LA PRIVACIDAD DE LOS DATOS EN LAS REDES SOCIALES

Dra. Esc. Prof. María José Viega(*)

1. Introducción

En la 30º Conferencia Internacional de Protección de Datos se hizo un interesante planteo sobre las redes sociales, el cual comenzó diciendo: "Mi nombre es Clara, tengo 14 años, aquí está mi vida privada, mis logros". El caso planteado relata que todos los días después de la escuela Clara se conecta a Internet, se ha registrado en Facebook, su primo –en cambio- ha preferido MySpace. En este sitio, ella no duda en poner fotos de sus últimas vacaciones con sus amigas en la playa, sus actores y cantantes favoritos. Ella participa en concursos y revela sus gustos de vestimenta, ocio, etc. Ella está registrada en la red social de su escuela, pero también en otras. En su perfil ha expresado su interés en los hombres y tiene más de 100 usuarios como sus amigos. Ella pertenece a una treintena de grupos, incluso ha creado un grupo sobre su profesora de matemáticas a quien considera realmente anticuada, los chats con sus amigos en el "muro", a los cuales les dice lo que está haciendo en este momento. Ella comenzó a interesarse en política, expresó sus puntos de vista y se inscribió con el grupo de seguidores de su político favorito[1].

"Estar en Facebook o MySpace": lo que es más natural ahora, lo que es más "hip"! Además, es libre y se puede decir lo que quiera, conocer gente nueva, hacer muchos amigos, sin sus padres detrás de ella. Pero Clara es consciente de que ella está entregando gradualmente, a todo el mundo, parte de su vida íntima, datos que serán almacenados durante años, que la información que le

---

(*)Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UDELAR). Directora de la Dirección de Derechos Ciudadanos de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC). Directora del Instituto de Derecho Informático (UDELAR) y Coordinadora del Grupo de Jurisprudencia del mismo Instituto. Profesora de Informática Jurídica, Derecho Informático y Derecho Telemático (UDELAR). Ex - Profesora de Derecho de las Telecomunicaciones en Universidad de la Empresa. Cursos del Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Miembro Honorario de la Asociación Paraguaya de Derecho Informático y Tecnológico. Miembro de la International Technology Law Association. Miembro de LA International Association of Privacy Professionals (IAPP). Miembro del Colegio de Abogados del Uruguay y de la Comisión de Derecho Tecnológico de la Asociación de Escribanos del Uruguay. Miembro del Instituto de Derecho Informático (UDELAR) y Coordinadora del Grupo de Jurisprudencia del mismo Instituto. Co-editora del Boletín Electrónico de Derecho y Tecnologías (www.viegasociados.com). Autora de múltiples trabajos de su especialidad y conferencista a nivel nacional e internacional.

[1] Informe sobre la asistencia a la 30th International Conference of Data Protection and Privacy Commissioners “Protecting Privacy in a Borderless World”. Publicado en Derecho informático Tomo IX. Fundación de Cultura Universitaria. Montevideo, 2009. Página 432.

regala cada día en su sitio favorito puede ser usado para determinar sus gustos, sus hábitos de consumo, su comportamiento y que todos estos datos permitirán definir un perfil de marketing. Que su identidad puede ser utilizada por personas desconocidas que no tengan propósitos muy loables, y si ella ha dado su dirección, sus fotos, algunas personas podrían intentar contactar con ella. ¿Qué pasaría si, en un plazo de cinco años, un empleador descubriera esta información y le pregunte acerca de ella? ¿Ella lee y entiende la política de privacidad del sitio? ¿Qué significa la protección de los datos para ella? ¿Entiende que podría restringir el acceso a su información? ¿Le han sido dados los medios para eliminar sus datos si así lo desea?

La labor educativa debe realizarse rápidamente a los más jóvenes, que son poco conscientes de los riesgos inherentes a la utilización de Internet. Si no se hace nada hoy en día, las generaciones futuras podrían reclamar mañana que su privacidad no está segura. ¿Cómo perciben los jóvenes su vida privada en Internet? ¿Y los riesgos potenciales de daños a su esfera privada? ¿Cómo hacer entender a los jóvenes la protección de datos? ¿Deben llevarse a cabo campañas de sensibilización? ¿Los propietarios de sitios web tienen una responsabilidad especial en este sentido? ¿Son conscientes de eso? ¿Cuál es su percepción sobre estas cuestiones? ¿Debemos y podemos regular la difusión de sus datos por parte de los menores en Internet?

Vemos entonces, que los datos personales publicados on line por un usuario, y sus relaciones con otras personas, puede crear un perfil muy preciso de sus intereses y actividades. Y éstos pueden ser utilizados por terceros con distintos fines, generalmente comerciales, pero también representar riesgos, como la usurpación de identidad, pérdidas económicas o posibilidades de empleo, o ataques a la integridad física.

El Grupo 29 de la Directiva de la Unión Europea de Protección de Datos entiende que: “Los Sitios Redes Sociales (SRS) pueden definirse generalmente como plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes. En sentido jurídico, las redes sociales son servicios de la sociedad de la información, según se definen en el artículo 1, apartado 2, de la Directiva 98/34/CE, modificada por la Directiva 98/48/CE. Los SRS comparten determinadas características:

- los usuarios deben proporcionar datos personales para generar su descripción o «perfil»;

- proporcionan herramientas que permiten a los usuarios poner su propio contenido en línea (contenido generado por el usuario como fotografías, crónicas o comentarios, música, vídeos o enlaces hacia otros sitios);

- las «redes sociales» funcionan gracias a la utilización de herramientas que proporcionan una lista de contactos para cada usuario, con las que los usuarios pueden interactuar.

Los SRS generan la mayoría de sus ingresos con la publicidad que se difunde en las páginas web que los usuarios crean y a las que acceden. Los usuarios

que publican en sus perfiles mucha información sobre sus intereses ofrecen un mercado depurado a los publicitarios que desean difundir publicidad específica y basada en esta información".

Mr. Jacques Barrot señaló en la Conferencia de Estrasburgo de 2008 que Eurobarómetro realizó encuestas respecto a los jóvenes que determinaron que los niños saben más que los padres en relación a Internet. En las escuelas deberían hacerse presentaciones a los niños explicándoles que sucede cuando sus datos llegan al ciberespacio. Destaca la labor del G29 sobre protección de los niños en el contexto escolar. Los bancos de datos, operadores tecnológicos y autoridades judiciales tienen que trabajar conjuntamente[2].

Es claro entonces, que la falta de conciencia vinculada al tema no alcanza solo a los niños, sino a todas las personas. Entiendo que los niños tienen otra perspectiva de ver esta nueva realidad. La información que se coloca en las redes sociales se hace en un contexto particular, y probablemente, quienes analicen estos contenidos, lo harán con la misma mirada de quien lo escribió, lo que disminuye ciertos riesgos. Pensemos que los nativos digitales crecen en un mundo diferente al de nuestra infancia, que no lo conciben sin el teléfono celular o sin Internet.

Mr. Leif Stenström comentó –también en la Conferencia de Estrasburgo- que realizaron una encuesta con 125 preguntas a jóvenes menores de 25 años, de la cual surge que el 98 % utilizan las redes una vez por semana y el 85 % una vez al día. Cada semana se reciben 1500 denuncias por Internet. Cada segundo, uno de cada 3 personas han encontrado fotos publicadas sin permiso y uno de cada 5 ha sido acosado sexualmente en Internet. La información no es la clave para eliminar el riesgo. Hay que cambiar las actitudes de las personas. Esto no se logra repartiendo folletos. Vamos a las escuelas y damos charlas, hacemos juegos, encuestas. Hay que tener cuidado con las campañas porque se corre el riesgo que a los niños o jóvenes les parezca aburrido. Hay que estar dispuestos a cambiar todos los años porque ellos cambian sus intereses año a año. Para cambiar actitudes hay que comparar las actitudes en líneas con las reales. Se les dice a los niños: mira al cruzar la calle, no hables con extraños, etc. Nos acercamos a los padres, a los profesores, porque creo que los actores deberían asumir su responsabilidad. Hay muchísimas organizaciones que pueden verse implicadas. La seguridad de los niños es importante, pero sería importante construir polos integrados por distintos tipos de personas, hay que tener en cuenta que la responsabilidad no es solo de las agencias[3].

Con relación a este tema encontramos documentos de mucha relevancia, de los cuales mencionaremos los siguientes:

1. El Grupo Internacional sobre protección de datos en las Telecomunicaciones de Berlín, plasmó este problema en su reunión de 4 de marzo de 2008 con la

[2] Informe sobre la asistencia a la 30th International Conference of Data Protection and Privacy Commissioners "Protecting Privacy in a Borderless World". Ob. Cit.
[3] Informe sobre la asistencia a la 30th International Conference of Data Protection and Privacy Commissioners "Protecting Privacy in a Borderless World". Ob Cit.

aprobación del “Memorándum de Roma”, y destacó que uno de los desafíos es que la mayoría de la información que se publica en las redes sociales se hace bajo la iniciativa de los usuarios y basado en su consentimiento[4].

2. ENISA (*European Network and Information Security Agency*). “Los niños en los mundos virtuales: lo que los padres deberían saber”, publicado en septiembre de 2008, y que aporta una serie de Recomendaciones a los padres, resaltando la necesidad de formar y educar tanto a progenitores como a los niños[5].

3. El Parlamento Europeo, en el 2009 aprobó el programa *Safer Internet*, dirigido a abarcar los temas relacionados con el uso seguro de Internet por parte de los niños y las nuevas tecnologías.

4. El Grupo de trabajo del artículo 29 (G29), en su Dictamen 5/2009, de 12 de junio sobre redes sociales en línea, manifestó que si un dato personal es cualquier información relativa a una persona física identificada o identificable, en las redes sociales, todo son datos personales. Así, el G29 es muy claro: a las redes sociales les será de aplicación muchas de las previsiones comunitarias sobre la materia, incluso si los proveedores de servicio están ubicados fuera del territorio español. Y a esta conclusión se llegó también en la 30ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad de 2008 celebrada en Estrasburgo.

5. Estudio sobre la privacidad de las personas y la seguridad de la información de las redes sociales on line. Agencia Española de Protección de Datos y el Instituto Nacional de Tecnologías de la Comunicación (INTECO).

6. Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes (Memorándum de Montevideo, de 27 y 28 de julio de 2009), redactado por un grupo de especialistas iberoamericanos en la materia, habiendo tenido la oportunidad de participar en su redacción. El documento establece recomendaciones sobre protección de datos y vida privada, en particular de niños, niñas y adolescentes en las redes sociales en Internet.

Analizaremos a continuación los tres últimos documentos mencionados.

2. Dictamen 5/2009, de 12 de junio sobre redes sociales en línea del Grupo de trabajo del artículo 29 (G29).

El dictamen distingue diferentes situaciones. Por un lado, los usuarios que publican en sus perfiles mucha información sobre sus intereses, permitirá crear un perfil específico a la hora de enviarle publicidad. Por otra parte, si un usuario decide, con perfecto conocimiento de causa, ampliar el acceso más allá de los

[4] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf
[5] http://www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf.

«amigos» elegidos, asume las responsabilidades de un responsable del tratamiento de datos.

El G29 entiende que un elemento importante en los parámetros de confidencialidad es el acceso a los datos personales publicados en un perfil. Las restricciones al acceso impiden que cualquier persona tenga acceso a datos íntimos de un usuario, ya sea a través de las redes sociales o inclusive de motores de búsqueda. El punto es relevante en la medida que solo una minoría de usuarios modifican los parámetros de privacidad, que en su configuración original dejan abierta la información.

“Los perfiles de acceso limitado no deberían ser localizables por los motores de búsqueda internos, incluso por la función de búsqueda por parámetros como la edad o el lugar. Las decisiones de ampliar el acceso pueden no estar implícitas, por ejemplo mediante la posibilidad de exclusión voluntaria proporcionada por el responsable del SRS”.

El documento hace hincapié en que los proveedores de SRS deberían informar a los usuarios de su identidad y de los distintos fines para los que tratan los datos personales, de conformidad con las disposiciones del artículo 10 de la Directiva relativa a la protección de datos sobre:

- la utilización de los datos con fines de comercialización directa;

- la posible distribución de datos a categorías específicas de terceros;

- una reseña de los perfiles: su creación y sus principales fuentes de datos;

- la utilización de datos sensibles.

El Grupo de Trabajo recomienda que:

- los proveedores de SRS adviertan adecuadamente a los usuarios sobre los riesgos de ataque a su intimidad y a la de otros cuando ponen información en línea en los SRS;

- los SRS recuerden a sus usuarios que poner en línea información relativa a otras personas puede perjudicar su derecho a la intimidad y a la protección de datos;

- los SRS aconsejen a sus usuarios que no pongan en línea fotografías o información relativa a otras personas sin el consentimiento de éstas.

Respecto a los datos sensibles se hace énfasis en que sólo pueden publicarse en Internet con el consentimiento explícito de la persona interesada o si esta misma persona ha hecho públicos estos datos.

“En algunos Estados miembros de la UE, las imágenes de personas se consideran una categoría especial de datos personales, puesto que pueden utilizarse para distinguir entre el origen racial o étnico o para deducir sus

creencias religiosas o datos relativos a la salud. El Grupo de Trabajo no considera, en general, que las imágenes en Internet sean datos sensibles, salvo si se utilizan claramente para revelar datos sensibles sobre las personas".

El dictamen refiere a los tratamiento de datos de no miembros, porque en las redes sociales se puede proporcionar datos sobre otras personas, etiquetar fotografías, o dar información sobre amigos o conocidos para realizar una búsqueda, proporcionar correos electrónicos de terceros, etc.

No es posible que el proveedor de los sitios de redes sociales envíe mensajes de correo electrónico por ningún motivo, ya que violaría el artículo 13, apartado 4, de la Directiva sobre la privacidad y las comunicaciones electrónicas, relativa al envío de mensajes electrónicos no solicitados con fines de comercialización directa.

También se hace referencia a las aplicaciones realizadas por terceros, se entiende que se debe informar a los usuarios clara y específicamente acerca del tratamiento de sus datos personales y que sólo se les permita el acceso a los datos personales necesarios.

3. Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales on line. AGPD e INTECO.

Este documento parte del análisis de que existen posibles situaciones de riesgo para la protección de la intimidad:

1. En el momento del registro de alta como usuario, en la medida en que no sea configurado correctamente el nivel de privacidad del perfil, así como por el hecho de que sea publicada información sensible desde el inicio de la actividad en la red.

2. En el momento de participación en la red como usuario, en la medida en que el grado de información, datos e imágenes publicados pueden ser excesivos y afectar a la privacidad, tanto personal como de terceros.

2.1 *Respecto a la privacidad personal*: a pesar de que sean los usuarios los que voluntariamente publican sus datos, los efectos sobre la privacidad pueden tener un alcance mayor al que consideran en un primer momento ya que estas plataformas disponen de potentes herramientas de intercambio de información facilitada por los usuarios.

2.2 *Respeto a la privacidad de terceros*: es esencial que los usuarios tengan en cuenta que la publicación de contenidos con información y datos respecto a terceros no puede ser realizada si éstos no han autorizado expresamente su publicación, pudiendo solicitar su retirada de forma inmediata.

Es importante tener en cuenta que las redes sociales permiten a los motores de búsqueda de Internet indexar en sus búsquedas los perfiles de los usuarios, junto con información de contacto y de perfiles de amigos, lo que puede

suponer otro riesgo para la protección de la privacidad, además de dificultar el proceso de eliminación de su información en Internet.

3. En el momento de darse de baja de la plataforma en la medida en que el usuario solicita dar de baja su perfil, pero aún así continúan datos publicados por éste, o información personal e imágenes propias publicadas en los perfiles de otros usuarios.

Es necesario destacar que el derecho a la protección de los datos de carácter personal supone el "derecho a controlar el uso que se realice de sus datos personales, comprendiendo, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención"[6].

El documento considera situaciones de riesgo para la protección de los datos de carácter personal:

Phishing

Los ataques de estafa a través de Internet por el método "phishing", que significa "pesca" en el argot informático, se han ido incrementando. El sistema más utilizado por los cyber-estafadores es el envío de correos electrónicos con falsos remitentes, como por ejemplo de entidades financieras, de forma tal que las víctimas cliquearan en un link y de esa forma podían obtener información personal[7].

En junio de 2005, se celebró en las instalaciones de la Dirección General de la Policía en Madrid unas jornadas sobre fraude en Internet, concretamente sobre phishing bancario. Se ha definido al phishing como "un acto de crimen organizado, y como tal debe ser tratado, que los actores que participan en el escenario del fraude tienen todos su porción de responsabilidad y que es preciso transmitir y recordar a los usuarios de banca electrónica que no deben desconfiar del canal bancario electrónico, sino que deben ser conscientes de que han de contemplarse medidas preventivas para evitar ser víctimas de los engaños. La banca electrónica es, salvo excepciones extraordinarias, seguras y confiables[8].

Pero ya se habla de una nueva generación de phishing. Hispasec[9] demuestra cómo es posible realizar ataques phishing en servidores seguros de entidades bancarias, aun cuando el usuario visualice que la URL comienza por https:// seguido del nombre de la entidad y que el icono del candado que aparece en la

[6] Sentencia del Tribunal Constitucional Nº 292/2000, que reconoce el Derecho a la Protección de Datos como un derecho fundamental absolutamente independiente del Derecho al Honor, Intimidad y Propia Imagen.
[7] VIEGA, María José. "El problema de los datos personales y el espionaje en Internet", presentada al Cuarto Congreso Internacional de Derecho (CIDER 2005) en las Sedes de Cochabamba, Santa Cruz y La Paz. Bolivia, 23 al 25 de noviembre de 2005. Publicada en el Libro de Ponencias.
[8] http://www.hispasec.com/unaaldia/2421 Página visitada 13 de junio 2005.
[9] http://www.hispasec.com/unaaldia/2406 Página visitada 13 de junio 2005.

parte inferior del navegador certifique que se encuentra en el servidor seguro del banco, lo que constituían hasta el momento las recomendaciones que se hacían para acceder de forma segura a la banca electrónica[10].

Como podemos ver esto se ha vuelto inseguro y el Pharming es la confirmación de esta afirmación.

Pharming[11]

Es una modalidad de fraude online, que ataca la vulnerabilidad del software de los servidores DNS o de los equipos de los propios usuarios, redireccionando el nombre de dominio a un sitio web falso, diseñado por el atacante.

El pharming deriva del término *farm* (granja en inglés), expresión utilizada cuando el atacante ha conseguido acceso a un servidor DNS o varios servidores (granja de servidores o DNS).

Esta modalidad delictual se utiliza normalmente para realizar ataques de *phishing*, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos personales del usuario, generalmente datos bancarios.

Si el phishing engaña a los usuarios uno por uno, conduciéndolos a visitar un sitio apócrifo de su banco o comercio preferido, el pharming interviene las comunicaciones entre el usuario y su proveedor de Internet (ya sea un proveedor de comunicaciones, o un servidor corporativo) para lograr que cuando un usuario teclea en su navegador una dirección legítima, éste sea conducido a una falsificación de la página Web que quiere visitar y sea ahí donde introduzca los datos de su cuenta[12].

Por tanto, el riesgo para el usuario en los casos de pharming es diferente, mientras que en el phishing requiere una actitud activa, hacer click en el link del correo electrónico, en el pharming el fraude se produce sin participación directa del usuario.

La utilización de medidas técnicas de seguridad en un sistema, como por ejemplo un firewall, herramientas de protección contra adware y spyware, contrarrestan este tipo de amenazas.

La finalidad de ambas conductas delictivas es la captura ilegítima de datos confidenciales, difiriendo en el modo de ejecutarlo.

---

[10] VIEGA, María José. "Privacidad Vs. Espionaje en Internet". Anuario de "Derecho Informático". Tomo VI Jurisprudencia correspondiente al año 2005 y en el Boletín de Derecho y Tecnologías Nº 16 Enero 2005 http://viegasociados.com/moodle//mod/forum/discuss.php?d=440

[11] VIEGA, María José y CARNIKIAN Federico. "Respuestas a los delitos informáticos: su visión desde la privacidad y la seguridad de la información.

[12] http://www.mx.terra.com/tecnologia/interna/0,,OI889426-EI4906,00.html Página visitada 21 de junio de 2010. El Pharming: amenaza de fraude a negocios. Trend Micro. 21 de febrero de 2006.

El pharming se realiza modificando el software, lo cual puede realizarse en forma remota o introduciendo un programa que lo realice en forma automática. Para ello es necesario introducir un troyano en el disco duro de la víctima, el cual puede autoeliminarse, borrando del disco duro las huellas del ataque.

"La respuesta es muy delicada para el banco, si hace responsable al cliente y el "pharming" se generaliza, los usuarios abandonaremos en masa la banca online por insegura y peligrosa, pero si el banco carga con los gastos. ¿A cuánto tendrá que subir las comisiones por operación el banco online para cubrir este riesgo? ¿Seguirá siendo competitivo? Si no se atajan estos riesgos, quizá el porvenir de la e-banca no sea después de todo tan brillante como se auguraba"[13].

Social Spammer y spam. Utilización de las redes sociales como plataformas para el envío de correo electrónico no deseado.

Indexación no autorizada por parte de buscadores de Internet.

Acceso al perfil incontrolado. La mayoría de las redes sociales analizadas disponen del perfil completo del usuario, o al menos de parte de este, en formato público, de forma que cualquier usuario de Internet o de la red social puede acceder a información de carácter personal ajena sin que el propietario de los datos tenga que dar su consentimiento expreso.

Suplantación de identidad. Cada vez es más frecuente que usuarios que nunca se habían registrado en redes sociales online, comprueben como en el momento en que intentan acceder, su "identidad digital", ya está siendo utilizada".

El Memorándum de Montevideo dice que: "La participación anónima o con seudónimo hace posible la suplantación de identidad".

Publicidad hipertextualizada. Esta aporta, a priori, una ventaja para los usuarios, ya que con ella evitan que se muestren durante su navegación contenidos, para ellos, irrelevantes e incluso ofensivos. Sin embargo, desde el punto de vista legal podría considerarse una práctica ilegal, ya que para poder contextualizar la publicidad que se va a mostrar a un usuario se tienen que examinar sus datos y preferencias.

Instalación y uso de "cookies" sin consentimiento del usuario. A través de las cookies las redes sociales pueden saber el lugar desde el que usuario accede (fijo o móvil), el sistema operativo utilizado, los sitios más visitados dentro de una página web, el número de clicks realizados, y otros datos relativos al usuario dentro de la red.

[13] http://www.laflecha.net/canales/seguridad/articulos/pharming/ El Pharming, un peligro para la e-banca. Página visitada 21 de junio de 2010.

4. Memorándum de Montevideo de 28 de julio de 2009

"El derecho a la vida privada es un valor que toda sociedad democrática debe respetar. Por tanto para asegurar la autonomía de los individuos, decidir los alcances de su vida privada, debe limitarse el poder tanto del Estado como de organizaciones privadas, de cometer intromisiones ilegales o arbitrarias, en dicha esfera personal"[14].

El documento divide las recomendaciones para:

a. Los Estados y Entidades Educativas para la prevención y educación de niñas, niños y adolescentes.

El artículo 16 de la Convención de Naciones Unidas sobre los Derechos del Niño (CDN) determina que: "(1) Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación. (2) El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".

Se recomienda tener en cuenta el rol de los progenitores o personas que tengan niñas, niños y adolescentes a su cuidado; toda medida que implique control de las comunicaciones tiene que respetar el principio de proporcionalidad y en tercer lugar, que se debe transmitir claramente a las niñas, niños y adolescentes que Internet no es un espacio sin normas, impune o sin responsabilidades.

b. Los Estados sobre el marco legal. El marco legal avanza lentamente en comparación con el desarrollo de nuevas aplicaciones y contenidos. Los Estados requieren el desarrollo de una normativa de protección de datos, aplicable al sector público y privado. Es importante destacar que Uruguay cumple con los estándares internacionales en protección de datos.

c. La aplicación de las leyes por parte de los Estados. Los sistemas judiciales tienen un rol muy relevante en el aseguramiento de un buen uso de Internet y las redes sociales digitales.

Se debe garantizar que existan procesos judiciales y administrativos sencillos, agiles, de fácil acceso. En Uruguay la Ley Nº 18.331 consagró la Acción de Habeas Data con las características mencionadas.

Dice el Memorándum en el punto 10.3: "Debería desarrollarse y difundirse una base de datos sobre casos y decisiones (fallos judiciales o resoluciones administrativas anonimizadas) vinculada a la Sociedad de la Información y el Conocimiento, en especial a Internet y las redes sociales digitales, que sería un instrumento para que los jueces puedan apreciar el contexto nacional e internacional en el que están decidiendo".

[14] Memorándum de Montevideo. Publicado por IFAI y IIJusticia.

El Instituto de Derecho Informático y Agesic han desarrollado una base de datos de jurisprudencia nacional de derecho informático, que ha sido un esfuerzo muy importante de ambas instituciones y especialmente del Grupo de Jurisprudencia del Instituto.

Fomentar el establecimiento de organismos judiciales especializados en protección de datos. Si bien, esto no ha sucedido en nuestro país, si ha creado la Unidad Reguladora y de Control de Datos Personales, que se especializa en el tema en el ámbito administrativo y es el órgano garante a nivel nacional del cumplimiento de las normas de protección de datos.

d. En materia de políticas públicas. Se recomienda considerar la implementación de las siguientes políticas públicas:

- Establecer mecanismos de respuesta para atención a las víctimas de abusos en la Sociedad de la Información y el Conocimiento.

- Establecer sistemas de información en línea, con número telefónicos gratuitos, centros de atención, etc.

- Elaboración de protocolos para canalizar los contenidos ilegales reportados.

- Deberían existir mecanismos regionales e internacionales para compartir la información reportada sobre la temática.

- Promover acciones de sensibilización y divulgación de información a través de medios de comunicación masivos.

- Promover el compromiso y la participación de asociaciones públicas y privadas.

- Impulsar la generación de conocimiento especializado con el fin de elaborar políticas públicas adecuadas.

e. La industria. Las empresas que proveen los servicios de acceso a Internet, desarrollan las aplicaciones o las redes sociales digitales deben comprometerse con la protección de los datos personales y la vida privada y cooperar con los sistemas de justicia, desarrollar códigos de conducta, etc.

Estos códigos de conducta no deberían permitir la recopilación, tratamiento, difusión, publicación o transmisión a terceros de datos personales, sin el consentimiento explícito de la persona concernida. En los casos de niñas, niños y adolescentes se deberá considerar la prohibición de tratamiento de datos personales.

Las reglas de privacidad de las páginas web deben ser explícitas, sencillas y claras, debiéndose informar sobre los propósitos y finalidades para los cuales se utilizarán los datos; indicando también la persona o personas responsables del tratamiento de la información.

La red social debe indicar explícitamente lo que refiere a publicidad, indicando que las informaciones personas de los perfiles de los usuarios se emplean para enviar publicidad.

Deben implementarse mecanismos para la verificación fehaciente de la edad.

Toda red social digital debería contar con formas de acceso a la información, rectificación y eliminación de datos personales para usuarios o no usuarios.

Deben suprimirse totalmente los usuarios que han desactivado su cuenta, tras un período razonable.

Debe también eliminarse la información de aquellas personas que no son usuarios y han sido invitados a ser parte de las redes sociales digitales y estas no deben utilizar esa información.

En el numeral 25 se establece que “Debe impedirse la indexación de los usuarios de las redes sociales digitales por parte de los buscadores, salvo que el usuario haya optado por esta función. La indexación de información de niñas y niños debe estar prohibida en todas sus formas, en el caso de adolescentes éstos deben autorizar de forma expresa la indexación de sus datos mínimos”.

5. Conclusiones

En el Diario El País del día de ayer, 17 de agosto de 2010, se publicó una nota de prensa titulada: “Los uruguayos son poco cuidadosos de los datos que publican en Internet”, por la cual se informa que Microsoft presentó los resultados de la encuesta "Cómo usan padres e hijos Internet en los hogares uruguayos" y se muestran los siguientes resultados:

63% - conoció personalmente a un contacto con el que sólo tenía relación en la red

67% - comparte información en redes sociales, como facebook y twitter

27% - tienen configurado su perfil "Amigos de de mis amigos" o "Todos" puedan verlo

80% - no se usa ningún filtro para contenidos, ya que muchos desconocen que existen

32% - reconoció haber dado información personal falsa

21% - abandonó una conversación en la que se le solicitaba datos

Pero hay que tener presente aquellos casos en que el usuario de la red social consintió a que sus datos fueran publicados y utilizados con una finalidad, y los están utilizando con otra finalidad completamente distinta.

Los problemas también se plantean en cuanto a los contenidos. A pesar de que la normativa sobre propiedad intelectual y derechos de autor es clara, en la práctica prima el "libre" intercambio de información.

En este punto hay que analizar cómo se tratarán los contenidos de las redes sociales, pues la mayoría de esta información se proyecta sobre la actividad y preferencias de sus titulares. De esta forma, la información de los usuarios de las redes sociales tiene un valor inestimable: se transforman en un verdadero "oro rosa" (como lo llama LAIMÉ, 2001)[15].

Sin lugar a dudas, el anhelo en Internet es la publicidad personalizada, existiendo en la actualidad muchas empresas que construyen bases de datos que recogen nuestras costumbres, gustos, sitios de interés, domicilio, datos familiares, etc.

Pero no solo interesa el perfil del usuario, que le convierte en un objetivo concreto al que difundir la publicidad, sino la información relativa a terceros.

En estos casos, no deja de ser frecuente, que una gran mayoría de usuarios de redes sociales publiquen información sobre conocidos y sin el previo consentimiento de éstos. Aquí tenemos que decir que la Agencia Española de Protección de Datos ha sancionado, en más de una ocasión, a personas que han colgado fotos o imágenes de tercero sin el consentimiento de éstos, como por ejemplo, el Procedimiento sancionador 000617/2008[16].

Uno de los mayores problemas de las redes sociales es el tema de los menores, enfrentándose a problemas que pueden superar las ventajas que estas redes ofrecen.

Proteger la vida privada en el ámbito de las redes sociales hace necesario un cambio en la interpretación, adecuación y fortalecimiento de la protección de datos personales existente hasta el momento. Porque el mayor peligro es la falta de conciencia de cada uno de nosotros, ya que "cedemos" o "vendemos" nuestra privacidad, sin conocer cuál será el real manejo de la información que estamos brindando.

---

[15] ARENAS RAMIRO Mónica. Profesora Ayudante Doctor del Área de Derecho Constitucional de la Universidad de Alcalá de Henares (Madrid). "Redes sociales, ¿un virus sin cura?: las ventajas y los problemas para sus usuarios". http://www.madrid.org/cs/Satellite?c=CM_Revista_FP&cid=1142581421779&esArticulo=true&idRevistaElegida=1142576007987&language=es&pag=2&pagename=RevistaDatosPersonales%2FPage%2Fhome_RDP&siteName=RevistaDatosPersonales Página visitada 14 de agosto de 2010.

[16] ARENAS RAMIRO Mónica. Profesora Ayudante Doctor del Área de Derecho Constitucional de la Universidad de Alcalá de Henares (Madrid). "Redes sociales, ¿un virus sin cura?: las ventajas y los problemas para sus usuarios". Ob. Cit.

Pero no podemos perder de vista que las redes sociales se encuentran sometidas a la normativa sobre protección de datos personales, en el caso uruguayo, a la Ley Nº 18.331 y sus decretos reglamentarios.

Montevideo, agosto de 2010