REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

PRIMER SEMESTRE 2016 VOL. 5 NÚM. 1

FACULTAD DE DERECHO
UNIVERSIDAD DE CHILE
REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista Chilena de Derecho y Tecnología* es una publicación semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile que tiene por objeto difundir en la comunidad jurídica nacional, regional e internacional, el conocimiento científico relevante y necesario para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en las ciencias jurídicas y sociales.

Revista Chilena de Derecho y Tecnología
Rev. chil. derecho tecnol. (en línea)
Centro de Estudios en Derecho Informático
Facultad de Derecho · Universidad de Chile
Pío Nono núm. 1, 4.º piso, Providencia
Santiago de Chile

+56 2 29785263
rchdt@derecho.uchile.cl
http://www.cedi.uchile.cl
http://twitter.com/rchdt

ISSN 0719-2584

Indexada en SciELO Chile, DOAJ y Latindex.

La *Revista Chilena de Derecho y Tecnología* es publicada en formatos electrónicos (pdf, epub y mobi) disponibles para descarga en la página web <http://www.rchdt.uchile.cl/>.

Una guía para la presentación de manuscritos está disponible en el enlace: <http://www.revistas.uchile.cl/index.php/rchdt/about/submissions#authorguidelines>.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO • UNIVERSIDAD DE CHILE
ISSN 0719-2584 • VOL. 5 NÚM. 1 (2016) • PÁGS. 87-112 • DOI 10.5354/0719-2584.2016.41268

El derecho a la vida privada y las redes sociales en Chile

The right to privacy and the social networks in Chile

PALOMA HERRERA CARPINTERO
Abogada, Chile

RESUMEN Este artículo tiene por objeto describir los principales problemas y amenazas que se suscitan en las redes sociales contra la privacidad de los usuarios y de terceros, en el derecho chileno. Para estos efectos, se analiza la Constitución Política de la República y la Ley 19.628 sobre Protección de la Vida Privada, con el afán de verificar si la normativa nacional es aplicada de forma eficiente y eficaz en este tipo de plataformas virtuales. El artículo termina con una serie de recomendaciones dirigidas tanto al legislador como al usuario común de redes sociales con la finalidad de fortalecer y cautelar el sistema jurídico imperante.

PALABRAS CLAVE Derecho a la vida privada, derecho a la protección de datos personales, redes sociales.

ABSTRACT The following article aims to describe the main problems and threats that raise in the social networks against the users and third parties' privacy, under the Chilean law. For these effects, the Political Constitution of the Republic and the 19.628 law about privacy protection are analyzed, with the purpose to verify if the national normative is applied in an efficient and effective way in this type of virtual platforms. This paper finish making a series of recommendations aimed equally to

both legislator and the common user of social networks with the goal of strengthen and watch over the prevailing legal system.

KEYWORDS Right to privacy, right to the protection of personal data, social networks.

EL DERECHO A LA VIDA PRIVADA

Desde tiempos inmemoriales el ser humano comprendió la trascendencia de mantener ciertas áreas de su vida ajena a la intromisión de terceros, pues sólo de esta forma puede desarrollar libremente su personalidad. Sin embargo, con el transcurso del tiempo, la protección a la privacidad[1] no ha sido una tarea sencilla.

El derecho a la vida privada, el cual tiene su fundamento en la dignidad inherente a todo ser humano, es considerado un derecho de difícil definición y delimitación debido al carácter relativo que le caracteriza, pues es una noción que muta con el transcurso del tiempo y es distinta en cada sociedad y cultura.[2] En efecto, si bien este derecho en sus inicios estaba únicamente asociado a una perspectiva negativa de exclusión, proyectada en «el derecho a ser dejado solo» (Cooley, 1879: 29),[3] hoy

1. Para efectos prácticos, en el presente artículo se utilizarán los vocablos *privacidad*, *vida privada* e *intimidad* como equivalentes jurídicos. Para una correcta comprensión del derecho a vida privada, véase Novoa (1979).

2. Novoa señala: «La noción general de vida privada queda determinada, en cierta medida, por los diferentes regímenes sociales, políticos y económicos que existen en el mundo. Éstos responden a concepciones diversas del hombre y de la sociedad y se basan en modelos ideológicos discrepantes, que conducen a una apreciación diversa de lo que han de ser las relaciones de un ser humano con otro y de lo que deben ser las relaciones del individuo con la sociedad» (1979: 43).

3. La consolidación de la privacidad como derecho tiene su origen en el artículo «The right of privacy» publicado por los abogados Samuel Warren y Louis Brandeis en 1890. El ensayo aborda la problemática de los medios de comunicación y las intromisiones que estos hacen en la vida privada de las personas. Los abogados para efectos de dar a entender la noción de *privacy*, acuñaron la frase del juez Thomas Cooley: «*The right to be alone*». Si bien el juez Cooley utilizaba dicha locución para definir el derecho individual de toda persona a repeler las intromisiones a su domicilio y documentos privado por parte del gobierno y público en general, Warren y Brandeis otorgaron un

en día ha adquirido relevancia su perspectiva positiva, la cual dota a las personas de una prerrogativa de control que se traduce en «la posibilidad de que los ciudadanos titulares y propietarios de los datos que les conciernen controlen el uso y eventual abuso de los antecedentes que a su respecto sean recopilados, procesados, almacenados y cruzados computacional y telemáticamente» (Jijena, 1992: 40).

Así, ante la relatividad que caracteriza a este derecho, otorgar un concepto de vida privada absoluto con límites y contenidos inmutables es imposible. La doctrina y la jurisprudencia tienen, por lo tanto, la difícil tarea de esclarecer, por una parte, cuándo una situación transgrede la privacidad de un individuo y, por otra, cuáles son los límites de lo público y lo privado.

El paradigma de lo público y de lo privado ha sido algo complejo de definir, debido a que son territorios que se interpenetran, espacios cambiantes en cada momento y situación, hasta el punto que una misma acción puede considerarse pública, privada o íntima con sólo variar el cómo y el dónde se realiza (Martínez, 2007). Así, en el siglo pasado era impensable considerar que las personas podían tener derecho a la privacidad en la vía pública, pues en aquella época se protegía la inviolabilidad del hogar y de las comunicaciones, más por un sentido de propiedad que de proteger la dignidad del ser humano proyectada en el derecho a la vida privada.

A mayor abundamiento, con el progreso de las nuevas tecnologías de la información y comunicación, la complejidad de delimitar lo público de lo privado se ve acrecentado, debido a la inmediatez e interconectividad del mundo actual. En consecuencia, los esfuerzos por parte de la doctrina y la jurisprudencia debiesen estar dirigidos al reconocimiento de criterios objetivos que permitan dar a conocer la expectativa de privacidad que tienen todas las personas, incluso en lugares considerados públicos. En efecto, como señala Novoa (1979), no todo lo que se dice en un espacio público es de contenido público; así las conversaciones personalizadas son privadas por ser consideradas una manifestación de un pensamiento que generalmente está dirigido a un destinatario deter-

---

significado nuevo a dicha frase, al definir *privacy* como «el derecho del individuo a determinar, ordinariamente, en qué medida sus pensamientos, sentimientos y emociones deben ser comunicados a otros» (Warren y Brandeis, 1890: 198).

minado, criterio que ha sido reconocido por nuestro Tribunal Constitucional[4] y el cual debe ser aplicado y respetado en el ámbito de las redes sociales.

NORMATIVA NACIONAL

El derecho a la vida privada está reconocido en diversos pactos internacionales[5] suscritos y ratificados por Chile, constando su consagración explícita en el artículo 19 núms. 4 y 5 de la Constitución Política de la República de 1980 y en la Ley 19.628 sobre Protección de la Vida Privada de 1999.

Mientras el artículo 19 núm. 4[6] de la Carta Fundamental reconoce a todas las personas «el respeto y derecho a la protección a la vida privada», el núm. 5 del mismo artículo asegura «la inviolabilidad del hogar y de toda forma de comunicación privada. El hogar sólo puede allanarse y las comunicaciones y documentos privados interceptarse, abrirse o registrarse en los casos y formas determinados por la ley». Sin embargo, no basta con la consagración explícita a nivel de garantía constitucional de este derecho, si no se establecen mecanismos efectivos que aseguren el respeto y protección de la privacidad en general.

A nivel constitucional, es la acción de protección reconocida en el

4. El Tribunal Constitucional acoge la doctrina de Novoa al reconocer la existencia de una expectativa de privacidad en los espacios públicos, señalando: «Que la intimidad no sólo puede darse en los lugares más recónditos, sino que también se extiende, en algunas circunstancias, a determinados espacios públicos donde se ejecutan específicos actos con la inequívoca voluntad de sustraerlos a la observación ajena». Para una acertada comprensión, véase la Sentencia del Tribunal Constitucional rol 1984-2011, y en especial su considerando vigésimo tercero.

5. Entre ellos encontramos la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos.

6. El Boletín 9384-2007, que está en tramitación, pretende incorporar al numeral 4 del artículo 19 de la Constitución Política de la República, el reconocimiento del derecho a la protección de datos personales, en los siguientes términos: «Asimismo, la protección de sus datos personales, el derecho a acceder a ellos y a obtener, en la forma que determine la ley, su rectificación, complementación y cancelación, si estos fueren erróneos o afectaren sus derechos. El tratamiento, circulación y traspaso de esos datos deberá realizarse en la forma y condiciones que fije la ley».

artículo 20 de la Constitución, el mecanismo jurídico encargado de resguardar el derecho a la privacidad. Sin embargo, ante la evolución tecnológica y el auge de las redes sociales, esta acción ha perdido eficacia. El ordenamiento jurídico nacional, a diferencia de otros países,[7] no exige, como prerrequisito para impetrarla, el agotamiento de la vía judicial ordinaria. De tal forma, el presunto afectado carece de una oportunidad procesal en la cual pueda exponer, en profundidad, los hechos y pruebas en los que basa su alegación. A mayor abundamiento, el desconocimiento de los alcances jurídicos del derecho a la privacidad por parte de los recurrentes tiene como consecuencia que en aquellos casos donde corresponde alegar la transgresión de alguna de las garantías reconocidas en el artículo 19 núm. 4 y 5 de la Constitución, éstos no las invocan, o si llegasen a hacerlo simplemente hacen referencia al articulado sin entrar en una mayor fundamentación,[8] impidiendo a los Tribunales Superiores de Justicia desarrollar el concepto actual de privacidad en los términos ordenados por el constituyente.[9]

Sin perjuicio de lo anterior, Chile fue el primer país latinoamericano en promulgar una ley sectorial en esta materia. Así, la Ley 19.628 sobre Protección de la Vida Privada[10] (LPVP) es la encargada de proteger y

7. A grandes rasgos, en Europa la mayoría de las legislaciones de protección de datos personales consagra el control jurisdiccional como un mecanismo de *ultima ratio*, para aquellos casos de mayor problemática o en los cuales se persigue algún tipo de responsabilidad civil. Lo anterior debido a que cuentan con mecanismos de control adicionales a la judicatura, destacando la existencia de una autoridad de control independiente y autónoma, que tiene por objeto promover, controlar y fiscalizar el cumplimiento de los principios y derechos reconocidos en materia de privacidad y datos personales.

8. En aquellos conflictos que involucran el uso de las redes sociales, los recurrentes invocan como garantía transgredida el artículo 19 núm. 4, sin especificar si hacen mención al derecho a la vida privada o al derecho a la honra. Y si lo llegasen a hacer, sólo invocan la honra.

9. La Comisión de Estudios de la Nueva Constitución optó por no especificar lo que se debe entender por vida privada a nivel constitucional, pues la consideraba como «un rubro en el cual difícilmente se pueden establecer líneas demasiado precisas desde un punto de vista general y va a tener que ser la jurisprudencia la que vaya sentando, en cierto modo, la doctrina sobre este punto». Para un mayor entendimiento, véase la Historia de la Ley de 1980.

10. Para una mayor profundización de la Ley 19.628, véase la Historia de la Ley

regular el tratamiento de datos de carácter personal. Sin embargo, con el pasar de los años se desvelaron una serie de falencias en la presente normativa (cf. Arrieta, 2009), llegando a ser considerado Chile, por parte de la comunidad internacional, como un país que no cumple con un estándar adecuado de privacidad, en razón de las siguientes consideraciones:

- La inexistencia de una autoridad de control, imparcial e independiente, dotada de facultades de oficio y técnicas en la resolución de conflictos surgidos en materia de privacidad y protección de datos personales (cf. Cerda, 2003).
- Falta de un registro de banco de datos privados. Lo cual tiene como principal consecuencia la imposibilidad del correcto ejercicio de los derechos de acceso, rectificación, cancelación y oposición[11] por parte del interesado.
- Sanciones y multas de baja cuantía y hasta irrisorias.[12]

Por estas consideraciones, y ante la disparidad normativa existente a nivel sudamericano, Chile se ha visto impedido de desarrollar criterios que permitan la adecuación de la Ley 19.628 en el ámbito de las redes sociales. Como señala Arrieta:

> La ley permite e incentiva, en abierta contradicción con su espíritu, ciertas estrategias que posibilitan la vulneración de los derechos supuestamente amparados por la misma, sin considerar sanciones para los responsables del tratamiento de datos personales que infringen la ley;

19.628. Además, es importante señalar que desde el año 2012 está en tramitación la reforma a esta ley, contenida en el Boletín 8.143-03, la cual tiene por objeto subsanar las principales deficiencias de la actual normativa, adecuando el cuerpo legal a las normas y principios exigidos por la Organización para la Cooperación y el Desarrollo Económicos (OCDE) de la cual Chile es miembro.

11. Mientras que los derechos de acceso, rectificación y cancelación, pueden ser ejercidos por el titular en cualquier operación de tratamiento de datos, el derecho de oposición, de acuerdo a lo preceptuado en el artículo 3 de la Ley 19.628, sólo puede ser ejercido cuando la utilización de los datos personales sea con fines de publicidad, investigación de mercado o encuesta de opinión.

12. A modo de ejemplo, en Chile la sanción contra el tratamiento de datos sin consentimiento de su titular configura una infracción grave, mientras que en España está calificada de muy grave y las multas son mayores.

igualmente, la acción judicial prevista para la protección del derecho no cumple estándares de aseguramiento del principio del debido proceso que debe regir en los procedimientos judiciales. A ello se suma que el sistema de información a los ciudadanos es insuficiente y que no se cuenta con una autoridad de control, lo que redunda en que las personas, que diariamente se ven afectadas por la forma en que se tratan sus datos personales, muchas veces abusivamente, tanto por parte de organismos públicos como privados, ni siquiera conocen o dimensionan cuáles son sus derechos ni cómo se ejercen (2009: 21).

LAS REDES SOCIALES

Las redes sociales[13] *online* son definidas por el Grupo de Estudios del artículo 29 del Consejo de Europa como aquellas plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes.[14] La Agencia Española de Protección de Datos (AEPD) las define como «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» (Agencia Española de Protección de Datos e INTECO, 2008: 6).

De ambas definiciones es posible desprender tres elementos que configuran una red social y de los cuales surgen las principales transgresiones hacia la vida privada de las personas:

- Comunicación: Es en razón del deseo de querer comunicarse que el usuario de redes sociales sobreexpone ámbitos de su vida privada con el objeto de acceder y participar en este tipo de plataformas. Así, en estos espacios virtuales las personas se despreocupan e incluso ignoran las dimensiones de sus acciones contra su privacidad y la de terceros.
- Identidad: Los datos personales que conforman nuestra personali-

13. Para una mayor profundización respecto al fenómeno de las redes sociales, véase Caldevilla (2010).

14. Véase el Dictamen del Consejo de Europa 05/2009 sobre redes sociales en línea.

dad son la moneda de cambio para poder ingresar y participar en estos servicios. Si bien no todos los datos concernientes a una persona son de importancia para el derecho a la vida privada, el exceso de contenido vertido en este tipo de plataformas hace posible obtener, mediante la unificación de éstos, una perspectiva general de la personalidad de determinado individuo, la cual claramente está protegida como una proyección de su privacidad.

- Interconectividad: La comunicación en las redes sociales se desarrolla de forma masiva, instantánea y recíproca. Los usuarios son, al mismo tiempo, transmisores y receptores de la información, haciéndolos responsables de los contenidos que comparten y que les comparten, lo cual puede tener implicancias en el ámbito legal. Así, los usuarios pueden llegar a ser considerados como responsables de un registro o banco de datos,[15] en los términos preceptuados en la Ley 19.628, al mismo nivel que un desarrollador de aplicaciones o proveedor de redes sociales. Además, el usuario está obligado a respetar la privacidad y los datos de los demás, no pudiendo, a modo de ejemplo, dar a conocer las comunicaciones vertidas en el sistema de mensajería interna pues para todos los efectos legales son consideradas comunicaciones privadas en los términos estipulados en artículo 19 núm. 5, debido a que, por el hecho de ser dirigidas a usuarios determinados, se infiere la intención de mantener esa comunicación apartada de la observación ajena.

De lo anteriormente expuesto, es posible identificar estos tres elementos en toda red social. Sin embargo, es en las redes sociales catalogadas de comunicación o de ocio,[16] como Facebook, en la cuales se presentan las mayores amenazas y transgresiones a la vida privada de las personas.

Es tan importante el elemento de comunicación en estas plataformas, que el uso del correo electrónico para temas domésticos ha sido des-

15. La Ley 19.628 define, en el artículo 2 letra f), al responsable del registro o banco de datos como «la persona natural o jurídica privada, o al respectivo organismo público, a quien compete las decisiones relacionadas al tratamiento de los datos de carácter personal».

16. Las redes sociales se pueden clasificar en base a los intereses y necesidades de sus usuarios. Así, destacan las redes sociales de información (Youtube), profesionales (Linkedin) y de ocio (Facebook). Para una mayor profundización, véase Gil (2012).

plazado por el uso del mensaje privado, lo que sumado al elemento de interconectividad permite al usuario acceder y compartir gran cantidad de información, unificada en una sola plataforma.

Las acciones que efectúa el usuario en las redes sociales, ya sea para acceder o compartir información, también están protegidas por el ordenamiento jurídico nacional. El artículo 19 núm. 12 de la Constitución Política de la República protege la libertad de emitir opinión y la de informar, mientras que la Ley 19.733 sobre Libertades de Opinión e Información y Ejercicio del Periodismo es la encargada de regular el tratamiento de los datos de carácter personal que se efectúan en el ejercicio de estos derechos. Así, el principal conflicto a nivel jurídico que se presenta en las redes sociales tiene relación con armonizar el resguardo de la privacidad de una persona con el derecho a opinar y a informarse que tienen los demás.

PROBLEMÁTICAS DE LAS REDES SOCIALES

Si bien este artículo no pretende poner en duda los beneficios y contribuciones de las redes sociales en la vida diaria, es trascendental que tanto los proveedores de estos servicios como sus usuarios sean conscientes de las amenazas y transgresiones hacia la privacidad que conlleva su uso. En efecto, si bien la tecnología es neutral, su utilización no lo es (Drummond, 2004: 27). Así, el exceso de información compartida en estos espacios sociales facilita que terceras personas, sean naturales o jurídicas, utilicen dicha información con fines ilícitos.

El peso de las redes sociales en el mercado es proporcional al grado de intimidad que los usuarios revelan en sus conexiones. De tal forma, estos servicios imponen a sus usuarios una serie de obstáculos tanto en el momento de registro, como en la participación y cancelación de la cuenta con el objeto de que viertan la mayor cantidad de sus datos personales. A través de la imposición de políticas de privacidad generales y condiciones de uso abusivas, estas plataformas virtuales buscan por sobre todo exponer al usuario en desmedro de su privacidad, pasando a llevar en la generalidad de los casos la expectativa de privacidad que éstos tienen en la red social.

La expectativa de privacidad[17] del usuario es un elemento esencial que debiese ser considerado por la judicatura al momento de establecer los límites del derecho a la vida privada en los servicios de redes sociales. Para tales efectos, este artículo estima que son tres los elementos a considerar:

- Grado de configuración del perfil.
- Cantidad de contactos.
- Perfil indexado a motores de búsqueda.

A grandes rasgos, la expectativa de privacidad del usuario será mayor en aquellos casos donde opte por comunicarse mediante mensajería privada, su perfil tenga un número reducido de contactos y no esté indexado a un motor de búsqueda, pues son acciones objetivas que demuestran la intencionalidad del usuario de mantener ciertas áreas de su vida excluidas del conocimiento público en general. Lo anterior adquiere mayor relevancia cuando los proveedores de redes sociales establecen una configuración por defecto casi pública de los datos y contenidos compartidos en ellas, lo que obliga a los mismos usuarios a graduar la configuración de privacidad de su perfil mediante la personalización de su cuenta; acciones de difícil realización para usuarios inexpertos, como por ejemplo los menores de edad, los que conforman uno de los grupos de mayor vulnerabilidad en este ámbito.[18]

De lo anteriormente expuesto, es posible vislumbrar lo imperioso que es educar y concientizar a la ciudadanía en temas de privacidad en la red, pues ante la dificultad de exigir a este tipo de servicios un estándar

17. Concepto desarrollado en Estados Unidos y utilizado por la jurisprudencia norteamericana con la finalidad de evaluar los límites de la privacidad en cada caso en concreto. Para mayor información, véase Saldaña (2012).

18. A diferencia de la normativa comparada, nuestra Ley 19.628 no establece un marco normativo especial para los menores de edad. Así, uno de los intentos de reforma de esta ley, contenido en el Boletín 8143-03, con el objeto de adecuar la normativa nacional en concordancia con la experiencia comparada, propuso un apartado especial a la regulación del tratamiento de datos personales de niños y adolescentes, exigiendo como requisito esencial para su tratamiento el consentimiento específico de quien ejerza su cuidado personal.

adecuado de privacidad,[19] es el usuario común quien debe comprender el riesgo que conllevan sus acciones hacia su privacidad y la de terceros.

REGISTRO

El usuario promedio de las redes sociales no tiene conciencia de la naturaleza jurídica de los datos que comparte en el formulario de registro, por tanto, en la generalidad de los casos, ignora los derechos que se le reconocen en la Constitución y en la Ley 19.628 en materia de privacidad y protección de datos personales.

Los servicios de redes sociales no son gratis, pues exigen una prestación recíproca por parte de los usuarios, la cual se traduce en que éstos deben suministrar información de carácter personal en el formulario de registro, como nombre completo,[20] correo electrónico, fecha de nacimiento e incluso número de celular, datos que para todos los efectos de la LPVP son considerados de carácter personal,[21] y, en consecuencia, los servicios de redes sociales son considerados responsables del registro o banco de datos en los términos de la referida ley. Esto les impone una serie de obligaciones a los servicios, como la de respetar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de su titular, el cumplimiento del deber de confidencialidad y, por sobre todo, del principio de finalidad, el cual informa persistentemente el contenido de la Ley 19.628, ya que no sólo tiene cabida al instante de verificarse

19. El estándar adecuado de privacidad, siguiendo a Arrieta, es aquél que concede una efectiva protección a la vida privada de las personas, mediante la articulación de un sistema jurídico coherente y, además, que comprenda la instauración de diversos mecanismos tendientes a tutelar la efectividad del cumplimiento de estas disposiciones legales (Arrieta, 2009: 1-2).

20. Algunos usuarios, con la intención de poder participar en las redes sociales, crean perfiles falsos o bajo un seudónimo con la finalidad de preservar la privacidad de sus datos. Sin embargo, algunas redes sociales, como Facebook, obligan al potencial usuario a entregar datos verídicos, prohibiendo de forma expresa en sus condiciones de uso la creación de cuentas falsas, instando a la comunidad en general a denunciar este tipo de cuentas.

21. La Ley 19.628, en su artículo 2 letra f), define datos de carácter personal como aquellos «relativos a cualquier información concerniente a personas naturales, identificadas o identificables».

la recogida de datos, sino que se extiende a toda operación que recaiga sobre los mismos (Cerda, 2003: 89).

La problemática del consentimiento y las condiciones abusivas

De acuerdo a lo preceptuado en el artículo 4 de la LPVP, los datos personales del usuario de una red social pueden tratarse cuando se cuente con el consentimiento expreso. Si bien la actual normativa no define qué se debe entender por consentimiento,[22] este principio está reconocido implícitamente en todo el articulado, señalando en términos generales que además de ser expreso, éste debe constar por escrito.

La manifestación del consentimiento en las redes sociales difícilmente cumple con los requisitos contenidos en la LPVP. En efecto, a modo de ejemplo, Facebook señala que el contrato de adhesión[23] suscrito entre el usuario y la red social se perfecciona en el momento en que éste hace clic en el botón de registro, aceptando en consecuencia las condiciones y políticas de privacidad de la red. Sin embargo, lo anterior es insuficiente para considerar que el consentimiento fue otorgado de forma expresa y por escrito, menos se entenderá otorgado de forma previa, libre, inequívoca e informada, como pretende estipular la reforma en tramitación en concordancia con la experiencia comparada.

La mayoría de los potenciales usuarios carece de interés por leer las políticas de privacidad y condiciones de uso, debido a que las consideran extensas y de difícil comprensión. El usuario no comprende el objeto, finalidad y plazo por el cual se recolectan y tratan sus datos. A mayor abundamiento, si bien existen personas racionales e informadas que valoran su privacidad, el entendimiento de estas condiciones y políticas no es suficiente. Las entidades que pueden tener acceso a estos datos son innumerables: en general, las personas carecen del tiempo necesario para administrar su privacidad en cada uno de los casos y, por lo tanto,

22. La reforma a la Ley 19.628, contenida en el Boletín 8143-03, sí lo hace, definiendo el consentimiento del titular como «toda manifestación expresa de voluntad efectuada de manera libre, inequívoca e informada, mediante la cual el titular acepta el tratamiento de datos personales que le concierne».

23. Es un contrato de adhesión ya que el contenido de las cláusulas es establecido de forma unilateral por la red social. En consecuencia, el usuario no puede alterar el contenido de las cláusulas, debiendo aceptar la totalidad de éstas.

fiscalizar el cumplimiento de las disposiciones de la Ley 19.628 resulta complejo.

En Facebook, en el momento en que el usuario termina su registro en la red social se le da la opción de completar otros datos adicionales y de contenido íntimo, sin entregar detalles en cuanto a la finalidad de su recolección ni menos señalar el carácter voluntario de su entrega.

Los datos sensibles,[24] de acuerdo al artículo 10 de la LPVP, no se pueden tratar, excepto cuando la ley o su titular consientan en ello. La Ley 19.628 no exige requisitos adicionales para su tratamiento, sin embargo, la reforma en tramitación, contenida en el Boletín 8143-03, en concordancia con la experiencia comparada viene en subsanar este aspecto al exigir que el consentimiento del tratamiento de estos datos deba ser expreso, previo, específico y por escrito. Así, los datos sensibles solicitados por Facebook, como la orientación sexual o ideología política, debiesen contar con un mayor resguardo por parte de la red social, debido al contenido íntimo que pueden develar.[25]

Ante la excesiva cantidad de datos personales y sensibles que pueden solicitar las redes sociales en la etapa de registro, sumado a la ignorancia del usuario promedio respecto a las implicancias que conlleva compartirlos, los ataques informáticos han aumentado con la intención de recabar, de forma maliciosa, esta gran base de datos. Así, entre las principales amenazas que se generan con el uso de las redes sociales está el *phishing*[26] y la suplantación de identidad. En efecto, el *pishing* facilita

24. La Ley 19.628, en el artículo 2 letra g), define datos sensibles como «aquellos datos personales que se refieren 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».

25. La Unión Europea ha señalado en su Dictamen 05/2009 que, si un servicio de red social incluye en el formulario de registro preguntas relativas a datos sensibles, deberá indicar muy claramente que la respuesta a tales preguntas es totalmente voluntaria.

26. El *phishing* consiste en la creación de sitios web falsos con la apariencia de inicio de la red social, los que tienen por objeto inducir por engaño al usuario a registrarse e identificarse en ellas, recabando automáticamente sus datos personales para ser utilizados de forma indebida, ya sea suplantando su identidad, exponiendo su vida privada, o robando información financiera, como el número de tarjeta bancaria, o para confeccionar grandes bases de datos con la finalidad de venderlas a terceros.

el aprovechamiento malicioso de estos datos, debido a que otorga acceso a los datos de identificación de un usuario en la red social. Lo anterior incentiva la generación de otras actividades abusivas y hasta delictivas al interior de estas plataformas. Así, la suplantación de identidad puede conllevar, desde la obtención de información de índole privada del usuario suplantado a través de comunicaciones engañosas que se mantienen con otros usuarios, hasta la obtención de datos de carácter bancario, con el objeto de perpetrar un fraude electrónico a través de los medios de pagos indexados a la red social.

Asimismo, tampoco existe certeza respecto de si los proveedores de estos servicios respetan la privacidad de los datos vertidos por sus usuarios, pues el contrato de adhesión impuesto por la red social al usuario permite la estipulación de políticas de privacidad deficientes y condiciones de uso que no especifican los fines del tratamiento de datos. Esto es una grave amenaza a la privacidad, pues induce a una serie de prácticas abusivas[27] por parte de estas plataformas con la intención de maximizar el uso de los datos recabados que, ante la generalidad de los términos y condiciones, expanden de forma arbitraria los fines para lo que se recopilaron.

PARTICIPACIÓN DEL USUARIO

Con el objeto de interactuar, el usuario comparte gran cantidad de información en estas plataformas, como fotografías, videos, comentarios y hasta su geolocalización. Con ello, sobrexpone de tal forma su vida privada que hace posible la construcción de una verdadera bitácora digital al alcance de un gran número de personas.

Configuración por defecto del perfil

Por regla general, los servicios de redes sociales establecen un grado de configuración casi público de la cuenta por defecto, el que otorga un

27. En Facebook, por ejemplo, un ejemplo de cláusula abusiva es aquella que señala: «Si no cumpliéramos alguna parte de esta Declaración, no se considerará una exención», pues deja en total indefensión al usuario, sin ninguna garantía de exigir a la red social que cumpla con lo preceptuado en sus condiciones de usos y políticas de privacidad. En efecto, si Facebook no cumple alguna de las cláusulas, el contrato no queda invalidado.

amplio acceso al contenido vertido por el usuario en su perfil. Esto tiene como principal consecuencia que mientras mayor sea el número de personas que accedan a ellos, mayores serán las repercusiones que estos datos puedan tener en el ámbito jurídico y, por sobre todo, social.[28]

La información vertida en las redes sociales sin la debida configuración de privacidad, puede ser considerada una fuente de acceso público[29] conforme a la definición contenida en la LPVP y, según los términos generales preceptuados en el artículo 4 del mismo cuerpo legal, no requerirían autorización por parte del titular para su tratamiento. Ciertamente, interpretar en este sentido la normativa nacional ante la realidad que presenta internet y las redes sociales, no es lo más recomendable. En consecuencia, es imperioso que el legislador establezca «un catálogo cerrado de bancos que puedan considerarse fuentes de acceso público a datos personales, de modo tal que la excepción quede limitada y que el consentimiento por parte del titular de los datos mantenga su fuerza de regla general» (Alvarado, 2014: 224).

Aun en aquellos casos en que el usuario controle el acceso a la información de su cuenta, esto no impide la posible viralización del contenido. De tal forma, es el usuario de estos servicios quien debe implementar medidas preventivas para no afectar su privacidad ni la de terceros. Así, en la medida en que se implementen políticas públicas tendientes a concientizar a la ciudadanía en materia y protección de datos, los usuarios serán más cautelosos con el contenido que compartan, evitando además la trasgresión a la privacidad de los demás.

Si un usuario comparte los datos personales de otra persona sin el consentimiento de ésta a través de la red social, el usuario emisor debe asumir la responsabilidad en los términos de la Ley 19.628[30] ante la

28. A modo de ejemplo, los *job hunters* al momento de elegir a un posible candidato para un puesto de trabajo, inspeccionan su perfil de las redes sociales, el que podría mostrar ciertos aspectos personales que podrían descalificar al postulante en el proceso de selección.

29. La Ley 19.628 señala en el artículo 2 letra i, considera que son fuentes accesibles al público: «los registros o recopilaciones de datos personales, públicos o privados, de acceso no restringido o reservado a los solicitantes».

30. La normativa nacional no contempla la excepción de vida privada o exención doméstica, como si lo hace la Unión Europea. A modo de ejemplo, España establece que no se aplicará la normativa relativa a la protección de datos personales en aquellos

persona afectada, sin perjuicio de la acción de protección que el presunto afectado pueda impetrar para el restablecimiento del imperio del derecho.

La LPVP reconoce a toda persona un poder de control sobre sus datos personales, el cual se materializa en el reconocimiento por parte del ordenamiento jurídico de los derechos de acceso, rectificación, cancelación y oposición, los que impone al responsable del registro o banco de datos. Para asegurar el efectivo ejercicio de estos derechos en el ámbito de las redes sociales, los proveedores de estos servicios deben mantener canales de comunicación expeditos con el usuario, debiendo contar con formularios de fácil comprensión, acceso y visibilidad para que los usuarios y terceros interesados puedan ejercer sus derechos. En el caso de los usuarios considerados responsables en los términos de la LPVP, como no se les puede censurar de forma previa —pues esto atentaría contra derecho a opinión e información—, la persona interesada en ejercer alguno de los derechos de acceso, rectificación, cancelación y oposición, puede solicitarle al usuario responsable la eliminación o modificación de un comentario, e incluso la cancelación u oposición, lo que se traduciría en dejar de ser amigos o en el *unfollow* según sea el caso (Rallo y Martínez, 2011).

En aquellos casos donde no se han respetado los derechos de acceso, rectificación, cancelación y oposición, y ante la carencia de una autoridad de control en Chile, ha sido difícil exigir el cumplimiento de la normativa contenida en la LPVP. Además, al ser el *habeas data*[31] un procedimiento totalmente judicializado, al momento de analizar el costo-beneficio las personas deciden no perseverar y prefieren recurrir de protección en aquellos casos de trasgresión grave a sus derechos, colapsando aún más el sistema judicial chileno.

---

ficheros mantenidos por personas naturales en el ejercicio de actividades exclusivamente personales o domésticas.

31. En gran parte de Europa, la expresión *habeas data* hace referencia a un proceso que comprende una etapa administrativa y otra judicial, mientras que en Chile dicho concepto se usa únicamente para referirse a la acción judicial reconocida en el artículo 16 de la Ley 19.628, configurándose «como el instrumento a través del cual los titulares de datos pueden ver protegidos sus derechos frente a acciones que resulten ilegales o arbitrarias o que importen un uso indebido de información de carácter personal que les concierne por parte del responsable del fichero o banco de datos» (Jervis, 2003: 27).

INSTALACIÓN Y USO DE COOKIES

Otra problemática que se presenta en las redes sociales durante la participación del usuario, se origina por el uso de *cookies*.[32] Éstas otorgan al proveedor de redes sociales la posibilidad de manipular la publicidad que los usuarios visualizan en la plataforma a través de un rastreo automático de sus hábitos de navegación, los que son indexados a su Internet Protocol (IP). La IP es un número que identifica o permite identificar un dispositivo conectado a internet perteneciente a un determinado individuo, y es considerado, por estos motivos, como un dato de carácter personal de acuerdo a lo preceptuado en la LPVP. Por lo tanto, se requiere exigir el consentimiento expreso y por escrito del usuario. Sin embargo, en la práctica las redes sociales no respetan estos requisitos debido a los términos generales que estipulan en sus políticas de *cookies*: pasan por encima del principio de finalidad e información, y además no se puede entender manifestado el consentimiento por el simple acto de cliquear un botón.

Siguiendo la teoría del mosaico (Madrid, 1984),[33] cada dato recabado a través de las *cookies* da la posibilidad de revelar la identidad real de las personas, exponiendo datos sensibles del usuario, concernientes a sus gustos, pasatiempos, ideología, entre otros. A modo de ejemplo, Facebook señala en sus condiciones de uso que utiliza *cookies* con el objeto de efectuar análisis y estudios para mejorar sus productos, y compartir estos datos con otras empresas socias de la red social, sin embargo, estas condiciones no especifican el objeto ni el plazo en que estarán activadas estas *cookies*. Lo anterior deja en evidencia que el usuario de redes sociales no sólo tiene que ser consciente del contenido y datos que comparte de forma explícita en las redes sociales, sino que también debe ser cauteloso con otras acciones, las que, en la generalidad de los casos, ignora que también son monitoreadas por estos servicios, como los *likes* de Facebook y Twitter que son monitoreados por *cookies*.

32. Término informático para hacer referencia a la información que guarda un servidor sobre un usuario en su equipo.

33. «Al igual que ocurre con las pequeñas piedras que forman mosaicos, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significados» (Madrid, 1984: 45).

SINCRONIZACIÓN DE APLICACIONES A LAS REDES SOCIALES

Con el auge de los teléfonos inteligentes y ante la necesidad de las personas de estar conectadas en todo momento y lugar, son diversas las aplicaciones[34] que interactúan con este tipo de plataformas mediante la sincronización del perfil del usuario con una aplicación determinada y viceversa. Esto puede generar riesgos adicionales a la vida privada cuando el acceso a la plataforma se realiza a través del teléfono móvil, pues permite a los desarrolladores de aplicaciones y proveedores de estos servicios acceder a información personal contenida en el dispositivo, como la lista de contactos, la geolocalización a través de GPS, los registros de llamadas, entre otros datos. Además, se debe mencionar que no todos los desarrolladores de aplicaciones cuentan con condiciones de usos y políticas de privacidad, o si las tienen, no informan a sus potenciales usuarios de forma clara sobre el tipo de datos personales que recabará la aplicación y su uso posterior. A mayor abundamiento, por lo general las redes sociales señalan que ante la discrepancia de las condiciones de usos, prevalecerán las de la aplicación, lo cual aumenta el peligro de un tratamiento de datos indebido, pues es más complejo fiscalizar varias aplicaciones que una red social. En consecuencia, el derecho al acceso reconocido en el artículo 12 de la LPVP se ve en gran medida restringido, pues si el usuario no conoce quién está tratando sus datos, se ve impedido de ejercer el derecho al acceso y los demás mecanismos de protección establecidos en la ley. Vale recordar que la actual normativa y el proyecto de reforma del Boletín 8143-03, no reconocen potestades de oficio al ordenamiento jurídico para fiscalizar las redes sociales; sólo el presunto afectado tiene la potestad de incoar el *habeas data* o acción de protección, según sea el caso.

Cancelación o eliminación de la cuenta

El derecho de cancelación está reconocido en el artículo 12 de la Ley 19.628, y señala que toda persona tiene derecho a exigir, a quien sea res-

34. El Consejo de Europa en el Dictamen 02/2013, sobre las aplicaciones de los dispositivos inteligentes, define a las aplicaciones como programas informáticos generalmente concebidos para un cometido concreto y dirigido a un determinado conjunto de dispositivos inteligentes.

ponsable de un banco de datos, la eliminación de su información personal en aquellos casos en que su almacenamiento carezca de fundamento legal o estuviese caduca.

En las redes sociales, el derecho de cancelación es el más incoado por los usuarios y terceros. Respecto a sus usuarios, éstos entregan a la red social gran cantidad de datos personales para así ingresar y participar en la plataforma virtual. En consecuencia, desde que el usuario quiere cancelar su cuenta se entiende revocado el consentimiento y, desde ese momento, los tratamientos de los datos obtenidos después de la revocación carecen de finalidad, vulnerando en consecuencia la normativa contenida en la LPVP. Sin embargo, el derecho de cancelación no es cumplido a cabalidad por las redes sociales. En efecto, pese a que el usuario solicita dar de baja el servicio conforme a las condiciones de uso de la red social, es imposible tener certeza respecto a si la cuenta fue cancelada de forma efectiva y eliminados sus datos, pues se han expuestos casos en los cuales los datos de sus usuarios quedan a disposición de las redes sociales y terceros por un tiempo prolongado, tanto en el servidor principal como en los servidores espejos.[35] Esta misma incertidumbre se produce durante la participación del usuario en la red social, pues no se tiene certeza respecto a si el contenido compartido en la plataforma, eliminado después por éste, efectivamente es retirado de la base de datos o no.

Conocido es el caso de Max Schrems,[36] quien al momento de exigir el cumplimiento de su derecho de acceso a Facebook, pudo corroborar

35. Los servidores espejos son una réplica exacta del servidor principal de una red social. Tienen por finalidad respaldar los datos con el objeto de prevenir cualquier pérdida de información que pudiera sufrir el servidor principal.

36. El ciudadano austriaco Max Schrems interpuso una denuncia en Irlanda contra Facebook, por considerar que la empresa no garantizaba la debida seguridad de sus datos. La denuncia de Schrems sirvió de argumento para que el Tribunal Europeo invalidara el acuerdo Safe Harbor, que reconocía a Estados Unidos como un territorio seguro para la intimidad y, en consecuencia, permitía la transferencia internacional de datos sin mayores impedimentos legales. Así, ante la invalidación del Safe Harbor, la Unión Europea y Estados Unidos anunciaron la suscripción de un nuevo acuerdo denominado EU-U.S. Privacy Shield, el cual impone mayores obligaciones a las empresas norteamericanas en la transferencia internacional de datos, en concordancia con lo señalado en la Directiva 95/46/CE. Para un mejor entendimiento, véase Unión Europea (2014) y Parlamento y Consejo Europeo (2016).

que la plataforma también guardaba registro de las conversaciones que habían sido eliminadas por él, lo que carecía de consentimiento y vulneraba su derecho a la privacidad y a la protección de sus datos personales.

La dificultad de ejercer el derecho de cancelación en la red social se ve acrecentada por el hecho de que, en la generalidad de los casos, debido a la configuración pública por defecto impuesta por estas plataformas, los perfiles de los usuarios se encuentran indexados en motores de búsqueda que almacenan en su base interna los datos presuntamente eliminados de las redes sociales. Así, el ciudadano carece de la facultad de que se respete su derecho de cancelación.

RECOMENDACIONES

Ante el problema de poder aplicar la Ley 19.628 en el ámbito de las redes sociales, desarrollamos una serie de recomendaciones dirigidas al usuario de estos servicios y al legislador nacional con el objeto de reforzar la tutela del derecho constitucional a la vida privada en esta era digital.

En primer lugar, es trascendental que Chile implemente una autoridad de control, independiente y especializada en materia de privacidad y protección de datos personales, investida de potestades de fiscalización, coerción y, por sobre todo, prevención, pues la actual legislación ha perdido eficiencia y eficacia en la resolución de conflictos relacionados con el uso de las nuevas tecnologías.

El hecho de que en Chile exista sólo una instancia judicial para asegurar el cumplimiento del derecho a la vida privada y de la Ley 19.628, conlleva a que los presuntos afectados, al analizar el costo-beneficio de comparecer ante los tribunales de justicia, decidan no perseverar en su accionar. A modo de ejemplo, en el ámbito de las redes sociales, una persona puede considerar excesivo tener que recurrir a la judicatura por el solo hecho de que se le ha denegado alguno de los derechos de acceso, rectificación, cancelación y oposición, lo cual tiene como consecuencia la impunidad de los presuntos responsables y, además, el incumplimiento del objetivo central de la referida normativa, que no es otro que garantizar el respeto y protección de la privacidad y los datos personales. Como consecuencia de lo anterior, la creación de una autoridad de control especializada en Chile es imperiosa, pues ante el nuevo escenario que ofrece internet y las redes sociales, el conocimiento técnico y normativo

que manejan este tipo de entidades es trascendental para adecuar la aplicación de la actual normativa en esos ámbitos.

España, país que ha inspirado gran parte de la normativa nacional en materia de privacidad y datos personales, a través de la Agencia Española de Protección de Datos (AEPD), ha tenido la oportunidad de instar a las redes sociales a adecuar sus políticas y condiciones de uso con lo preceptuado en la normativa española.[37] Además, existe un procedimiento prejudicial obligatorio de naturaleza administrativa ante la Agencia, que permite la resolución expedita de las reclamaciones de sus ciudadanos y la imposición de altas multas a los que resulten responsables de un tratamiento indebido de datos. Esto deja la instancia judicial para aquellos casos de mayor complejidad.

En segundo término, y en directa relación con la potestad de prevención que debiese tener esta autoridad de control, ante la dificultad que conlleva al legislador y a la judicatura la aplicación de la normativa en las redes sociales, es primordial educar y concientizar al usuario. El principal objetivo debiese ser concientizar a los menores de edad respecto a la importancia de su privacidad y los peligros que conlleva el uso de las redes sociales.

Es primordial la realización de informes anuales y manuales de educación por parte de la entidad que el Estado decida consolidar como garante en la protección de datos personales de los ciudadanos, los que además permitirían a la doctrina y jurisprudencia a generar criterios acordes a la realidad actual, permitiendo al gobierno conocer los principales desafíos que se deben superar en materia de privacidad y protección de datos. Lo anterior permitiría crear usuarios conscientes de su privacidad y empoderados para exigir el cumplimiento de los derechos de acceso, rectificación, cancelación y oposición en estas plataformas. Esto también ayudaría a disminuir la colisión con otros derechos de igual trascendencia, como el derecho a la libertad de opinión e información reconocido en el artículo 19 núm. 12 de la Constitución Política de la República.

37. Uno de los requerimientos de mayor trascendencia realizado por la AEPD a Facebook tuvo como consecuencia que la red social adecuara la edad mínima de sus usuarios en concordancia con la normativa española. Así, en el resto del mundo la edad mínima para participar en Facebook es de 13 años, mientras que en España es de 14.

CONCLUSIONES

El derecho a la vida privada ha mutado a lo largo del tiempo, tanto a nivel doctrinal como jurisprudencial. Si bien en sus inicios era considerado una emanación del derecho de propiedad, posteriormente con el desarrollo de los derechos humanos, y en específico con el valor de la dignidad, se consagró a nivel fundamental como un derecho autónomo desde una perspectiva negativa, manifestada en el derecho a ser dejado solo.

Ante el progreso de las tecnologías de la información y comunicación, nuevas amenazas surgieron contra la privacidad de las personas y es necesario volver a redefinir el contenido y alcance de este derecho. Como consecuencia de lo anterior, surgió la necesidad de proteger la perspectiva positiva e informada de este derecho, manifestado en el derecho a la protección de datos personales, el cual se concreta en la facultad de control que tiene el titular de los datos personales respecto al tratamiento de éstos.

En Chile, si bien el derecho a la vida privada está consagrado a nivel constitucional, los intentos de sistematización de la jurisprudencia existente en esta materia han sido precarios por parte de la doctrina y la judicatura. Lo anterior se debe, por una parte, a la dificultad de determinar el bien jurídico protegido en el ejercicio de la acción de protección, y, por otra, a la ineficacia del *habeas data*, por ser un procedimiento únicamente judicializado y de extensa duración.

Desde la perspectiva específica del derecho a la protección de datos personales, se han detectado una serie de falencias en la actual normativa contenida en la Ley 19.628, destacando entre ellas la ausencia de una autoridad de control que se encargue de fiscalizar el cumplimiento de esta ley, unas sanciones con bajas multas asociadas, la inexistencia de una obligación de registro de datos de índole privado, la inexistencia de potestades de oficio para poder inspeccionar y fiscalizar el cumplimiento de la ley, entre otras. En consecuencia, la comunidad internacional ha llegado a considerar a Chile como un país que no cumple con un estándar adecuado de privacidad, lo cual se verifica, por una parte, en la inexistencia de una declaración de adecuación de privacidad en concordancia con los estándares exigidos por la Unión Europea en la Directiva 95/46/CE, y, por otra, por la inexistencia de una legislación

que contenga las recomendaciones efectuadas por la OCDE en materia de protección de datos personales.[38]

De lo anterior se colige la imperiosa necesidad por parte de nuestro país de implementar diversas reformas a nivel legislativo con el propósito de proteger la privacidad de los datos en el ámbito de internet, de las redes sociales y de futuras amenazas que surjan con el desarrollo de la tecnología. Para tales efectos, este artículo considera ineludible el reconocimiento explícito a nivel constitucional del derecho a la protección de datos personales, así como la pronta promulgación de alguna iniciativa legislativa tendiente a dar una adecuada protección de los datos personales en Chile, y la consagración efectiva de una autoridad de control que asegure el cumplimiento de esta ley.

Si bien este artículo estima que la alternativa más razonable para una efectiva protección de la privacidad y datos personales en esta era tecnológica es la creación de una Agencia de Protección de Datos, es posible vislumbrar que no es una opción pronta a considerar por el Estado. De tal forma, se espera que la reforma a la Ley 19.628 otorgue verdaderas potestades de oficio, inspección y coerción a la entidad que se implemente para velar por el cumplimiento de esta ley.

Finalmente, como prevención general, este artículo estima que la mejor forma de proteger la privacidad y los datos personales de los ciudadanos en el ámbito de las redes sociales, es educando a la población respecto a sus derechos, y dar a conocer los diversos peligros y consecuencias que conlleva la sobreexposición de su privacidad en estos servicios. Por tanto, la labor de prevención es trascendental, pues permitirá generar ciudadanos cautelosos y responsables en el resguardo de su privacidad. En efecto, si bien las potestades de fiscalización y coerción son importantes, la implementación restrictiva de ambas facultades podría implicar la vulneración del derecho a la libertad de opinión e información, garantía que adquiere trascendencia en el ámbito de las redes sociales, pues proyecta el objetivo por el cual las personas se registran y participan en estos medios, que no es otro que el deseo de comunicarse e informarse a gran escala.

38. Para mayor abundamiento del tema, véase Directiva 95/46/CE (1995) y OCDE (2002).

REFERENCIAS

Agencia Española de Protección de Datos e INTECO (2009). «Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online». Disponible en <http://bit.ly/1Pmgus8>.

Alvarado, Francisco (2014). «Las fuentes de acceso público a datos personales». *Revista Chilena de Derecho y Tecnología,* 3 (2): 205-226.

Arrieta, Raúl (2009). «Chile y la protección de datos personales: compromisos internacionales». En *¿Están en crisis nuestros derechos fundamentales?* Serie de Políticas Públicas (pp. 13-22). Santiago: Universidad Diego Portales.

Caldevilla, David (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, Alberto (2003). *La autoridad de control en la legislación sobre protección frente al tratamiento de datos personales*. Tesis para optar al grado de Magíster. Santiago, Escuela de Derecho, Universidad de Chile

Cooley, Thomas (1879). *A Treatise on the Law of Torts, Or the Wrong which Arise Independently of Contract*. Chicago: Callaghan.

Drummond, Víctor (2004). *Internet, privacidad y datos personales*. Madrid: Reus.

Gil, Ana (2012). «El fenómeno de las redes sociales y los cambios en la vigencia de los Derechos Fundamentales». *Revista de Derecho UNED*, 10: 209-255.

Grupo de Trabajo sobre Protección de Datos del Artículo 29 (2009). «Sobre redes sociales en línea». Disponible en <http://bit.ly/1DRtBRN>.

—. (2013). «Sobre las aplicaciones de los dispositivos inteligentes». Disponible en <http://bit.ly/23WLyqz>.

Historia de la Ley, Artículo 19 núm. 4 de la Constitución Política de la República (1980). «El derecho a la privacidad». Disponible en <http://bit.ly/1YAEyhH>.

Historia de la Ley 19.628 (1999). «Artículo 17 sobre protección de la vida privada». Disponible en <http://bit.ly/1R7z9c5>.

Jervis, Paula (2003). «Derechos del titular y *Habeas data* en la Ley 19.628» *Revista Chilena de Derecho Informático,* 2: 19-33.

Jijena, Renato (1992). *La protección penal de la intimidad y el delito informático*. Santiago: Jurídica de Chile.

Madrid, Fulgencio (1984). *Derecho a la intimidad, informática y Estado de Derecho*. Valencia: Universidad de Valencia.

Martínez, Ricard (2007). «El derecho fundamental a la protección de datos: perspectivas». *Revista de Internet, Derecho y Política,* 5: 47-61.

Novoa, Eduardo (1979). *Derecho a la vida privada y libertad de información*. México: Siglo XXI.

Organización para la Cooperación y el Desarrollo Económicos, OCDE (2002). «Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales». Disponible en <http://bit.ly/293qttu>.

Parlamento y Consejo Europeo (1995). Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos». Disponible en <http://bit.ly/205dRTn>.

—. (2016). «EU-U.S. Privacy Shield». Disponible en <http://bit.ly/21vyeOf>

Rallo, Artemi y Ricard Martínez (2011). «Protección de datos personales y redes sociales: obligaciones para los medios de comunicación» *Quaderns del CAC,* 14 (2): 41-52.

Saldaña, María (2012). «The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: El centenario legado de Warren y Brandeis». *Revista de Derecho Político,* 85: 196-239.

Unión Europea (2014). «Maximillian Schrems y Data Protectión Comissioner. C-362/14 del Tribunal de Justicia» Disponible en <http://bit.ly/1swM0QX>.

Warren, Samuel y Luis Brandeis (1890). «The Right to Privacy» *Harvard Law Review*, 4 (5): 193-220.

SOBRE LA AUTORA

Paloma Herrera Carpintero es abogada. Licenciada en Ciencias Jurídicas y Sociales de la Universidad de Chile. Su correo electrónico es paloma.herrerac@gmail.com y su dirección postal es La Tepa 7403, Peñalolén, Santiago.

Este trabajo fue recibido el 19 de mayo y aprobado el 25 de junio de 2016.