Título: Derecho a la privacidad y protección de datos personales en las condiciones de uso y políticas de privacidad de las redes sociales(*)(**)
Autor: Grover Dorado, John
País: Argentina
Publicación: El Derecho - Diario, Tomo 268, 609
Fecha: 09-06-2016 Cita Digital: ED-DCCLXXVI-59

Voces | Documentos Relevantes

Sumarios

Derecho a la privacidad y protección de datos personales en las condiciones de uso y políticas de privacidad de las redes sociales(*)(**)

1

Introducción

El proceso de registro o suscripción a una red social presupone la aceptación de un instrumento jurídico complejo (pues suele estar formado por varios cuerpos escritos, entre los que se incluyen las “Política de Privacidad”, los “Principios”, las “Normas de Publicidad” y “de la Plataforma”, las “Políticas de Cookies”, las “Políticas de Propiedad Intelectual” o “Políticas de Copyright” , las “Directrices de Fotos”, “Directrices Comunitarias”, entre otros nombres que cada red social les otorga) que se conoce como “Términos o Condiciones de Uso” (“Terms of Use” o “Terms of Service”), los cuales son imprescindibles para dejar constancia de la mecánica de su funcionamiento, además de regular los derechos y las obligaciones de los usuarios y del prestador del servicio de red social (en adelante “PSRS”).

En este trabajo, analizaremos las condiciones a las que generalmente el usuario adhiere durante el proceso de registro en las redes sociales, destacando aquellas cláusulas que pueden afectar su privacidad o el recto uso de sus datos personales.

2

Condiciones de uso del servicio

2.1. Concepto y características

Los “Términos o Condiciones de Uso” o “Términos o Condiciones Generales del Servicio” constituyen el contrato marco que regula la relación de los usuarios y el proveedor de red social. Son de utilidad no solo para que el usuario conozca y cumpla determinadas normas de conducta, sino también para limitar la responsabilidad de los encargados de la red social. Por lo general, aquí se incluyen cláusulas relativas al contenido e información que el usuario cede a la red social, cuestiones de propiedad intelectual, de seguridad, de conducta con otros usuarios, resolución de conflictos, eximición de responsabilidad, competencia, entre otras.

En cuanto a la naturaleza jurídica de la suscripción o registro del usuario al servicio de red social, consideramos que se trata de un contrato click-wrap, electrónico, online, atípico y de adhesión a cláusulas generales. Veamos de qué se trata cada una de estas características:

- Contrato click-wrap: es un acuerdo en el cual se requiere que una de las partes (aceptante) manifieste su voluntad de aceptar las cláusulas redactadas por la otra (predisponente) mediante un simple clic del mouse en la leyenda “Acepto”, “Estoy de acuerdo” o similar, que aparece normalmente al final del documento escrito que se muestra en la pantalla de la computadora del usuario.

De la definición propuesta, emergen diversas particularidades, a saber:

a) No son tipos de contratos o contratos autónomos, sino una modalidad de contratación; en particular, entendemos que los click-wrap son una especie dentro del género contratos de adhesión. Es decir, gozan de las mismas características que los contratos de adhesión, pero se destacan por una forma especial de manifestar el consentimiento: a través del click del aceptante.

b) En cuanto a la terminología, cabe aclarar que los contratos click-wrap deben su nombre a una variación de los que se conocen como contratos shrink-wrap (en referencia a que, con la acción de romper el celofán con el que está envuelta la caja de un programa de computación, inmediatamente el usuario acepta las Condiciones Generales de las Licencias de Uso de software). También se usan los términos web-wrap o browse-

wrap para hacer énfasis en la adhesión a cláusulas generales habitualmente publicadas en sitios web o en los navegadores de Internet, respectivamente.

c) En cuanto a los sujetos, hablamos de aceptante y predisponente, pues los click-wrap pueden ser perfectamente utilizados en relaciones entre comerciante y consumidor (Business to Consumer o B2C), e inclusive entre comerciantes (Business to Business o B2B) y entre consumidores (Consumer to Consumer o C2C); es la primera relación la que interesa a los efectos del presente artículo.

d) Los click-wrap, si bien usados mayormente para acuerdos de licencia de uso final de software (EULA o End-User License Agreement), sean adquiridos en formato físico (en caso de que la licencia sea impresa y se adjunte con el paquete del software, hablaremos de shrink-wrap) o digital a través de Internet (web-wrap), también se utilizan para el otorgamiento de licencias de otros productos digitales disponibles en la red, como, por ejemplo, libros digitales (e-books), música, aplicaciones, videojuegos, entre otros, y para la aceptación de servicios ofrecidos por los sitios web, como, por ejemplo, adherirse a una base de datos o a una red social, obtener un espacio virtual para crear y moderar un blog, adherirse a una plataforma de compraventa o subasta de bienes o servicios online, etc.

e) Por último, en lo que respecta al formato en que se presenta el contrato en la pantalla del usuario, por lo general este trae aparejadas serias dificultades que obstan a su validez (v. gr., el texto del contrato suele aparecer en idioma extranjero o con deficiencias en la traducción que lo hacen inentendible; se requiere que el usuario acepte las condiciones generales antes de utilizar el producto, pero después de haberlo adquirido, incluso cuando el usuario no pudo tener acceso a ellas para leerlas; al pie de dichos contratos, se estila colocar la leyenda “Acepto”, “Estoy de acuerdo” u otra similar, marcada por defecto, sin requerir acción alguna del usuario, entre otras).

- Contrato electrónico: entendemos que estamos en presencia de una contratación electrónica, entendiendo por tal a “la que se realiza mediante la utilización de algún elemento electrónico, con influencia decisiva, real y directa sobre la formación de la voluntad, el desarrollo o la interpretación de un acuerdo”(1). Asimismo, entendemos que se trata de un contrato celebrado online o en línea, es decir, se trata de una contratación electrónica en la que el consentimiento (oferta y aceptación) se perfecciona a partir del intercambio de mensajes de datos transmitidos en tiempo real a través de una red telemática (v. gr., Internet).

En el derecho argentino, cabe encuadrar la presente caracterización bajo los arts. 1105, relativo a los contratos a distancia (a los cuales define como aquellos celebrados “con el uso exclusivo de medios de comunicación a distancia, entendiéndose por tales los que pueden ser utilizados sin la presencia física simultánea de las partes contratantes. En especial, se consideran los medios postales, electrónicos, telecomunicaciones, así como servicios de radio, televisión o prensa”), y en particular el 1106 del cód. civil y comercial

(en adelante, CCyC), el cual establece que la exigencia de escritura se hallará satisfecha siempre que el contrato contenga “un soporte electrónico u otra tecnología similar”.

- Contrato atípico: es también atípico o innominado en cuanto no está legislado expresamente y su forma y contenido resultan de libre creación de las partes. Como corolario de ello, rige de manera plena el principio de la autonomía de la voluntad, con los límites de aquellas disposiciones de orden público que alcancen al contrato de marras (v. gr., derecho del consumidor, de protección de datos, administrativo, etc.).

- Contrato de adhesión y de consumo: dada su naturaleza de contrato click-wrap, entendemos que se trata de un contrato de adhesión, en cuanto resulta ser una convención por medio de la cual la parte contractual más fuerte (el PSRS) predispone las cláusulas del convenio de modo tal que la otra (el usuario) no puede modificarlas, sino que solo tiene la facultad de aceptarlas o rechazarlas en bloque(2).

Resultan aplicables las normas generales del Código Civil y Comercial referidas a los contratos por adhesión a cláusulas predispuestas (art. 984 y sigs.), definidos por el ordenamiento jurídico nacional como aquellos en los que “uno de los contratantes adhiere a cláusulas generales predispuestas unilateralmente, por la otra parte o por un tercero, sin que el adherente haya participado en su redacción” (art. 984, CCyC).

Finalmente, entendemos que las Condiciones del Servicio, dada la amplitud con la que nuestro Código Civil y Comercial y la Ley 24.240 de Defensa del Consumidor (en adelante, LDC) definen la relación de consumo (se trata del “vínculo jurídico entre el consumidor o usuario y el proveedor”, según disponen los arts. 1092 del CCyC y 3º de la LDC), constituyen un acuerdo de voluntades entre partes con entidad suficiente para encontrarse comprendido en dicha normativa (de hecho, deben comprenderse bajo la categoría “contrato de consumo”, en los términos del art. 1093, CCyC). Es claro que tanto quien utiliza el servicio de red social como quien pone a su disposición la plataforma sobre la cual se desarrolla dicha prestación constituyen consumidores (arts. 1092, CCyC y 1º, LDC) y proveedores (art. 2º, LDC), respectivamente.

2.2. Contenido y cláusulas habituales

Entre las cláusulas que habitualmente encontramos incluidas en los referidos “Términos o Condiciones del Servicio”(3), deben destacarse aquellas disposiciones relativas a:

- Privacidad de los datos personales: las normas tendientes a regular la protección de datos personales se encuentran en las famosas “Políticas de Privacidad”, las cuales serán analizadas ut infra en el punto 3.

- Contenidos de Propiedad Intelectual: una de las cláusulas más importantes es aquella que otorga al PSRS derechos sobre todo material escrito, fotográfico o audiovisual del usuario, por lo cual queda aquel con derecho a administrar y disponer de derechos de propiedad intelectual. Debemos recordar en este punto que los contenidos aportados y cedidos por los usuarios que sean protegibles vía derecho de autor, si bien pueden ser de lo más variados, muchas veces consistirán en comentarios, fotografías y videos que guardan relación con la intimidad de la persona. De esta forma, no solo se comprometen derechos de autor sino, además, el derecho de imagen que corresponde reivindicar a quienes hayan sido retratados, o el derecho de autodeterminación informativa sobre datos personales en caso de que el material permita la vinculación con la identidad de una persona en particular.

La mayor discusión respecto de estas cláusulas tiene lugar a nivel de la falta de claridad en los textos de las condiciones de contratación, pues, en muchas ocasiones, el alcance de la mentada licencia puede ser excesivo con el fin meramente "social" y de compartir contenidos con otros usuarios, al que tiende la mayoría de las redes sociales. En este sentido, y a los fines de un recto tratamiento de datos personales, los términos de la licencia debieran circunscribirse a autorizar al PSRS la reproducción y comunicación pública de los contenidos, siempre y cuando sea con el único fin de que se preste el servicio prometido, además de garantizar la resolución de la licencia al momento en que el usuario elimine todos los contenidos de la plataforma o bien cuando dé de baja su perfil(4).

Si bien muchas de las redes sociales en la actualidad orientan sus textos en este sentido, algunas con mayor o menor claridad, luego, en la realidad de la dinámica contractual ocurre algo muy distinto, pues, en el fondo, la cláusula de licencia de propiedad intelectual –que suele afirmar que el usuario es el propietario de todo el contenido y la información que se publica en la red social– funciona como una autorización para que el PSRS pueda disponer de dicho material –inclusive aun cuando el usuario dio de baja su perfil–, de modo tal que termina siendo lisa y llanamente una cesión gratuita y exclusiva de PI, que, además, suele permitir utilizar los contenidos cedidos con fines publicitarios u otros fines no previstos en las Condiciones de Uso.

- Seguridad informática: también es muy común que las redes sociales, al ser enormes plataformas de alojamiento de contenidos de propios y de terceros, quieran garantizar a sus usuarios un estándar mínimo de seguridad informática y, en tal sentido, prevean prohibiciones –muchas de ellas vinculadas a la privacidad online–, tales como no publicar comunicaciones no deseadas (spam), no recopilar información o contenidos de otros usuarios (data mining), no utilizar medios automáticos para ingresar al sitio web (robots o arañas), no subir virus o códigos maliciosos (spyware, malware, badware, rootkits, gusanos, troyanos, etc.), no realizar ataques de denegación de servicio (DoS) o alterar la presentación de páginas u otra funcionalidad de la plataforma de la red social, entre otras.

- Normas de conducta de los usuarios: otro de los puntos esenciales que merecen regulación lo constituye el conjunto de estándares de conductas esperables del usuario,

es decir, el proveedor suele incluir un listado de “buenas prácticas” para los usuarios, y adquieren diversos nombres, a saber: directrices comunitarias profesionales (LinkedIn), derechos y responsabilidades o normas comunitarias (Facebook), o reglas y políticas de uso (Twitter).

Entre dichas cláusulas, los proveedores usualmente incluyen también prohibiciones que puedan afectar legítimos derechos de terceros, como, por ejemplo, la de crear cuentas falsas o inexactas, de suplantar identidades, de afectar la seguridad informática de las cuentas propias, de terceros o de cualquier otro software, hardware, sistema, servidor, redes, equipo de telecomunicaciones, o cualquier sistema, datos, contraseña u otra información de la cual el proveedor es propietario, de publicar contenidos ofensivos, pornográficos, que inciten a la violencia o que contengan desnudos o violencia gráfica o injustificada, o que impliquen molestia, hostigamiento, intimidación o acoso a otros usuarios, que impliquen injurias, fraudes o, en fin, que resulten actos engañosos, malintencionados, discriminatorios y, en general, contrarios a toda legislación tuitiva del honor, imagen e intimidad, del secreto en las comunicaciones, de los derechos de propiedad industrial e intelectual o de las normas reguladoras de la protección de datos de carácter personal.

- Sistemas de bloqueo ante la violación de derechos de terceros: dentro de las plataformas de las redes sociales se estila crear y poner a disposición de los usuarios sistemas de denuncia ante cualquier eventual infracción a las normas comunitarias ya referidas. Este mecanismo permite notificar al PSRS de cualquier contenido inadecuado, ilícito o contrario a las Condiciones del Servicio, con el objeto de bloquearlos o darlos de baja de su plataforma.

Cabe resaltar que estos sistemas suelen utilizarse en el resto de los sitios web que alojan contenidos que pueden afectar principalmente derechos de propiedad intelectual (v. gr., sitios de compraventa o subastas online e ISP de alojamiento o hostings), y se conocen como “Notice and Take Down”, aludiendo al bloqueo inmediato que debe efectuar el ISP luego de que fue puesto en conocimiento de su existencia, bajo pena de ser responsables legalmente. También se habla de “safe harbour” para referirse al “puerto seguro” que constituye la falta de responsabilidad de los ISP siempre y cuando no tengan conocimiento efectivo y actual del contenido que se pretende dañoso.

- Resolución de conflictos: para el eventual caso de conflicto judicial entre usuarios y proveedores del servicio, los “Términos de Uso” suelen comprender disposiciones típicas que limitan las responsabilidades de los proveedores, y que fijan la legislación y la competencia en el lugar en el que el proveedor tiene su sede principal (Facebook, Twitter y LinkedIn someten sus disputas a los tribunales estatales o federales de California, por lo que son de aplicación las leyes de dicho estado; Tuenti hace lo propio en Madrid, España; y Foursquare fija ley y jurisdicción en Nueva York), así como también cláusulas compromisorias que prevén la opción del arbitraje como método alternativo de resolución de disputas (LinkedIn, por ejemplo, prevé que para cualquier demanda en la que el importe total solicitado sea inferior a USD 10.000, la parte demandante podrá decidir resolver el conflicto mediante arbitraje, cuya decisión será vinculante y no exigirá la presencia física de las partes involucradas).

- Otras estipulaciones: finalmente, encontramos otro tipo de normas más específicas que se aplican o bien a diversos partícipes o intermediarios en el servicio, distintos del consumidor, o bien para casos particulares. Así encontramos normas: para anunciantes que deseen hacer publicidad; para desarrolladores de software y aplicaciones; para creadores de grupos o páginas de empresa; relativas a pagos de alguno de los servicios que no son gratuitos; relativas a enlaces o hipervínculos a contenidos, productos o servicios ofrecidos desde otras páginas web o fuentes; referidas a la rescisión, integridad y a los cambios en las "Condiciones de Uso"; referidas a la descarga y al acceso desde las aplicaciones móviles y desde otros complementos (plugins) interactivos distribuidos en distintos sitios web, etc.

3

Políticas de privacidad

El apogeo en el uso de las redes sociales ha generado el procesamiento de una enorme cantidad de datos que no registra precedentes en la historia, con el agravante de estar muchos de ellos disponibles pública y globalmente.

La forma de proteger esa cantidad masiva de datos elegida por los PSRS hoy en día consiste en proveer a los usuarios de las herramientas necesarias para establecer distintos niveles de privacidad de acuerdo a sus preferencias ("privacidad desde el diseño"). Sin embargo, debe advertirse que la configuración que es establecida por defecto por los PSRS ("privacidad por defecto"), en la mayoría de los casos permite a los usuarios mostrar sus datos de perfil a todos sus contactos o al público en general, lo que es un riesgo para quienes no configuran el nivel de privacidad de sus contenidos.

En este marco, cabe destacar que este enfoque de resguardo de privacidad se desarrolla en el marco contractual que los PSRS imponen dentro de sus "Términos y Condiciones", específicamente en documentos anexos o integrantes del texto principal, llamados "Políticas de Privacidad", sobre cuyas cláusulas nos referiremos en detalle a continuación.

3.1. Privacidad desde el diseño y por defecto

La "privacidad desde el diseño" (privacy by design)puede considerarse un paradigma actual de protección de la privacidad, basado en la idea de que los titulares de bases de datos o quienes tengan la responsabilidad legal de procesar datos implementen medidas y procedimientos técnicos y organizacionales apropiados para tal fin, de modo tal que el

procesamiento de datos personales cumpla con la legislación vigente, asegurando los derechos de los titulares de dicha información.

Dentro del ámbito de las redes sociales, la concreción de esta idea consiste en permitir a los usuarios establecer diferentes niveles de privacidad de datos, eligiendo qué datos, información o contenido serán publicados en la plataforma del PSRS, con quién se compartirán (v. gr., si con una persona, grupo de personas o el público en general), cuáles de ellos serán indexados o no por los motores de búsqueda, cuáles requerirán autorización para ser compartidos con terceros (v. gr., el "etiquetado" [tagging] de fotos, que la vincula con el perfil de la persona etiquetada), etc.

La "privacidad por defecto" (privacy by default(5)), por otra parte, significa que las referidas medidas y procedimientos adoptados deben asegurar que, por defecto, el procesamiento de datos personales incluya solamente aquella información necesaria para cada propósito específico de recolección de datos, aplicándose en particular a la cantidad de datos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad.

En las plataformas de las redes sociales, una práctica harto difundida consiste en la diferenciación de los datos por ser recolectados, en la que existen dos categorías, a saber: datos que son siempre públicos y datos que son voluntariamente públicos. En relación con estos últimos, los datos son por defecto públicos desde el momento en que el usuario se registra en la plataforma del PSRS(6), lo que requiere una acción positiva consistente en el cambio de las configuraciones de privacidad.

Por lo dicho, la esencia de este concepto es la de contribuir en la mitigación de una innecesaria divulgación de datos que son consecuencia de las configuraciones referidas. Por ende, en la práctica, los mecanismos que los PSRS otorgan a los usuarios deberían tender a garantizar que, por defecto, los datos personales no sean accesibles al público en general.

3.2. Contenido y cláusulas habituales

Las llamadas "Políticas de Privacidad" son cláusulas contractuales que prevén las condiciones de protección de los datos personales de los usuarios en distintas páginas web. Si bien estas generalmente se encuentran en documentos separados, a los cuales remiten las "Condiciones Generales del Uso", en realidad se trata de cláusulas principales que integran el contrato de servicio y que resultan esenciales a los fines de informar –con anterioridad a formar parte de la red social– al usuario respecto de si existe un procesamiento de sus datos personales; quién es el responsable de esto; cuál va a ser su finalidad; si se van a ceder o no dichos datos y a quién; cómo va a ser el proceso de recolección, tratamiento, almacenamiento, revelación y otros usos de la información,

y cuáles son sus derechos, es decir cómo se accede a los datos que se tengan sobre él y cómo se modifican, eliminan o someten a confidencialidad en caso de ser erróneos.

Es de rigor destacar que en este conjunto de cláusulas se incluyen disposiciones referidas a:

• Recolección y uso de datos: los PSRS recolectan distintos tipos de información, que incluye toda aquella que el propio usuario voluntariamente provee a la plataforma con motivo del registro y toda aquella que se recolecta automáticamente o a través de terceros proveedores de distintos servicios que interactúan con la plataforma, como ser, principalmente, proveedores de servicios de pagos, proveedores de aplicaciones y sitios web que integran botones, cuadros y demás widgets o plug-ins desde los cuales pueden los usuarios registrarse para autenticación o identificación, o bien simplemente para acceder a contenidos de la red social.

Entre estos datos encontramos: datos que otros usuarios comparten sobre una persona (v. gr., comentarios, etiquetas sobre fotografías, videos, ubicaciones), datos del uso de la plataforma (v. gr., perfiles visitados, tiempo de tal visita, palabras buscadas, clicks), datos del dispositivo (v. gr. si se accedió desde una computadora o un teléfono móvil, identificadores de hardware, sistema operativo, navegador), de la red (v. gr., proveedor de servicios de Internet, ubicación, dirección IP, identificadores de red), metadatos (v. gr., fecha, hora y lugar de los archivos subidos), etc.

Ahora bien, muchos de estos datos, en cuanto permitan ser vinculados a la identidad de una persona, constituyen datos personales protegidos por las leyes de protección de datos y, por tal motivo, deben ser sometidos a estándares de protección más altos que cualquier otro dato o información.

• Responsable del tratamiento de datos personales: no hay duda alguna de que la actividad que desarrollan los PSRS puede encuadrarse en el concepto previsto por las leyes de protección de datos personales referido al “tratamiento de datos personales” y que, por consecuencia, resultan “responsables” por ella. Es por ello que en toda “Política de Privacidad” se especifican los datos de identificación del responsable del tratamiento de los datos personales de los usuarios, particularmente, el nombre o razón social, domicilio y demás datos de contacto (dirección postal o electrónica) de la casa matriz o filial que hará el procesamiento de los datos según la ubicación del usuario.

• Consentimiento de menores de edad: las redes sociales por lo general establecen que los menores de 13 o 14 años no pueden registrarse como usuarios, en razón de ser esa la edad legal mínima exigida para consentir válidamente el tratamiento de datos personales. Así, la ley federal estadounidense “Children’s Online Privacy Protection Act” (COPPA) establece que los titulares de sitios web o proveedores de servicios online no podrán recolectar información personal de sus usuarios menores de 13 años sin

autorización parental. En España, el art. 13 del real decreto 1720/07 establece que "podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela".

Desde el punto de vista de la legislación argentina, la ley 25.326 nada dice respecto de los datos de menores de edad ni de la capacidad de estos para consentir su disposición. Por ello, cabe la aplicación de las normas generales del Código Civil y Comercial (arts. 25, 261, 382, 387, 1000, 1001 y concs.) y, por tanto, entendemos que no solo las disposiciones relativas al tratamiento de datos personales, sino todo el contrato de adhesión a redes sociales celebrado por menores de 18 años sería ineficaz en razón de su nulidad, y dicha nulidad, de carácter relativo.

No obstante, entendemos que en el caso de los menores de 13 años, al carecer estos no solo de capacidad de ejercicio sino también de discernimiento para actos lícitos, sus actos deberán considerarse involuntarios y presumirse nulos por disposición legal (art. 261, CCyC).

• Derechos del titular de datos personales: es de rigor incluir a nivel contractual disposiciones protectorias de los datos personales del usuario, entre las que se destacan los derechos a acceder a los datos que se tengan sobre él, a modificarlos, a eliminarlos y a someterlos a confidencialidad.

A los fines de hacer efectivos estos derechos, la tendencia adoptada por las redes sociales es otorgar a sus usuarios la posibilidad de configurar el grado de privacidad de sus datos, con la posibilidad de elegir qué datos, informaciones o contenidos se publican o no en el sitio web del proveedor de red social; si se quiere que estos sean indexables o no en los motores de búsqueda; con quiénes se comparten; si se requiere de una autorización para compartir determinados datos o contenidos propios o de terceros (ejemplo de esto último es el famoso "etiquetado" en fotos que se suben a Facebook), etc.

• Transferencia de datos: el referido tratamiento de datos personales puede realizarlo directamente el responsable de la base de datos o bien, indirectamente, a través de una cesión a terceros proveedores de alojamiento, proveedores de servicios de estadísticas y análisis de datos, desarrolladores y proveedores de servicios de aplicaciones, juegos y demás páginas web desde las cuales se accede a las redes sociales a través de plugins o widgets, quienes por lo general llevan a cabo funciones o prestan servicios fuera del país en el que el responsable tiene su casa matriz. En este último caso, el proveedor principal se reserva la facultad de compartir los datos personales con terceros proveedores de servicios conforme a las obligaciones de confidencialidad compatibles con sus "Políticas de Protección de Datos" y a condición de que los terceros utilicen sus datos personales únicamente conforme a sus instrucciones(7).

• Cambios en la estructura organizacional: en toda “Política de Privacidad” suele disponerse que, para el caso en que el proveedor sufra alguna eventualidad en su estructura societaria (concurso, quiebra, fusión, adquisición, reorganización o venta de activos, etc.), los datos de los usuarios –acaso el activo más importante de los PSRS– también podrán ser vendidos o transferidos a terceros participantes de dichos cambios.

• Conservación y divulgación de datos: los PSRS, en su afán de intentar cumplir con las legislaciones locales, comunican al usuario que existe la posibilidad de que todos sus datos, incluidos los datos personales, puedan ser conservados o revelados si se considera que es necesario para cumplir con una ley, reglamento o requerimiento legal o judicial, o bien para hacer cumplir o aplicar las “Condiciones de Uso” y otros acuerdos que sean partes de aquellas, o proteger los derechos, propiedad o seguridad del proveedor de red social, de sus empleados, usuarios u otros terceros.

• Cookies y tecnologías similares: todas las redes sociales se valen de la utilización de pequeños archivos llamados cookies (o tecnologías similares(8)), que se almacenan en el dispositivo del usuario a instancias del navegador web y que tienen por objeto mejorar la experiencia de navegación del usuario al facilitar al sitio web sus datos de identificación y de preferencia.

La información recolectada por estos medios, no obstante, permite la creación de perfiles de usuarios, que comprenden datos sobre su comportamiento online, preferencias en la web, cantidad de tiempo que se dedica a cada preferencia, avisos y publicidades visitados, entre otros(9).

En el contexto de las redes sociales, las “Políticas de Privacidad” suelen estipular que las cookies y tecnologías similares sirven para: a) autenticación, b) recordar preferencias de usuarios, c) detección de spam, abuso y otras actividades violatorias de las reglas de conducta, d) análisis e investigación de datos, e) mostrar al usuario contenido personalizado, f) elaboración de avisos publicitarios precisos, etc.

• Eliminación de datos: una cláusula harto habitual es aquella que dispone que, incluso después de eliminar la información de la cuenta o perfil del usuario, pueden permanecer copias de esa información visibles en otros lugares, en la medida en que haya sido compartida con otras personas, haya sido distribuida de alguna manera conforme a la configuración de privacidad del usuario o haya sido copiada o almacenada por otros usuarios. Asimismo, se prevé que toda información eliminada o borrada pueda permanecer en copia de seguridad por un plazo razonable antes de ser eliminada de los servidores de los PSRS.

Cláusulas violatorias de normas imperativas

Las “Políticas de Privacidad”, como parte integrante de las “Condiciones de Uso” –las cuales, según lo apuntado al referirnos a su naturaleza jurídica, constituyen un contrato de consumo sujeto a normas imperativas del CCyC y de la ley 24.240–, pueden contener cláusulas abusivas en el sentido de los arts. 988 del CCyC y 37 de la LDC, las cuales naturalmente infringen no solo dicha normativa, sino también la Ley 25.326 de Protección de Datos Personales (en adelante, LPDP). Veamos a continuación ejemplos de este tipo de cláusulas.

4.1. Cláusulas que infringen los derechos del consumidor

En la actualidad, las “Condiciones de Uso” han sido mejoradas ostensiblemente si se las compara con los textos vigentes de hace unos pocos años; ahora son bastante completos y, dependiendo de la masividad y globalidad de cada red social, en lo posible, adaptados a la legislación regional o local. Es decir, en líneas generales, se cumple con las obligaciones legales esenciales que toda legislación tuitiva de los consumidores impone.

Ahora bien, algunas condiciones que usualmente se estipulan, sean en las “Condiciones de Uso” o en las “Políticas de Privacidad”, pueden contravenir lo dispuesto por el CCyC y la LDC –sobre todo, pero no excluyentemente, cuando se trate de informaciones que no encuadran en el concepto de “dato personal”(10), ámbito en el que entra a regir, por su especialidad y mayores estándares de protección de orden público, la LPDP–, en los casos que se enumeran a continuación:

• Falta de consentimiento informado: es típico que en los casos de cesión o transferencia internacional de datos se autorice a terceros (sobre todo desarrolladores o proveedores de aplicaciones y titulares de sitios web que incluyen complementos o botones desde los que el usuario se registra o accede a contenido de la plataforma de la red social) a utilizar datos sin consentimiento informado del consumidor del servicio. Tales prácticas acaban por ser contrarias al principio de certeza y claridad de la información (arts. 1100, CCyC; 4º, LDC y resolución 21 del Grupo Mercado Común del Mercosur), presupuesto básico de toda negociación de consumo.

• Incumplimiento del deber de informar: generalmente se concreta ante la falta de identificación completa del PSRS o de los terceros que procesan datos por cuenta de este y que también forman parte de la prestación esencial del servicio, pues estos suelen estar identificados simplemente con una dirección postal y, eventualmente, con una dirección de correo electrónico ante la cual pueden hacerse reclamos o comentarios respecto de las “Políticas de Privacidad”, por lo cual se pierde todo tipo de posibilidad de contacto directo o personal con el usuario, que generalmente es de otro país y habla otro idioma.

Asimismo, conspiran contra el cumplimiento de lo dispuesto por los arts. 985 del CCyC y 10 de la LDC y, por tanto, socavan los derechos del consumidor, todo tipo de dificultades de forma y contenido del contrato, como ser convenciones redactadas en idioma extranjero (cabe recordar que la mayoría de los textos vigentes son meras traducciones de otros idiomas y sin demasiado rigor técnico-jurídico), en forma parcial, poco clara e ilegible, con reenvíos a textos o documentos que no se encuentran fácilmente accesibles a la vista del consumidor para su conocimiento y posterior aceptación, etc.

Cabe recordar, asimismo, que el art. 1107 del CCyC dispone que, además de la información relativa a las características del bien o servicio que provee o presta, el proveedor que utiliza medios electrónicos para contratar debe "informar al consumidor, además del contenido mínimo del contrato y la facultad de revocar, todos los datos necesarios para utilizar correctamente el medio elegido, para comprender los riesgos derivados de su empleo, y para tener absolutamente claro quién asume esos riesgos".

• Legislación y jurisdicción: son particularmente abusivas aquellas cláusulas que disponen la aplicación de la ley y jurisdicción de países extranjeros en favor de los PSRS en caso de conflictos que involucren protección de datos, en tanto implicaría una elusión inaceptable de las normas nacionales, amén de constituir una renuncia o restricción de los derechos del consumidor o una ampliación de los derechos del proveedor de red social (arts. 988, inc. b], CCyC y 37, inc. b], LDC). Asimismo, tales cláusulas podrían eventualmente afectar el principio de gratuidad en el acceso a la justicia (art. 53, LDC) al imponer al consumidor la carga económica de un eventual litigio en el extranjero.

• Limitación de responsabilidad: todo tipo de limitación de responsabilidad será abusiva en los términos de los arts. 988, inc. a), del CCyC y 37, inc. a), de la LDC.

En relación con la responsabilidad contemplada por la LDC, sea cuando existe una deficiente prestación del servicio (art. 23) o cuando resulta del vicio o riesgo de la cosa o de la prestación del servicio (art. 40), ambas en perjuicio del consumidor, aquella será solidaria para el productor, el fabricante, el importador, el distribuidor, el proveedor, el vendedor y quien haya puesto su marca en la cosa o servicio.

Cabe aclarar en este punto que la mentada responsabilidad solidaria de la LDC aplica a los daños patrimoniales y no a los daños derivados de "la violación de los derechos personalísimos del consumidor, su integridad personal, su salud psicofísica, sus afecciones espirituales legítimas, las que resultan de la interferencia en su proyecto de vida ni, en general, a las consecuencias no patrimoniales" (art. 40 bis in fine, LDC). En este último caso rigen los principios generales de la responsabilidad civil (art. 1708 y sigs., CCyC, en especial, el art. 1741 relativo a la indemnización de las consecuencias no patrimoniales y el art. 1770 relativo a la protección de la vida privada). No obstante, creemos que cualquier otro tipo de limitación contractual de responsabilidad derivada de consecuencias no patrimoniales también será una cláusula abusiva, en los términos del

art. 1119 del CCyC (“es abusiva la cláusula que, habiendo sido o no negociada individualmente, tiene por objeto o por efecto provocar un desequilibrio significativo entre los derechos y las obligaciones de las partes, en perjuicio del consumidor”); se la tendrá por no convenida (art. 1122, CCyC) y será aplicable lo dispuesto por los arts. 988 y 989 del CCyC, relativos a cláusulas abusivas y sus efectos en los contratos celebrados por adhesión a cláusulas generales predispuestas.

4.2. Cláusulas que infringen los derechos

a la protección de datos personales

Entendemos que, en muchas oportunidades, tanto las “Condiciones de Uso” como las “Políticas de Privacidad” pueden encontrarse reñidas con las disposiciones de orden público de la ley 25.326, las cuales resultan inderogables por vía contractual(11). Veamos brevemente de qué tratan algunas de ellas:

• Falta de consentimiento: para disponer el tratamiento lícito de datos en un banco de datos personales es menester que el titular del dato haya prestado su consentimiento libre, expreso e informado (art. 5º, LPDP). En muchos casos, los proveedores no respetan este principio: a) cuando se recolectan y tratan datos sensibles, sin que medien razones de interés general autorizadas por ley, o cuando exista formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles (arts. 2º y 7º, LPDP), b) al no solicitar el consentimiento en caso de cesión o transferencia internacional de datos en favor de terceros que intervienen en aplicaciones y páginas web complementarias a la plataforma de la red social (arts. 11 y 12, LPDP), c) al presumir el consentimiento del usuario del mero uso que este hace del servicio luego de que se hayan efectuado y publicado cambios –incluso intempestivos e inconsultos– en las “Condiciones de Uso” o “Políticas de Privacidad”, d) cuando se etiquetan contenidos audiovisuales, vinculándolos con el perfil de terceros sin su consentimiento.

• Inseguridad de los datos: creemos que la protección que se brinda en el sistema de privacidad desde el diseño es lisa y llanamente una eximición total o parcialmente al PSRS de toda responsabilidad por los daños que puedan derivarse de dicho tratamiento. Tal inaceptable conducta implica, en rigor, una transferencia de responsabilidad al usuario de resguardar bajo privacidad sus propios datos personales y eventualmente datos o contenidos de terceros y, por tanto, una renuncia o al menos una limitación a la responsabilidad del PSRS de velar por la seguridad de la información (arts. 988, CCyC y 37, LDC).

Asimismo, entendemos que, cuando se prevé que las configuraciones de privacidad tengan por defecto el mayor grado de publicidad, existe una negligencia en la obligación de resguardar la seguridad y confidencialidad de los datos personales.

En ambos casos, se contraviene lo dispuesto por el art. 9º de la LPDP, el cual prevé la obligación del titular de la base de datos de adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

• Recolección de datos con fines publicitarios: la utilización de cookies y tecnologías similares permite al PSRS recolectar diversos tipos de datos (v. gr., dirección IP, fecha de acceso, nombre de usuario, palabras de búsqueda, sistema operativo y tipo de navegador), los cuales permiten ser vinculados a la identidad de una persona; resulta de ello la obtención de datos personales de sus usuarios, los cuales, a su vez, forman parte de bases de datos con fines principalmente publicitarios o que permiten establecer hábitos de consumo. Esto último, a su vez, resulta contrario al principio de calidad de los datos que surge del art. 4º, inc. 3º, de la LPDP, en cuanto se excede el fin para el cual esos datos fueron recolectados, pues normalmente las "Condiciones de Uso" o "Políticas de Privacidad" afirman obtener datos con fines "de personalización" o "estadísticos" o "de seguridad".

En todos estos casos, la utilización de estas técnicas será ilícita cuando esos datos no figuren en documentos accesibles al público o no hayan sido facilitados por los propios titulares u obtenidos sin su consentimiento (art. 5º, LPDP), o bien cuando no se les otorgue el derecho de acceder sin cargo alguno o el de solicitar el retiro o bloqueo de su nombre de los bancos de datos referidos (art. 27, LPDP).

• Eliminación de datos: la mayoría de las "Políticas de Privacidad" estipulan cláusulas poco claras –y, por tanto, violatorias del principio de consentimiento informado del art. 5º de la LPDP– en materia de eliminación de los datos de la cuenta del usuario, intentando confundir a este con dos conceptos diferentes: desactivación y eliminación de cuenta.

La primera de ellas es una mera suspensión temporal, que simplemente mantiene fuera del sitio la información de perfil del usuario y que le permite restaurar su cuenta antes de un determinado plazo, que normalmente oscila entre 30 y 60 días. La eliminación, por su parte, es efectivamente el borrado definitivo de los datos del usuario del sitio y de los servidores del proveedor, los cuales, no obstante, pueden permanecer como copias visibles en otros lugares, en la medida en que haya sido compartida con otras personas, haya sido distribuida de alguna manera conforme a la configuración de privacidad del usuario o haya sido copiada o almacenada por otros usuarios. Asimismo, esta información eliminada, informan los PSRS, puede permanecer en los medios de copia de seguridad por hasta un plazo razonable –normalmente de 90 días– antes de ser eliminada de los servidores del proveedor.

En el mismo sentido, también resulta contraria a las normas de consentimiento de la LPDP y al principio de calidad de datos emergente del art. 4º, inc. 7º, de la LPDP, que en nuestro ordenamiento consagra implícitamente el llamado "derecho al olvido"(12), la falta de eliminación de la información del usuario que ha dejado de ser necesaria para el fin para el cual fue recolectada, que en el caso de las redes sociales, tal como lo sostuviéramos con anterioridad, solo debe limitarse a la prestación del servicio.

• Competencia federal: finalmente, en relación con la competencia en razón de la materia, los arts. 36, inc. b), y 44 in fine de la LPDP disponen la procedencia de la competencia federal en caso de que los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales. La jurisprudencia ha dejado bastante clara la interpretación de este tema: "Si la información que se pretende suprimir fue proporcionada por Internet, que constituye una red interconectada a la que se refiere el art. 44 citado, es claro que deben intervenir en la controversia los jueces federales con competencia Civil y Comercial"(13). Entendemos que cualquier tipo de disposición que establezca una competencia distinta encuadraría en los arts. 988, inc. b), y 37, inc. b), de la LDC.

5

Conclusión

A modo de colofón, luego de haber examinado algunos de los problemas jurídicos relativos a la contratación del servicio de redes sociales, debe concluirse que, más allá del paradigma actual utilizado por los proveedores del servicio, basado en una protección de la privacidad desde el diseño –el cual implica otorgar al usuario herramientas de configuración de privacidad–, este debe necesariamente complementarse con un enfoque de privacidad por defecto que mitigue la divulgación masiva de información en las redes sociales y, además, por previsiones contractuales contenidas en las "Condiciones de Uso" y principalmente en las "Políticas de Privacidad" aún más fuertes que las vigentes, en tanto estas últimas, como vimos, suelen resultar lesivas de la privacidad, de los datos personales del usuario y de sus derechos como consumidor frente a una contratación electrónica.

6

Bibliografía

Libros y artículos de doctrina

- Anzit Guerrero, Ramiro - Tato, Nicolás - Profumo, Santiago, El derecho informático. Aspectos fundamentales, Buenos Aires, Cathedra Jurídica, 2010.

- Fariña, Juan M., Defensa del consumidor y del usuario, Buenos Aires, Astrea, 2008.

- Uicich, Rodolfo D., El derecho a la intimidad en Internet y en las comunicaciones electrónicas, Buenos Aires, Ad-Hoc, 2009.

Jurisprudencia extranjera

- Sentencia del Tribunal de Justicia Europeo (Gran Sala) del 13-5-14 en el Asunto C-131/12, "Google Spain, S.L., Google Inc. c. Agencia Española de Protección de Datos (AEPD)".

Jurisprudencia nacional

- CNCiv., sala G, "Svatzky, Betina L. c. Datos Virtuales S.A. s/hábeas data", 28-4-04.

Sitios web

- Sitios web de Facebook, Twitter, Foursquare, LinkedIn y Tuenti.

- Defensa del Consumidor, Secretaría de Comercio: ttp://www.consumidor.gob.ar/.

- EurLex: http://eur-lex.europa.eu/.

- InfoLeg: http://www.infoleg.com/.

- Curia Europa: http://curia.europa.eu/.

VOCES: INTERNET - INFORMÁTICA - PERSONA - TECNOLOGÍA - CONSTITUCIÓN NACIONAL - HÁBEAS DATA - DERECHO A LA INTIMIDAD

(*) Nota de Redacción: Sobre el tema ver, además, los siguientes trabajos publicados en El Derecho: Los buscadores en Internet. La protección de los derechos personalísimos. Utilización de la medida cautelar innovativa: adecuada pero... ¿suficiente?, por Gustavo J. Vaninetti y Hugo A. Vaninetti, ED, 222-335; Estafa por medios electrónicos. Análisis del art. 173, inc. 16 (ley 26.388). Crítica. Manipulación informática. Estafas cometidas vía Internet, por Gustavo J. Vaninetti y Hugo A. Vaninetti, ED, 229-776; Contenidos discriminatorios en un sitio web: anotaciones acerca de un fallo que no responsabiliza a un sitio web, por Verónica E. Melo, Ros-Online, 26-10-09, nº 33; La responsabilidad civil de los buscadores en Internet. Afectación de los derechos personalísimos. Supuestos para analizar, por Hugo A. Vaninetti, ED, 238-808; Buscadores en Internet: responsabilidad civil, por Gustavo J. Vaninetti y Hugo A. Vaninetti, ED, 240-253; Buscadores en Internet. Tres recientes sentencias que delimitan el alcance de su responsabilidad civil y las dificultades para hacer efectivas medidas judiciales de bloqueo a páginas web. Lo que establece la Declaración Conjunta sobre Libertad de Expresión e Internet de la ONU al respecto. Necesidad de una regulación legal, por Hugo A. Vaninetti, ED, 245-775; La víctima del delito informático, por Hugo A. Vaninetti, ED, 249-700; Responsabilidad civil de los buscadores, por Gustavo J. Vaninetti y Hugo A. Vaninetti, ED, 251-165; Facebook, estado de reposo y derecho, por Tomás I. González Pondal, ED, 254-844; Responsabilidad civil de los buscadores. Reflexiones sobre los peligros de caer en una nueva "industria del juicio". Necesidad de un sinceramiento de los involucrados en esta problemática, por Gustavo J. Vaninetti y Hugo A. Vaninetti, ED, 256-668; El derecho al olvido en Internet (un fallo del Tribunal de Justicia de la Unión Europea que contribuye a la preservación de la imagen en los entornos virtuales), por Guillermo F. Peyrano, ED, 258-918; Motores de búsqueda en Internet. La Corte Suprema de Justicia de la Nación examina la legitimidad de su operación, por Antonio Millé, ED, 260-197; La protección de los datos personales en Internet: lineamientos que caben deducirse del fallo de la Corte Suprema, por Esteban Ruiz Martínez, ED, 260-861; Polémica en los Estados Unidos por la utilización de datos personales con fines comerciales, por Leonardo Geri, ED, 261-897. Todos los artículos citados pueden consultarse en www.elderecho.com.ar.

(**) El autor es abogado especialista en Derecho de Alta Tecnología por la Universidad Católica Argentina, y es magíster (LLM) en Derecho de las TIC por las Universidades de Hannover (Alemania) y Oslo (Noruega).

(1) Anzit Guerrero, Ramiro - Tato, Nicolás - Profumo, Santiago, El derecho informático. Aspectos fundamentales, Buenos Aires, Cathedra Jurídica, 2010, pág. 19.

(2) Para un análisis pormenorizado de los contratos de adhesión, ver Fariña, Juan M., Defensa del consumidor y del usuario, Buenos Aires, Astrea, 2008, págs. 434/439.

(3) Es importante destacar que para el presente análisis se tendrán en cuenta principalmente los "Términos y Condiciones" de Facebook, Twitter y LinkedIn, por ser las redes sociales más populares.

(4) Un buen ejemplo de redacción clara de estas cláusulas lo podemos encontrar en la red social española Tuenti. En la actualidad, tal política dispone: "Al publicar contenidos en tu perfil –fotos, archivos, textos, vídeos, sonidos, dibujos, logos o cualquier otro material– conservas todos tus derechos sobre los mismos y otorgas a TUENTI una licencia limitada para reproducir y comunicar públicamente los mismos, para agregarles información y para transformarlos con el objeto de adaptarlos a las necesidades técnicas del Servicio. Esta autorización es mundial, no exclusiva (lo que significa que puedes

otorgar otra licencia sobre tu contenido a cualquier persona o entidad, además de a TUENTI), por todo el tiempo que tengas vigente tu perfil y con la única y exclusiva finalidad de que TUENTI pueda prestarte el servicio en los términos explicados en estas Condiciones de uso. "La anterior licencia quedará resuelta una vez que elimines tu contenido del Servicio o des de baja tu perfil. A partir de ese momento, TUENTI interrumpirá la comunicación de tu contenido a la mayor brevedad posible. "En relación con el contenido que publiques en el Servicio, garantizas: "- Que eres el propietario o titular de los derechos que te permiten conceder a TUENTI la licencia para su publicación y que, en su caso, has obtenido de terceros el consentimiento necesario para ello. "- Que no vulnera leyes aplicables tales como las relativas al derecho a la intimidad, a la imagen y/o al honor, derechos de propiedad intelectual o industrial o similares ni ningún derecho de un tercero, ya sea una persona o una entidad. "- Que en caso de que publiques datos de carácter personal de alguno de tus amigos o de otra persona, les has informado y obtenido previamente su consentimiento para la publicación de dichos datos. "Por ello, responderás frente a TUENTI de la veracidad de lo afirmado, manteniendo indemne a TUENTI ante cualquier demanda o reclamación presentada por un tercero en relación a las anteriores afirmaciones y en relación a cualquier derecho legítimo sobre el contenido que hayas publicado en el Servicio".

(5) Tan en boga se encuentran estos conceptos que, de hecho, el art. 25 del flamante Reglamento General de Protección de Datos (Reglamento [UE] 2016/679 del Parlamento Europeo y del Consejo del 27-4-16, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE) establece las obligaciones del controlador en el procesamiento de datos personales de acuerdo con los principios de protección desde el diseño y por defecto.

(6) Un buen ejemplo de ello puede encontrarse en la "Política de Privacidad" de Twitter cuando se estipula lo siguiente: "Nuestros Servicios están principalmente diseñados para ayudarle a compartir información con el mundo. La mayoría de la información que usted nos facilita a través de los Servicios de Twitter es información que nos está pidiendo que hagamos pública. Su información pública incluye los mensajes que usted twittea; los metadatos facilitados con los Tweets, tales como cuándo ha twitteado y la aplicación cliente que utilizó para twittear; el idioma, el país y la zona horaria asociados a su cuenta; y las listas que crea, las personas a las que sigue, los Tweets que retwittea o marca como Me gusta, y muchas otras informaciones que se generan mediante su uso de los Servicios de Twitter".

(7) En este sentido, la "Política de Protección de Datos" de Twitter establece: "Estos otros proveedores de servicios pueden recoger información enviada por su navegador como parte de una petición de una página web, como por ejemplo cookies o su dirección IP. Es posible que nuestros socios comerciales compartan información con nosotros, como un ID de cookies del navegador o el hash criptográfico de un identificador de cuenta común (como una dirección de correo electrónico) para ayudarnos a evaluar la calidad de los anuncios y a personalizarlos".

(8) Por tecnologías similares, debe entenderse a aquellas que tienen por objeto recolectar datos adicionales de uso de un sitio web, tales como los llamados "etiquetas de pixel" o "almacenamiento local". Conforme a la "Política de Privacidad" de Facebook, se denominan "etiquetas de píxel" (o web beacons o gifs o web bugs) a aquellas líneas de códigos (generalmente añadidas en imágenes de un píxel) incluidas en sitios web, utilizadas para el rastreo y el seguimiento de las acciones de los usuarios que visitan dichas páginas. Por otra parte, el "almacenamiento local" es una técnica –similar a las cookies permanentes– que permite a las páginas web y aplicaciones almacenar y acceder a gran cantidad de información de las computadoras, teléfonos móviles o dispositivos del usuario a partir de los navegadores que este utiliza. La gran diferencia respecto de las cookies es el tamaño que cada navegador permite almacenar: 4 kilobytes para las cookies

y entre 5 y 25 megabytes para el almacenamiento local, dependiendo de cada navegador.
(9) Cf. Uicich, Rodolfo D., El derecho a la intimidad en Internet y en las comunicaciones electrónicas, Buenos Aires, Ad-Hoc, 2009, pág. 82.
(10) La LPDP define en su art. 2º a los datos personales como "Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"; es complementario de esta definición la aclaración de que no habrá datos personales si hay una disociación de datos, entendiendo por ello a "todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable".
(11) En virtud del art. 44 de la LPDP, "las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional".
(12) Es recomendable la lectura de la Sentencia del Tribunal de Justicia Europeo del 13-5-14 en el Asunto C-131/12, "Google Spain, S.L., Google Inc. c. Agencia Española de Protección de Datos (AEPD)", en el cual se analiza la cuestión del derecho al olvido en los buscadores de Internet. Tal fallo se encuentra disponible al 18-5-16 en español en http://curia.europa.eu/juris/document/document_print.jsf?doclang=ES&docid=152065.
(13) CNCiv., sala G, "Svatzky, Betina L. c. Datos Virtuales S.A. s/hábeas data", 28-4-04. El mismo criterio ha sido ratificado por la Corte Suprema, el 30-12-04, en los mismos autos de referencia. Puede consultarse el texto del fallo en http://www.jus.gov.ar/scripts/dnpdp-jurisprudencia/im_verpag.asp?ID=161, consultado el 18-5-16.