un sistema de distribución de documentos de *hipertexto* o *hipermedia* interconectados y accesibles a través de *Internet*. Con un *navegador web*, un usuario visualiza *sitios web* compuestos de *páginas web* que pueden contener *textos, imágenes, vídeos* u *otros contenidos multimedia*, y navega a través de esas páginas usando *hiperenlaces*. La Web se desarrolló entre marzo del año *1989* y diciembre del año *1990*, por el *inglés Tim Berners-Lee* con la ayuda del *belga Robert Cailliau*, publicando su trabajo en *1992*.

Internet y la Web han permitido el surgimiento y desarrollo de las redes sociales, que para efectos de este trabajo podemos concebirlas como plataformas o aplicaciones virtuales que permiten a sus usuarios conectarse con amigos y familiares o crear relaciones con nuevas personas, grupos o comunidades vinculadas por un interés común, las que son de diversa índole y persiguen diferentes propósitos o fines.

Así, el surgimiento de las redes sociales que genera en los participantes la relación con un grupo determinado de personas, facilitando un sin número de datos personales tales como residencia, preferencias, aficiones, compartir fotografías y videos, permite a dichas redes sociales la configuración de perfiles personales casi exactos de los intervinientes, sin que en la mayorías de los casos sepan que han entregado su consentimiento para ello.

La importancia de la información es irrefutable y dicha información puede utilizarse para fines benéficos o perjudiciales, tanto en el ámbito de la actividad privada o empresarial, como en el ámbito de la administración o actividad pública, lo que le asigna un valor no solo jurídico, que desde luego lo tiene, si no también económico. Así entonces para el derecho, la influencia de Internet y la Web se ha traducido en nuevos enfoques y especializaciones como el derecho de las nuevas tecnologías o el derecho informático o digital, sin embargo, si bien el derecho ha ido incorporando algunos aspectos que dan cuenta de esta nueva realidad virtual, aún hay mucho camino por recorrer, la Ley N° 19.628 del año 1999 sobre protección a la vida privada es un claro ejemplo de que el derecho camina después de los avances tecnológicos.

Internet plantea varios desafíos que en el contexto nacional muestran el déficit que tenemos para regular adecuadamente los datos personales que circulan, su uso y privacidad, y lo que es el foco de este trabajo, muestra también la ausencia de una agencia u órgano de control que de manera integral pueda resguardar la información personal que circula en Internet, respetando el derecho de los titulares de dicha información.

El gran desafío de la actualidad es lograr un marco regulador de la privacidad, que consiga un efectivo equilibrio entre los intereses de las empresas, la innovación y el crecimiento, la libertad de expresión e información, con los intereses de los ciudadanos salvaguardando su privacidad y la seguridad nacional. Los avances tecnológicos, tal como señala Alierta (en Pérez. & Badía, 2012) han destruido las barreras históricamente asentadas como la ubicación, la distancia y el acceso presencial, abarcando datos, personas e información.

Este trabajo, que reconoce el desarrollo de Internet, como espacio de comunicación e interacción de las personas para los más variados y diversos fines, se argumenta la necesidad de actualizar la regulación vigente en materia de protección de datos personales y lo que aparece como más trascedente, el establecimiento de una entidad u órgano de control que regule esta materia y que resguarde adecuadamente el derecho a la protección de datos personales.

Al respecto, resulta necesario indicar que para la doctrina y la jurisprudencia la protección de los datos personales constituyen un derecho de tercera generación. que trascienden el solo derecho a la intimidad, tal como lo expresa Del Castillo (2007)

> No se trataría entonces del "puro derecho a ser dejado solo, en la formulación decimonónica del derecho a la intimidad ("the right to bel et alone"), sino del derecho a la autoderminación informativa, esto es, el derecho de las personas a controlar sus datos personales, incluso si estos no se refieren a su intimidad (Pág, 214).

Internet y los derechos de las personas

Resulta indiscutible que Internet permite que tanto información y datos circulen en el universo virtual de la web, por diferentes páginas, redes sociales o que incluso dicha información y datos queden almacenados en los denominados motores de búsqueda a los que es posible llegar por los usuarios de las mismas, generando publicidad y accesibilidad.

De hecho, cualquier persona con conectividad a Internet puede también acceder a una gran variedad de sitios, que no son más que diferentes vías de comunicación y también de publicidad, expresión de aquello son los correos electrónicos, páginas web

y redes sociales. Esta verdadera realidad virtual trae múltiples beneficios pero también exige nuevas regulaciones.

Desde lo positivo es fácil inferir que la Internet y la Web reducen los costos de recolección, procesamiento y conservación de los datos y son expresión también del avance tecnológico como el fenómeno del cloud computing[2] o computación en la nube, que posibilita el almacenamiento de datos y su deslocalización.

De igual forma esta virtualidad multiplica las oportunidades de recopilar datos, elaborar perfiles de los usuarios, personalizar la publicidad y promoción en la red, permitiendo también a sus usuarios el acceso a un listado de información de manera automatizada, instantánea y continuada en el tiempo, sin que la información caiga en el olvido, constituyendo una verdadera "memoria digital eterna", pudiendo compartirse además en tiempo real, haciendo uso licito de ella.

Internet desde sus orígenes ha sido concebido como una red abierta, que permite la interconexión y la globalización de la información , teniendo acceso desde cualquier lugar en que se esté conectado, lo que evidentemente supone un riesgo para la privacidad de las personas, contribuyendo a afectar sus derechos, por lo que resulta indispensable en el espacio digital respetar la vida privada y familiar, la libertad de conciencia y religión, así como la libertad de expresión e información, en definitiva la protección de datos de carácter personal. Toda esta información según López Portas, estaría afecta a un nuevo tipo de control social digital que deberá enfrentar a lo menos tres problemas

> En primer lugar, la manipulación en el escrutinio y datos disponibles por los usuarios; en segundo lugar, el hecho de que los ciudadanos son fuente y destino de la información disponible en la red; y, en tercer lugar, las dificultades para establecer algún tipo de censura sobre la actividad informativa desarrollada en la web pues los parámetros de espacio y tiempo se difuminan en la misma (2015, pág.272*)*.

La Internet, la globalización y la vertiginosa evolución tecnológica plantean nuevos retos para la protección de datos, el incremento en el intercambio de datos personales como la mayor difusión que las personas hacen de su información a escala mundial, sumado al creciente intercambio de datos personales entre operadores público y privados, incluidas las personas físicas, las asociaciones y las empresas, requiere mayor transparencia de los operadores económicos así como un mayor control de los datos por parte de los titulares e interesados, además del establecimiento de un marco regulatorio que tutele adecuadamente la privacidad y la vida privada de las personas. Se necesita en definitiva un adecuado equilibrio, por un lado entre el incontenible

2 El cloud computing o servicios en la nube, es un nuevo modelo que ofrece servicios de computación por Internet, posibilitando al usuario acceso a un conjunto de prestaciones o servicios estandarizados, dando así respuesta a las necesidades del respectivo negocio, de forma flexible, pagando solo por el consumo efectuado e incluso gratuitamente en caso de proveedores que se financien mediante publicidad o por organizaciones sin fines de lucro.

y positivo desarrollo de la información, la transferencia de datos y su connotación económica, la expansión de una sociedad conectada que fomente y respete la liberta de expresión e información, así como la transparencia y el acceso a esa información. Y por otro, la protección a la vida privada, a la intimidad y privacidad de las personas, con el desarrollo de un entorno digital seguro que permita un armónico control y que tutele los datos de las personas, para lo que resulta imprescindible el establecimiento de una agencia de control para la protección de datos, más todavía con la reciente incorporación del mismo como una garantía constitucional y en efecto en 2018 se publicó la ley 21.096, que consagra la protección de datos personales como garantía constitucional.

La protección de datos personales

Lo primero a abordar aquí es ¿Qué es la protección de datos personales?, y sin entrar en mayores disquisiciones doctrinarias ni filosóficas, lo cierto es que constituyen un derecho fundamental que se relaciona con otros derechos, especialmente con el de acceso a la información pública. En efecto, si la protección de datos personales ampara la intimidad y la auotoderminación informativa, el acceso a la información pública favorece la transparencia, la probidad y la participación ciudadana.

Al respecto, Mañas (2009), plantea que es la importancia de la transparencia para una sociedad abierta y democrática, sin utilizar la protección de datos como una excusa para enervar el acceso a la información pública, aun cuando una de las excepciones que puede invocarse al ejercer el derecho de acceso, es precisamente la derivada de la protección de datos o de la existencia de información o documentos que afecten la intimidad de las personas, por lo que ni la transparencia ni la protección de datos son absolutos, siendo preciso conseguir un equilibrio entre ambos, en tanto Sanz (2013) , en aras de la adecuada ponderación, estudia el tema tanto desde la privacidad como desde el acceso, vinculando los derechos fundamentales que involucran.

De esta manera, la protección de datos, como todo derecho fundamental requiere tutela y acciones efectivas para su desarrollo, y en esa línea los ordenamientos jurídicos han establecido elementos de garantía, de entre los cuales es posible distinguir tres tipos de mecanismos para promover la plena vigencia de tales derechos.

1. Los primeros se denominan garantías normativas al reconocimiento expreso de los derechos**,** las que se insertan en las constituciones y tienen un desarrollo jurídico en la ley. Es lo que ocurre con las denominadas garantías constitucionales que en el caso chileno están contenidas en el capítulo III de la Carta, artículo 19 numeral primero al veintiséis.

Sobre este punto es pertinente señalar que hasta el año 2018, la protección de datos personales en nuestro sistema constitucional se encontraba subsumida, es

decir era un derecho fundamental implícito en el numeral cuarto del artículo 19 de la Constitución[3]. Luego de cuatro años de tramitación legislativa se publicó en el Diario Oficial el 16 de junio de 2018, la Ley 21.096, que consagro explícitamente la protección de datos personales como una garantía constitucional, quedando finalmente de la siguiente forma:

> El respeto y protección a la vida privada y a la honra de la persona y su familia y asimismo la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley. (Numeral cuarto del art. 19).

De este modo, se elaboró una redacción que incluye la protección de datos personales dentro del numeral cuarto que consagra el derecho a la privacidad y a la honra, que con la expresión "asimismo" antes de establecer un nuevo derecho consigno la existencia de un derecho con autonomía pero amparado por la misma acción que tutela al numeral cuarto, esto es el recurso de protección señalado en el artículo 20 del texto constitucional. La expresión "asimismo", entonces, expresa la intención del constituyente de generar un derecho independiente y diferente a la privacidad y la honra, pero que tendrá la misma protección que dichos derechos, para luego establecer la remisión a la ley de su regulación.

2. Los segundos, para asegurar la vigencia de los derechos son los procedimientos jurídicos específicos. En el caso de Chile, la Ley 19.628 consagra en su art. 16 un procedimiento para que los afectados puedan acudir a tribunales a fin de tutelar sus derechos en relación al tratamiento de sus datos personales, así, quien se vea afectado puede ejercer la acción de habeas data, que es aquella procedente cuando el responsable del banco de datos no se pronuncie sobre la solicitud de información, modificación, cancelación o bloqueo en un plazo de dos días hábiles cuando ésta sea denegada. Con la concurrencia de estos requisitos la persona afectada puede recurrir al tribunal del domicilio del responsable del registro o banco de datos y de acogerse la reclamación se puede aplicar una multa (Violler, 2017).

Este procedimiento, ha resultado engorroso y poco efectivo, primero porque requiere la asesoría letrada, es decir patrocinio de abogado, sumado al bajo valor de la multa que deben pagar los infractores, que en la práctica se traduce en que el incumplimiento a las normas señaladas genera un pago pecuniario que resulta irrisorio para la envergadura de las entidades responsables del registro de datos.

3 El señalado artículo disponía: "La Constitución asegura a todas las personas... 4° El respeto y protección a la vida privada y a la honra de la persona y su familia".

3. Los terceros son los institucionales, mediante la creación de órganos autónomos e independientes cuyo objetivo es velar y promover los derechos y las libertades fundamentales para la protección de datos personales.

Algunas referencias internacionales.

A nivel mundial, es posible encontrar diversas configuraciones normativas, políticas e institucionales.Tal como indica Saarempää (2003), los primeros órganos de control en la protección de datos se originaron en Alemania en 1970, al promulgarse la ley sobre tratamiento de datos personales mediante la cual se pretendía brindar protección a las personas naturales ante la amenaza que representaba el tratamiento informatizado de datos nominativos por las autoridades y administraciones públicas del Estado, los municipios y entidades locales rurales, así como las demás personas jurídicas de derecho público y agrupaciones sujetas a la tutela estatal. A efectos de asegurar su cumplimiento, la ley creaba el Comisario de Protección de Datos, al cual garantizaba independencia para el desempeño de sus funciones, cuáles eran velar por la observancia de los preceptos de la propia ley y cuantos otros hicieren referencia al trato de los datos de los ciudadanos.

Luego, en Suecia se dicta la Data Lag de 1973, conformándose una institución independiente, unipersonal, nombrada por el parlamento, la que estableció un sistema de registro abierto para publicitar los bancos de datos personales relativos a personas físicas realizado por medios automatizados, los que debían ser previamente autorizados para funcionar, asociado a una autoridad de control la Datainspektionen, expresión del Ombusman proyectado al tratamiento de datos que vela por el respeto de la ley, con facultades inspectoras, normativas y procesales para requerir la aplicación judicial de sanciones

Un modelo distinto es el PrivacyAct de 1974 en Estados Unidos, cuya norma dispone que la protección de datos no tendrá una institucionalidad específica u órgano concreto para su tutela, si no que serán los tribunales de justicia los encargados de su defensa. La exposición de motivos de la Privacy Act manifiesta que su objetivo es proteger la privacidad de los individuos identificados en sistemas de información llevados por entes y órganos federales, por excepción alcanza al sector privado, cuando se encuentra vinculado contractualmente al público para el tratamiento de datos por su encargo , mediante la regulación de la captación, conservación, uso y difusión de información por éstos, prescindiendo del soporte en que se contiene, de modo que la ley resulta aplicable sea que las operaciones de tratamiento se realicen por medios informáticos o manuales (Cerda 2003, Nieves, 2011).

Otro enfoque da cuenta de la existencia de un órgano colegiado para la tutela de la protección de datos personales como es el caso de Francia, que prevé un órgano de control, representativo e interpoderes, la Commission Nationale de l'Informatique

et des Libertés, encargado de velar por su aplicación, recibir las reclamaciones de los afectados y dotado de potestad reglamentaria, cuyo ejercicio ha garantizado la perdurabilidad normativa (Cerda 2003).

En el derecho comparado, en España se ha generado debate en relación a la autonomía de la protección de datos como un derecho consagrado en el art. 18.4 de la Constitución Española de 1978, que sigue a la Constitución Portuguesa de 1976, en esta materia, que fue pionera en reconocer el tratamiento informático de datos. En efecto, el derecho al control de la información de uno mismo fue incorporándose en las diferentes legislaciones protectoras de datos, tanto de la primera generación (Alemania y Suecia), como de la segunda (Francia o Luxemburgo), de la tercera (España) como la cuarta (Privacy and Data Bill de 1994, Australia). Sin embargo a nivel constitucional en el ámbito europeo, la pionera en reconocer y constitucionalizar el derecho a la intimidad fue la Constitución Portuguesa de 1976, que en su artículo 35 dice: "Todos los ciudadanos tienen derecho a formar conocimiento de todo aquello que les concierna y se halla en registros informáticos y la finalidad para la cual se destinan las informaciones" (en Álvarez, 2015, pág., 54).

Por otra parte, el Reglamento de la Unión Europea 2016/679 del 27 de abril del año 2016, regula la protección de datos personales y la libre circulación de estos datos, con lo que de conformidad al considerando 2° de su texto, busca contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al esfuerzo y convergencias de las economías dentro del mercado interior, así como al bienestar de las personas físicas (Ortega & Gonzalo, 2018).Según lo dispuesto en el considerando 13° del Reglamento, éste tiene por finalidad, garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior.

De igual forma, busca otorgar seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrecer a las personas físicas de todos los Estados miembros, el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros.

Es interesante constatar que la titularidad del derecho a la protección de datos le es atribuida exclusivamente a las personas naturales o físicas, independientemente de su nacionalidad o lugar de residencia.

Ya la Directiva 95/46 CE antecesora del Reglamento UE 2016/679 establecía la necesidad de crear una entidad encargada de controlar la protección de datos, su artículo 28 obligaba a cada Estado miembro a la creación de una Autoridad de Control y a nivel de la Unión Europea crea el denominado Grupo que tiene carácter consultivo e independiente, siendo su función principal el estudio de las cuestiones relativas a la protección de datos, teniendo competencia para emitir informes y dictámenes asesorando a la Comisión Europea, la que si tiene facultades resolutivas.

El Reglamento 2016/679 deroga la señalada Directiva radicando el control de la protección de datos a la Comisión, al Supervisor Europeo de Protección de Datos y al Comité Europeo de Protección de Datos.

En lo relativo a la Autoridad de Control el artículo 51 del Reglamento dispone:

1. "Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes, en adelante "autoridad de control", supervisar la aplicación del presente Reglamento, 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.
2. Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII[4].
3. Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63[5].
4. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el presente capítulo a más tardar el 25 de mayo de 2018[6] y, sin dilación, cualquier modificación posterior que afecte a dichas disposiciones".

4 Capítulo que hace referencia a la cooperación y coherencia. El artículo 60 dispone en su inciso primro "Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas".

5 El artículo 63 se refiere al, "Mecanismo de coherencia. A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección".

6 Que es la fecha en que entro en vigencia el Reglamento de la Unión Europea (UE) 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.

Por lo expuesto, en definitiva es posible distinguir tres modelos de órganos de control para la protección de datos;

a) Órganos unipersonales; el caso más emblemático es el de España con la Agencia de Protección de Datos[7], que se establece como una autoridad administrativa independiente de ámbito estatal, con personalidad jurídica y plena capacidad pública y privada que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones y que se relaciona con el gobierno a través del Ministerio de Justicia. También se distingue el Comisario Federal de Protección de Datos en Alemania, el candidato es propuesto por el gobierno y requiere la aprobación del parlamento, tiene competencia en todo el país y considerando la estructura descentralizada alemana en las provincias o "Lander" existen órganos con idénticas funciones.

b) Órganos colegiados; en Francia, el artículo 6 de la ley de protección de datos crea la Comisión Nacional de la Información y Libertades, la que está compuesta de 17 miembros, los cuales eligen a su presidente. La integran parlamentarios, magistrados y altos funcionarios tanto del sector público y privado con fuertes incompatibilidades para evitar conflictos de interés. Siguiendo el modelo francés se crea por la ley de protección de datos portuguesa de 1991 la Comisión Nacional de Protección de Datos y un año más tarde por la Ley Orgánica de tratamiento automatizado de datos personales (LORTAD) se crea la Agencia de Protección de Datos.

c) Tribunales ordinarios; la protección de los derechos queda radicada en los tribunales ordinarios y es el Tribunal Supremo en última instancia quien determina la posible vulneración o no de los derechos. El inconveniente de este sistema es que la actuación jurisdiccional es a posteriori, es decir una vez que se ha producido la vulneración del derecho. Eso sí la labor de promoción de la protección de datos queda radicada en el gobierno.

El caso chileno

En Chile , el 28 de agosto de 1999 se publica en el Diario Oficial, la Ley 19.628, para regular la Protección de Datos Personales (en adelante LPDP), es la propia ley, la que en su artículo 1° establece que regulara el "tratamiento de los datos de carácter personal en registros de bancos de datos por organismos públicos o por particulares[8]" y

7 La Ley Orgánica 3/2018, del 5 de diciembre de Protección de datos personales y garantía de los derechos digitales consagra en su Título VII, capítulo I artículos 44 y siguientes a la Agencia de Protección de Datos.

8 Banco de datos, según el art. 2 m es el "conjunto organizado de datos personales, sea automatizado o no y cualquiera sea la forma o modalidad de su creación u organización, que permita relacionar los datos entre sí, así como realizar todo tipo de tratamiento de datos". En definitiva es el dato que se encuentra al interior de un sistema que permite su interacción con otros datos.
Tratamiento, según el art. 2 o es "cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma pública". Es decir la extensión y diversidad verbal expresan que toda utilización que se haga del dato cabe dentro de la noción de tratamiento.

luego en su art. 2° conceptualiza los datos personales como "aquellos relativos a cualquier información concerniente a personas naturales, identificadas o identificables". Es decir, se refiere a información que permita vincular o asociar a ella a una determinada persona. Luego el art. 2 g, se refiere a los datos sensibles, que corresponde a una categoría de datos que requiere mayor protección o tutela y que son los referidos a "Las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual".

La protección de datos personales constituye una derivación del derecho a la protección a la vida privada, que en nuestro ordenamiento jurídico se consagra en el art. 19 numeral 4° de la Constitución que antes de julio de 2018 aseguraba el "respeto y protección a la vida privada y a la honra de la persona y su familia", es así como la ley 19.628 sobre Protección a la vida privada y ley sobre protección de datos de carácter personal

Asimismo, durante la reforma constitucional del año 2005 se analizó la incorporación de la intimidad en remplazo de privacidad, estableciéndose finalmente el concepto de protección a la vida privada (Anguita, 2007).

Lo cierto es que la señalada ley 19.628, requiere una reformulación, no solo por su ya casi más de veinte años de entrada en vigencia o por la reforma constitucional que elevó la categoría de la protección de datos personales a una garantía explicita, si no que fundamentalmente por carecer de una autoridad pública de control que promueva y tutele adecuadamente los derechos de las personas especialmente en lo referido a la enorme cantidad de datos personales que entidades públicas y privadas recogen, procesan y mantienen, sin su necesario e indispensable consentimiento. Esta carencia afecta directamente la aplicación y eficacia de dicha ley para los ciudadanos y por consiguiente los deja en una indefensión.[9]

Surge entonces preguntarse el tipo de órgano de control requerido para Chile, y tal como ya se ha señalado, uno de los principales déficit del sistema de protección de datos (si es que se puede hablar de un "sistema de protección de datos"), es la ausencia de un órgano o autoridad de control en la materia. En la actualidad, se encuentra en el Congreso Nacional en tramitación un proyecto de ley[10] que asigna como autoridad de control para la protección de datos, al Consejo para la Transparencia (CPLT), en las siguientes líneas abordaremos las ventajas y desventajas que existen para que dicha entidad asuma esta tarea.

9 Si bien la ley 20.285 sobre Acceso a la información pública, le otorgó al Consejo para la Transparencia la competencia para verificar el cumplimiento de la ley 19.628 por parte de los órganos de la Administración del Estado no lo hizo respecto de las entidades privadas. Además respecto de los organismos públicos el señalado consejo carece de facultades sancionadoras por lo que el incumplimiento de la Administración no se ha visto amenazado ni ha disminuido.

10 El 5 de agosto la Comisión de Constitución del Senado aprobó la indicación que entrega la protección de los datos personales al Consejo para la Transparencia (CPLT) y lo reconoce como la agencia a cargo de su protección.

El Consejo para la Transparencia surge en el marco de la ley 20.285 sobre Acceso a la Información Pública del año 2008, que en lo sustancial, estableció un procedimiento para que cualquier ciudadano pudiera acceder a información pública, determinó los conceptos de transparencia activa y transparencia pasiva[11] y creo como órgano de control sobre estas materias a una entidad con autonomía legal, que es precisamente el mencionado Consejo. En lo que respecta al tratamiento de datos personales la letra m del art. 33 de la ley 20.285, le asigna competencia al CPLT para "Velar por el adecuado cumplimiento de la ley 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado". Como puede apreciarse la injerencia sobre la protección de datos que realiza el CPLT es muy indirecta y sólo interviene cuando los involucrados en el tratamiento de datos son órganos públicos, ya sea porque la Administración del Estado realiza el tratamiento de datos personales o cuando el requerimiento de acceso a información pública afecta dichos datos, en cualquier caso, no puede sancionar el incumplimiento a las disposiciones de la ley 19.628, ni tampoco promover o tomar un rol activo en la defensa de dicho derecho.

Las ventajas que tendría que el CPLT fuera el órgano de control en materia de protección de datos son variadas. En primer lugar, la experiencia comparada ya da cuenta de agencias o entidades gubernamentales que abordan simultáneamente la función de promover y tutelar el acceso a la información pública y la protección de datos personales, dos casos emblemáticos son el de México[12] y Reino Unido[13], sumado a que autores como Sanz plantean que

> Nos encontramos ante dos bienes jurídicos (tutela de la información de naturaleza personal y derecho de acceso), reconocidos en el ámbito legal y, por ende potencialmente antagónicos, tensión manifestada (entre otros factores) con el gran número de decisiones de amparo emitidas por el Consejo para la Transparencia desde su creación, decisiones originadas dentro del estudio de la relación entre los mencionados bienes jurídicos (2016, pág., 325).

En segundo lugar, durante los diez años de existencia del CPLT, este se ha constituido como un organismo creíble y con capacidad para cumplir su misión y funciones, lo que para algunos hace suponer que con las reestructuraciones institucionales necesarias, sumado a la mayor dotación de recursos humanos y financieros, el abordaje de la protección de datos por este organismo traería buenos resultados, propendiendo al adecuado arbitraje interno entre los conflictos o tensiones entre transparencia y protección de datos personales. Para ello, deberían realizarse sobre el CPLT las

11 La transparencia activa consiste en el deber que tienen los órganos de la Administración del Estado de mantener a disposición permanente del público, a través de sus sitios electrónicos, toda información relevante, como su estructura orgánica, funciones, actos y contratos que ejecuta y celebra entre otra información a la que se hace referencia en el art. 7° de la ley 20.285. A su vez la transparencia pasiva consiste en el derecho que le asiste a toda persona de requerir información de los órganos de la Administración del Estado respecto de la actividad o función pública que éste desarrolla, a ella se refiere el Artículo 10° de la citada ley cuando señala que "Toda persona tiene derecho a solicitar y recibir información de cualquier órgano de la Administración del Estado, en la forma y condiciones que establece esta ley".

12El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)

13 El Information Commissioner Office (ICO)

adaptaciones a su estructura orgánica, que permitieran dos instancias paralelas, una para el abordaje de la transparencia y el acceso a la información pública y la otra para la protección de los datos personales, con una instancia de resolución que debiera ser la máxima autoridad, ojala colegiada del organismo, resolviendo las controversias que se susciten en esas instancias paralelas. Esto obviamente implica una ampliación en la actual integración del CPLT que deberá ser mixta e igualitaria con expertos en materia de transparencia por un lado y de protección de datos por el otro.

Por último y en tercer lugar, reunir en un solo organismo público ambas funciones, permitiría una gestión más eficiente de los recursos fiscales que se deberían asignar, como se ha dicho mediante la ampliación de competencias de una agencia que ya existe, disminuyendo los costos de instalación, infraestructura y recursos humanos. En este sentido el informe del Centro de Sistemas Públicos de la Universidad de Chile, sobre un modelo organizacional del Consejo de Transparencia en su nueva función de protección de datos, señala:

> Al tratarse de una única institución la que vela por los derechos de acceso a información pública y protección de datos personales, existe un ahorro de recursos al tener funciones que, en caso de estar en instituciones separadas, debieran duplicarse. Típicamente los procesos más estratégicos y transversales pueden tener economías de ámbito al estar radicados en una misma institución, y por ende reducir el costo país de introducir la función de protección de datos (2010, pág. 111).

De lo expuesto, la asignación de competencias en materia de protección de datos al CPLT, podría implicar un mejor resguardo de dicho derecho, que al igual que el acceso y la transparencia tiene que ver con la regulación de la información desde distintas perspectivas, replicando así la experiencia de países como el Reino Unido que concentran en un misma entidad la tutela de ambos derechos; además de permitir un mejor arbitraje entre las tenciones que se produzcan entre la protección de datos y la transparencia en la información pública; así como una asignación y utilización más eficiente de los recursos que se requieran para ello.

¿Qué desventajas tendría que el CPLT fuera el órgano de control en materia de protección de datos?

El cuestionamiento anterior, podría ser reformularlo, señalando ¿porque es necesaria la creación de una nueva agencia de protección de datos para Chile?, en este punto se estima que la misión o si se quiere el sentido que guía la protección de datos es diametralmente distinto al acceso a la información pública, tal como lo sostiene Jijena (2013) y que Álvarez replica de la siguiente manera:

> Por una parte los principios que inspiran los sistemas jurídicos que fomentan la transparencia y el acceso a la información pública tienen orígenes y focos que serían contradictorios con la idea de privacidad que esta detrás de los regímenes de protección de datos personales. Si bien ambos sistemas se basan en información (que puede o no ser información personal), unos propugnan la máxima apertura y transparencia posible, en tanto que los otros, abogan por su circulación restringida (2016, pág. 59).

En definitiva, se requiere un cambio no solo organizacional sino también de visión y misión, lo que además estaría sustentado en la abrumadora mayoría de países integrantes tanto de la Unión Europea como de la OCDE, que cuentan con entidades de control o agencias gubernamentales que solo abordan la protección de datos personales y no ejercen ni regulan conjuntamente esa protección con el acceso a la información pública (Vergara, 2018), en efecto existe un claro predomino de sistemas unifuncionales, con órganos de control encargados exclusivamente de la función de protección de datos personales o de la privacidad (en el caso de la UE; Austria, España, Irlanda, Portugal, Bélgica, Eslovaquia, Italia, República Checa, Bulgaria, Finlandia, Latvia, Rumania, Croacia, Francia, Lituania, Suecia, Chipre, Grecia, Polonia, Dinamarca, Holanda y Luxemburgo. Y en el caso de los países que integran la OCDE, excluidos Chile y EE.UU que no tienen una agencia de protección de datos propiamente tal, encontramos a; Austria, Finlandia, Italia, Polonia, Bélgica, Francia, Letonia, Portugal, Canadá, Grecia, Lituania, Rep. Checa, Corea, Holanda, Luxemburgo, Rep. Eslovaca, Dinamarca, Irlanda, Japón, Suecia, Eslovenia, Islandia, Noruega, Turquía, España, Israel y Nueva Zelanda).

A lo anterior hay que agregar que la jurisprudencia del CPLT, muestra una clara tendencia a favor del acceso a la información pública sobre la reserva o protección de datos personales. Estudios de Expansiva – UDP, ya en el año 2011 mostraban que solo una cuarta parte de las decisiones de fondo dictadas por el Consejo en un trimestre determinado tenían relación con la protección de datos personales. Lo que aparece como bastante posible si como se ha dicho la misión de este organismo es promover y tutelar el acceso a la información pública y solo de manera residual abordar, de conformidad a la letra m del art. 33 de la ley 20.285, la protección de datos personales.

Desde la perspectiva funcional tampoco parece adecuado concentrar las dos funciones, de promover el acceso a la información pública y la protección de datos personales, en un mismo organismo, y que sea la misma entidad la que dirima, por cuanto la ponderación de que debe primar es inaplicable en un mismo organismo, o incluso más ¿podría el propio CPLT resolver contra sí mismo?, eso nos llevaría a que sea otro organismo posiblemente jurisdiccional el que sea quien dirima las controversias que el propio Consejo no pueda resolver, lo que significaría un supuesto que es precisamente el que se quiere evitar, por lo cual se requiere el establecimiento de un órgano público con autonomía e independencia que tenga la estructura, competencia, recursos y capacidad de fiscalización para promover y tutelar la privacidad y autodeterminación informativa, dicho organismo debe tener esa misión y función desde su origen, debe ser concebido y creado con ese propósito.

Por último, diversificar estas funciones públicas y no concentrarlas haría un sistema más abierto y efectivo a la hora de promover y tutelar ambos derechos, especialmente si tenemos en cuenta, que como ya se ha explicado la experiencia del CPLT en materia de protección de datos es residual e indirecta, del Centro de Sistemas Públicos del Departamento de Ingeniería Industrial de la Facultad de Ciencias Física y Matemáticas de la Universidad de Chile, respalda esta postura, al concluir:

> Un segundo aspecto crítico que hace dudar de la conveniencia de que ambas funciones estén en una misma institución es que el "negocio" de la protección de datos es muy distinto al del acceso a la información. Esto se puede ver descrito en una serie de factores como: a. Principios: Ambos tienen orígenes y focos muy distintos e incluso contradictorios. b. Funciones: El negocio de la protección de datos está orientado hacia la seguridad y tratamiento de información con procesos de alta complejidad. Tanto los procesos como los perfiles profesionales que se requieren son muy distintos a lo que puede ser en el acceso a la información donde el foco está hacia la adopción de buenas prácticas en el sector público y no hacia la fiscalización de procesos complejos. c. Mercados: El mercado principal de la protección de datos está en el sector privado. Es en este sector donde se encontrarán los principales detractores del Consejo en su función, donde se tendrá que lidiar con industrias enteras dedicadas a lucrar con la información personal de terceros y donde se presentarán los mayores desafíos a la regulación. El mercado del acceso a la información es el sector público y, los dilemas entre la protección y acceso a la información están orientados a la primacía de un derecho sobre el otro y la construcción de dicha normativa. d. Conflictos de intereses: La institucionalidad ligada al acceso a la información está pensada principalmente en su independencia frente al Poder Ejecutivo. En el caso de la protección de datos los principales conflictos de intereses se darán con el sector privado, por ende se torna mucho más complejo (Pág. 123).

Consideraciones finales

Como se puede apreciar son múltiples las razones que llevan a concluir la inconveniencia de radicar la competencia de la regulación de la protección de datos en el Consejo para la Transparencia, sin embargo, con la misma fuerza y vigor también resulta imprescindible contar con una agencia gubernamental que aborde integralmente esta materia.

Muchos de los que han seguido ese debate plantean que sea el CPLT el que la asuma más por cansancio que por convicción, agotados por años de discusiones, donde frente a la incapacidad actual que muestra la ley 19.628 prefieren tener una agencia de protección de datos a cualquier precio, a que el país se demore otro par de años en obtener una nueva agencia en condiciones de autonomía.

Se estima que si bien ese camino pude ser más corto, finalmente será más costoso para el país y lo que es peor, no asegurará adecuadamente la protección de datos personales frente a las grandes empresas y mundo privado en general, sino que además deslegitimará una entidad que en sus diez años de existencia, como el CPLT, ha dado muestras, como se ha dicho, de credibilidad y eficiencia.

Referencias bibliográficas

Álvarez Caro, M. (2015). *Derecho al Olvido en Internet: el nuevo paradigma de la privacidad en la era digital*. Madrid: Editorial Reus.

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 Universidad católica del Norte, año 23, N° 1, pp. 51-79.

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.

Canales Gil, A. (2004). *La protección de datos personales como derecho fundamental, en anuario de derecho informático* 4 (Montevideo, Fundación de Cultura Universitaria), p.264.

Centro de Sistemas Públicos de la Universidad de Chile (2010) *Diseño de un modelo organizacional del Consejo para la Transparencia en su nueva función de protección de datos*. Santiago de Chile: Universidad de Chile.

Cerda A. (2003) *Autodeterminación informativa y leyes sobre protección de datos. Revista Chilena de Derecho informático*. No. 3 diciembre 2003 pp. 47-75, extraído de: http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_complex/0,1491,SCID%253D14331%2526ISID%253D507,00.html

Del Castillo, C. (2007), *Protección de datos: Cuestiones constitucionales y administrativas*, Madrid: Thomson-Civitas.

Delpiazzo, C, (Coord.) (2009) *Protección de Datos Personales y Acceso a la Información Pública*. Montevideo, Uruguay; Instituto de Derecho Informático.

Jijena, R. (2013). *Tratamiento de datos personales en el Estado y acceso a la información pública*. Revista Chilena de Derecho y Tecnología, vol. 2, N° 2, pp. 49-94.

Ley 21.096, *Consagra el Derecho a Protección de los datos personales.* Diario Oficial de la República de Chile, 16 de junio de 2018.

Ley 19.628, *Sobre Protección de vida privada*. Diario Oficial de la República de Chile. 28 de agosto de 1999.

López Portas, B (2015). *La protección de datos personales en el universo* 3.0: el derecho al olvido en la Unión Europea tras la sentencia del TJUE de 13 de mayo de 2014", Revista Aranzadi de Derecho y Nuevas Tecnologías, número 38, p. 272.

Nieves, M. (2011). El derecho a la privacidad en los Estados Unidos: aproximación diacrónica a los intereses constitucionales en juego. Teoría y Realidad Constitucional, 0(28), 279-312. Doi: https://doi.org/10.5944/trc.28.2011.6960

Ortega Giménez, A., 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), 31-73. https://dx.doi.org/10.22187/rfd2018n44a2

Pérez. J. Badía E. (2012) *El debate sobre la privacidad y seguridad en la red. Regulación y mercados*. Barcelona: Fundación Telefónica, Ariel.

Piñar Mañas, José (2009). *Seguridad, transparencia y protección de datos: El futuro de un necesario e incierto equilibrio*. Madrid. Fundación Alternativas.

Rajevic, E- (2011). *Protección de datos y transparencia en la administración pública chilena: inevitable y deseable ponderación*. En VVAA, Reflexiones sobre el uso y abuso de los datos personales en Chile. Santiago, Expansiva – Ediciones Universidad Diego Portales, pp. 137-158.

Saarenpää, A. (2003) *La protección de los datos personales*. Revista de Derecho Informático. N°3, diciembre 2003.pp 15-29, extraído de: http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_completo/0,1492,SCID%253D14232%2526ISID%253D507,00.html

Sanz Salguero, F. (2013). *Solicitud de acceso a la información y tutela de los datos personales de un tercero*. Revista de Derecho de la Pontificia Universidad Católica de Valparaíso año 41, N° 2, pp. 457-502.

Sanz Salguero, F- (2016). *Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado*. Revista Ius et Paraxis. Año 22, N° 1, pp. 323-376.

Vergara Araya, G. (2018) *Informe Institucionalidad en protección de datos personales: examen de variables regulatorias en el contexto de los proyecto de ley boletines* 11.144-07 y 11.092-07 (refundidos)", pp. 5-10.

Violler, P. (2017). *El Estado de la Protección de Datos Personales en Chile. Derechos Digitales.* Disponible en: https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf