Instituto de Investigaciones Gino Germani
VII Jornadas de Jóvenes Investigadores
6, 7 y 8 de noviembre de 2013
Ezequiel Passeron (UBA)
epasseron@gmail.com
Eje 11: Estado y políticas públicas

Protección de datos personales en redes sociales y webs 2.0

Perez Luño en su libro “Derechos Humanos, Estado de derecho y Constitución” afirma que: “las *sociedades actuales precisan de un equilibrio entre el flujo de informaciones, que es condición indispensable de una sociedad democrática* y *exigencia para la actuación eficaz de los poderes públicos, con la garantía de la privacidad de los ciudadanos. Ese equilibrio precisa de un -Pacto social informático-”* (2010, p.361)

Desde el año 2000, la Argentina cuenta con la **Ley N°25.326** sobre Protección de los Datos Personales, también conocida como la “Ley de Hábeas Data”. La misma fue reglamentada por el **Decreto 1558/01**. En la reforma del año 1994, la Constitución Nacional en su Artículo 43 preveía la acción de habeas data: *“Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley”* (1994,art. 43). Desde allí, se constituyó el marco jurídico sobre esta temática.

La ley 25.326 asegura la protección integral de datos personales asentados en archivos, registros, bancos de datos u otros, sean estos públicos o privados. Su función es la de garantizar el derecho al honor y a la intimidad de las personas, y también el acceso a la información que sobre las mismas existe. En un principio, el motivo principal que originó la sanción de una ley de esta índole fueron las informaciones crediticias y las violaciones a la intimidad de las personas que se daban, por parte de las entidades financieras.

Pero en la actualidad, el mayor riesgo que afronta la ley no son las violaciones por publicación de información financiera, sino la cantidad de datos personales que existen (ya no solo el nombre, apellido, documento, teléfono, dirección; sino también fotos, videos, emails, y cualquier información que pueda identificar a una persona como tal) y la multiplicidad de plataformas y sitios por donde fluyen. Existe una tendencia hacia la publicación de información en la web (sobre todo con la llegada de las redes sociales, blogs, foros, chats), en donde los usuarios vuelcan gustos, intereses, experiencias, comparten información, suben fotos y videos, etc. En otras palabras, hay una propensión en publicar (volver público) muchísimas cuestiones que antes quedaban reservadas para la vida privada. Esto hace que los parámetros de intimidad y privacidad se modifiquen, generando un desafío enorme para el Estado, para que los derechos de sus ciudadanos se cumplan.

Estos servicios que nos ofrecen las nuevas tecnologías son de gran utilidad, y es necesario alentar el uso de los mismos ya que nos otorgan infinidad de oportunidades como ser un mayor acceso a la información, el achicamiento de las distancias, una comunicación más fluida, etc., pero lo peligroso es la falta de conciencia de que existen riesgos que pueden producirse durante el uso de estas tecnologías. Es necesario por eso informarse y valerse de herramientas de protección para poder gestionar y disminuir los riesgos.

Surge como fundamental entonces contar con espacios de comunicación, información y participación sobre la protección de los datos personales en la web. Ya que la ciudadanía debe estar al tanto de las leyes, sus alcances, y conocer así los derechos que tenemos para poder cuidar nuestra información personal. Estos espacios no solo deben difundir los derechos, deben alentar el uso de las nuevas tecnologías, pero pregonar un uso responsable, conociendo los posibles riesgos y amenazas que existen el mundo de las TIC (Tecnologías de Información y Comunicación).

En Argentina existen distintas políticas públicas referidas al “mundo digital”. Por un lado tenemos “Conectar Igualdad”, un plan diseñado para concretar la entrega de 3 millones de netbooks destinadas a chicos de escuelas secundarias de todo el país. También existe el Plan Sarmiento que entrega computadoras a alumnos de escuelas primarias. Por otro lado, contamos con el Plan Nacional de Telecomunicaciones Argentina Conectada que tiene como finalidad expandir el servicio de banda ancha y TV digital a lo largo de todo el país. El objetivo del programa es la democratización del acceso a la información, comunicaciones y tecnología digital. Sumado a esto, están los NAC (Núcleos de acceso al conocimiento) y PAD (Puntos de acceso digital) que son espacios creados en distintos puntos del país que garantizan un lugar de conexión en donde hay un Microcine, una sala de computadoras y uno de juegos (con Playstation y Wii). Así tenemos garantizados el acceso a los dispositivos, por un lado, y el acceso a la conexión por el otro. Como complementaria a estas políticas se puede situar “Con vos en la web”, iniciativa de concientización acerca de la importancia de la protección de los datos personales. Es decir, un programa que aporta herramientas e información para lograr un uso seguro de las TIC y nuevas tecnologías.

Surge como necesario entonces, alentar el uso de las nuevas tecnologías, aprovechando y explotando al máximo todas sus oportunidades, pero pregonar por un uso responsable y seguro de las mismas, para poder así garantizarnos el cumplimiento de derechos humanos fundamentales, como son la intimidad y la privacidad. Para eso debemos

tomar los cuidados que tenemos en la "vida real" y llevarlos a la "vida virtual", entendiendo así a Internet como perteneciente al espacio de lo público (como una plaza pública). De esta manera podremos romper la falsa percepción de privacidad que genera la web y que hace que sus usuarios piensen que están totalmente seguros y que no corren ningún riesgo en la interacción con estas tecnologías.

En un contexto en donde, por un lado cada vez tenemos mayor conectividad y mayor acceso a los dispositivos digitales, y por el otro no existe una percepción de los riesgos que pueden producirse en la interacción con las nuevas tecnologías es importante, es fundamental crear espacios de comunicación, de información, para tener un correcto uso de Internet y las nuevas tecnologías en general.

La protección de datos personales en Internet

Dentro del libro "Derechos y Nuevas Tecnologías", Gabriel Martinez sostiene que "*El mundo de la comunicación se ha revolucionado en los últimos años merced a la conjunción de las tecnologías informáticas y de las telecomunicaciones. Este fenómeno ha sido denominado "Sociedad de la Información" y tiene como fundamental avance tecnológico la digitalización de la información, lo que permite su almacenamiento en grandes cantidades y su desplazamiento en cuestión de segundos" (2000).*

En la actualidad, la mayoría de los procesos de la vida cotidiana están mediados por Internet. Las actividades comerciales, el ocio y entretenimiento, la investigación y el estudio están condicionados por esta poderosa herramienta. Es quien gobierna el mundo y quien dicta las leyes afirma nuevamente Gabriel Martinez en el mismo libro mencionado anteriormente "*Internet ha sido caracterizada como un conjunto de redes de Protocolo Internet (IP) todas interconectadas entre sí (…) Internet permite a los usuarios examinar archivos, buscar información, enviar mensajes electrónicos y penetrar en ordenadores a grandes distancias" (*2000*).*

Toda la información requerida se encuentra en Internet. Nada escapa al alcance que posee la web. Pablo Palazzi en el libro "El Modelo informático desafía al derecho Antitrust" de Roberto Chacón de Albuquerque lo afirma de la siguiente manera "*La tecnología informática está en todas partes. La información se convirtió en el cuarto mayor factor económico, convirtiéndose en un factor de producción cada vez más importante"* (2000, p.43) Los datos personales no son la excepción. Ya que para entrar a la World Wide Web hay que aportar

datos: para registrarse y sacar una cuenta de correo electrónico, para subscribirse a un newsletter de un diario o revista, para buscar empleo, para crear un perfil en una red social, en portales de compra de artículos, etc. uno tiene que dejar sus datos personales. Por ende, el mundo digital viene a multiplicar por un lado la cantidad de datos personales referidos a las personas, y por el otro a aumentar los canales de publicación de los mismos. Logrando así un flujo continuo e incontrolable de información personal referida a las personas, y haciendo que éstas pierdan el control sobre la misma.

Los datos personales que aportamos en Internet son: nombre y apellido; fecha de nacimiento; domicilio; número de DNI o pasaporte; dirección de correo electrónico; número de teléfono; código de tarjeta de crédito; fotografías.

Estos datos son de suma importancia por qué revelan la identidad de la persona, la forma de contactarla, puede sugerir su procedencia u origen, pueden mostrar sus aficiones, preferencias, hábitos de consumo, así como su entorno o familia. Por eso debemos saber que a la hora de facilitar datos de carácter personal en Internet hay que asegurarse de la fiabilidad y seguridad que nos ofrece quien los solicita, debiendo aportar en todo caso, exclusivamente los necesarios para la finalidad con la que están siendo recabados. Para eso, es conveniente siempre acudir a las políticas de privacidad y las condiciones de uso que se publican en los distintos sitios web. Y es importante saber que toda la información que subimos a la web, quedará alojada allí, para siempre, ya que es muy difícil poder darla de baja.

La Red Mundial de Internet es una inmensa colección de páginas de hipertexto. Ya no constituye como en su origen una herramienta para científicos, sino que es un medio para toda la ciudadanía que navegue en la web, para realizar las distintas y diversas actividades que ese usuario desee. "*Esta expansión de Internet ha planteado así mismo un fenómeno inédito. Como "autopista de la información" es, en los hechos, la máquina copiadora y transmisora de datos más grande del mundo, y la mayor base de datos concebible"* Así lo explica Claudia R. Brizzio en su libro "La informática en el nuevo Derecho" (2000, p.39).

Pero no solo existen los datos personales que los usuarios subimos a la web, sino que también contamos con datos personales publicados por terceros (entendiendo por terceros a personas no titulares de los datos en cuestión). Esto sobre todo sucede en sitios web como las redes sociales, los distintos portales de contactos, de vídeo, blogs y foros. Todos estos datos son importantes porque pueden estar en la red sin conocimiento, ni consentimiento del titular de los datos, y en muchas ocasiones, su indexación por los buscadores puede darles una

difusión global en Internet. En cuanto a esto, es importante saber que como ciudadanos tenemos derechos. Y entre otros, podemos solicitar que se cancelen los datos publicados en esos sitios web o, al menos, a que se evite su recuperación por los buscadores. Para ello, es necesario dirigirse a los responsables de los sitios webs pertinentes donde se alojan los contenidos con nuestros datos.

También es importante destacar que existen datos de navegación y de comportamiento en la red. Los mismos en cuanto a que se pueden vincular o relacionar con una persona o usuario son datos personales. Existen las llamadas Direcciones IP, que son un conjunto de números que identifican a una computadora cuando se conecta a una red. La dirección IP puede servir para localizar geográficamente al usuario de esa PC, y dado que se asigna unívocamente a la línea de conexión por la compañía que nos presta el servicio de acceso, puede permitir en muchos casos la identificación del titular de la línea y, en consecuencia, del probable usuario de la misma. Vale saber entonces, que muchos servicios de Internet, como las redes sociales o los buscadores, conservan nuestras direcciones IP.

Las *cookies* son ficheros o pequeños archivos de texto que se almacenan en la computadora del usuario que navega a través de Internet y que, en particular, contienen información sobre el sistema operativo y el navegador utilizados en la navegación. Estos ficheros se asocian a un número que permite identificar unívocamente el ordenador del usuario. Las cookies son creadas por el sitio web que visita el usuario y permiten a éste conocer con detalle su actividad en el mismo sitio o en otro con lo que se relaciona éste, por ejemplo: el lugar desde el que accede, el tiempo de conexión, el dispositivo desde el cual se accede, el sistema operativo y navegador utilizados, las páginas más visitadas, el número de clics realizados e infinidad de datos respecto al comportamiento del usuario en Internet. El peligro con las cookies es que son utilizadas por los sitios de Internet para informarse de nuestros movimientos y así pueden registrar las visitas y las operaciones realizadas en su sitio, o cualquier otra información útil para ellos. En lo que atañe a datos personales el peligro es que pueden permitir elaborar perfiles sobre nuestra navegación por Internet, y así saber nuestros gustos y preferencias (para campañas publicitarias o de marketing de productos). Por eso es que se deben utilizar las herramientas de los navegadores para borrar regularmente las cookies que se almacenan en nuestras computadoras.

Por eso, como dice Esteban Ruiz Martinez en el libro “Derecho y nuevas tecnologías” *de Pablo Palazzi,* “C*orresponde aquí una seria consideración sobre la legalidad de dicha*

*operatoria informativa de las cookies, pues nuestros movimientos en un sitio consisten en un actuar concreto, son nuestros actos personales, que revelan nuestros gustos, preferencias, formas de ser y de pensar, todos alcanzados, claramente, por el derecho a la intimidad cuando se pueda identificar al usuario" (*2000, p.19*).*

Límites legales

Es importante destacar siempre cuáles son los mecanismos legales que existen para poder legislar en cuanto a la temática de protección de datos personales en Internet. Con referencia a esto, cabe decir que, la ley 26.032 del año 2005 establece que la búsqueda, recepción y difusión de información e ideas por medio del servicio de Internet se considera comprendida dentro de la garantía constitucional que ampara la libertad de expresión. Al mismo tiempo, la protección de datos personales protege a la persona de toda afectación en sus derechos con motivo del tratamiento de su información personal.

Por ende, en Internet se estarían cruzando la libertad de expresión y la protección de los datos personales y es ahí donde existe un conflicto a resolver. Primero, cabe decir que la libertad de expresión no es un tratamiento de datos personales. Porque difundir información, ya sea a través de una noticia o una opinión es un acto espontáneo y libre, y con intencionalidad de amplia difusión -sin que esto implique un tratamiento sistemático de datos personales-.

Ahora bien, como se encuentra en la página web de la Comunidad de Madrid "*la protección de datos personales lo que hace es regular precisamente el tratamiento sistemático, organizado, de la información personal, o sea, no regula la expresión espontánea de una opinión o noticia, sino aquella información que es sometida a un tratamiento específico que tiene por finalidad obtener información sobre las personas*"(http://www.madrid.org/, 2011). Por eso, podemos sostener que la actividad informativa estará alcanzada por la Ley 25.326 de protección de datos personales

Por ello, el periodismo o bien portales de internet u otra forma de comunicación, en su ejercicio del derecho a informar, no se pueden extender en detrimento de la necesaria armonía con los restantes derechos constitucionales, entre los que se encuentran el de la integridad moral y el honor de las personas. El mismo sitio web nos indica que, "*la libertad de expresión impide toda censura previa, pero acarrea responsabilidades ulteriores, y*

cuando se afecta la intimidad o el honor, el responsable de la información deber responder por el prejuicio caudado" (http://www.madrid.org/, 2011)

Es decir, la actividad periodística siempre gozará de su privilegio de no ser controlada previamente, pero debe tener presente la necesidad de ser estricta en su contenido, objetivos y modalidad de difusión, previendo la utilización de una técnica o arte en su ejercicio que garantice la no afectación de los derechos de las personas.

Así, sostenemos que en Internet no todo es libertad de expresión. Ya que hay múltiples actividades que se desarrollan en dicho medio electrónico que son relativas al tratamiento de datos personales. Como por ejemplo, los bancos de datos que operan en Internet sin realizar una actividad de libertad de expresión sino de tratamiento de datos personales, y lo realizan, en algunos casos, como responsables directos, y en otros como indirectos (ya sea poniendo a disposición datos personales en la red o facilitando la herramienta de tratamiento de datos a terceros, como hacen los buscadores de Internet). *"Así sucede en materia de información, en la que el hombre presenta una dualidad de tendencias instintivas: por un lado el ser humano tiene necesidad de saber y por otra tiene necesidad de ocultar"* dice Luis Manuel C. Meján (1994, p.5). Llegando así a la idea que el dato personal en Internet, en la medida que no sea el adecuado ejercicio de la libertad de expresión, está protegido por la ley 25.326.

Casos en lo que cabe considerar que la información que se haya en Internet incurre en tratamiento de datos personales en los términos de la ley 25.326:

a) **Bancos de Datos Personales radicados en Internet:** Son lisa y llanamente bancos de datos personales, que al igual que los que manejan las empresas en la vida "no-virtual" deben estar inscriptos ante la Dirección Nacional de Protección de Datos Personales, como órgano de control de la ley.
b) **Tratamiento de datos encubierto en noticias:** Son datos personales que con motivo de una actividad informativa, son tratados de forma abusiva o inapropiada, generando así una difusión innecesaria de datos personales al momento de difundir la noticia misma. Por lo tanto se desnaturaliza así la actividad informativa, y esos datos debería ser eliminados del sitio web al que pertenecen.
c) **Información personal obsoleta:** Es la información personal que está en Internet que pierde actualidad pero aún permanece disponible. La misma debería ser eliminada,

siempre y cuando no exista un interés público y tenga potencialidad de afectar derechos de las personas.

d) **Información personal lesiva de derechos de las personas:** Es información que lesione el honor, intimidad, o cualquier otro derecho de las personas sin que quepa presumir la eventual existencia de un derecho o interés legítimo superior de terceros para su difusión. Los mismos, deberían ser eliminados de los sitios donde se encuentran. En estos casos, la ley se aplica de manera plena y directa sobre los sitios o páginas que difundan dicha información (fuente), pero no a quienes brinden servicio de réplica, memoria caché o difusión de los contenidos de Internet, como es el caso de los buscadores. Estos mismos, por brindar un servicio de mera intermediación y réplica de la información, no son responsables de dicho contenido (más adelante se aclara en el apartado dedicado a los buscadores).

e) **Tratamiento de datos personales en los servicios destinados al ejercicio de la libertad de expresión:** Se habla aquí de las empresas prestadoras de servicios de Internet, en los casos en que realicen un tratamiento de datos personales en los términos de la ley 25.326, sobre información que poseen en sus servidores. Aquí se excede la finalidad meramente informativa o de libertad de expresión, por ende se debe aplicar la ley a dicho tratamiento devenido en banco de datos personales.

En cuanto a los **buscadores de Internet** (Google y Yahoo son los principales) es que al ser la web una red interconectada, genera que un dato personal cargado en cualquier página web, con la actividad de los buscadores pasa a formar parte de un banco de datos global por su natural relacionamiento. Por lo tanto, se deduce que no se puede solicitar a Internet que se inscriba ante el órgano de control de cada país y cumpla con las respectivas leyes de protección de datos personales. De esta manera, la aplicación de la ley 25.326 en nuestro país será atípica en cuanto a Internet.

El mayor problema surge con el tratamiento de datos realizado por terceros. Es decir, el tratamiento de datos personales que realizan todos aquellos que carguen un dato personal en el buscador y activen su búsqueda. Las mismas pueden darse o bien para noticias de interés público o en otros casos pueden ser datos perjudiciales a los derechos del titular del dato tutelado por la ley 25.326. Ahora bien, el responsable de dicho tratamiento es aquel que busca información de una persona y pone en marcha el programa. Pero este usuario común de la web en principio está exento de la ley 25.326, porque cabe presumir que lo utiliza para su uso exclusivo personal. Por eso no se lo puede responsabilizar ni al usuario ni al buscador.

No obstante cabe exigirle al titular del buscador, como dueño del mecanismo, un adecuado diseño y políticas de uso. Pues como dueño de la herramienta no debe permitir que la información sea utilizada de manera prejudicial para terceros. Por eso debe tomar los recaudos para que ello no vuelva a producirse, debiendo así bloquear el acceso a los links que producen dicho tratamiento.

En tal sentido, se podrá aplicar a las relaciones que efectúa el buscador las disposiciones de la ley 25.326 de protección del titular del dato frente al tratamiento de datos personales en contravención con la ley (sin que esto afecte la tarea informativa de los buscadores, ya que esto solo protege al titular del dato en actividades de relacionamiento de su información personal en los términos de la ley).

Si bien no es posible que el buscador elimine o suprima el dato (ya que solamente es intermediador) si puede requerírsele, cuando se encuentre en juego la protección de datos personales, que dicho relacionamiento cumple con ciertas condiciones y garantías relativas al tratamiento de datos.

La conclusión en cuanto a los buscadores es que deben bloquear el acceso a cualquier resultado de su buscador que afecten derechos de las personas, ya que como así lo afirma Luis Manuel C. Meján en su libro *"el fenómeno de la información cuenta con dos sujetos: uno es el que posee, o recaba, o almacena, o está en posibilidades de difundir la información; y el otro es el individuo sobre el cual versa la información o al que le afecta. Entre los dos: el agente de la información y el sujeto de la información existe una necesaria relación y vinculación jurídica, no es el caso de la bilateralidad sinalagmática de Derecho de las Obligaciones, sino una relación de Derecho Constitucional, pues se ponen en juego garantías individuales" (1994)*

La Web 2.0

En los últimos años Internet ha evolucionado desde un modelo en el que el usuario ocupaba un papel pasivo (prácticamente de simple lector y reproductor de la realidad), a un papel activo (protagonista, creador de contenidos y de la realidad). El universo web se ha convertido en un espacio social dinámico donde los individuos se relacionan, interactúan y se juntan en comunidades.

Las aplicaciones y servicios han evolucionado permitiendo que no resulte necesario tener un gran conocimiento para utilizar estas herramientas. Basta con registrarse para

acceder a un conjunto de programas y servicios que permiten editar nuestro blog o página web y convertirnos en “periodistas digitales”, colgar nuestros vídeos e imágenes, o mantener una interacción en tiempo real con miles de personas en todo el mundo. Los mundos virtuales emulan el mundo físico generando entornos amigables que se perciben como el usuario del mismo modo que si existieran en el mundo físico.

Tal como señala la Guía de recomendaciones para usuarios de Internet:“*Esta realidad que se ha denominado Web 2.0 no es únicamente un conjunto de recursos tecnológicos y servicios sino que ha creado un universo social propio poblado por comunidades locales, profesionales y globales, entre otras, cuya simple descripción requiere de un esquema claro de contenidos*”(2011).

Redes Sociales y su impacto

En éste ámbito de webs 2.0 se destacan las redes sociales, por su complejidad e incidencia en el derecho fundamental a la protección de datos. Se trata de un fenómeno que ha supuesto una verdadera revolución en Internet. A través de las redes sociales es posible compartir información personal y contactarse con otros usuarios de la red. Son plataformas online desde las que los usuarios, previamente registrados (dejando sus datos personales), pueden interactuar mediante mensajes, compartir información de todo tipo, ya sea fotos, videos, artículos, etc. permitiendo así que estas publicaciones sean accesibles de forma inmediata para todos sus contactos.

Los sitios de redes sociales están formados por personas enlazadas por uno o diversos tipos de relaciones (parentesco, amistad, trabajo, creencias) según el tipo de red que se trate. Existe la teoría de los seis grados de separación iniciada en 1930 por el escritor húngaro Frigyes Karinthy, y luego profundizada por el sociólogo Duncan Watts. El concepto está basado en la idea de que el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y sólo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en la población humana entera. Por ende cualquier individuo podría estar conectado con cualquier otra persona a través de una cadena de no más de 6 grados.

El origen de las redes sociales se remonta al año 1995, cuando Randy Conrads creó el sitio web ´classmates.com', con la que pretendía que los usuarios pudiesen recuperar o mantener el contacto con antiguos compañeros de colegio, instituto, universidad, etc. En el año 2002 comienzan a aparecer páginas que promocionan círculos de amigos en línea, adquiriendo popularidad en el año 2003 con la llegada de portales como MySpace o Xing. La popularidad de estas plataformas creció exponencialmente. Las grandes empresas empezaron a ver nuevos proyectos de negocios en el entorno de las redes sociales, por la gran popularidad que éstas generaban en los usuarios. A estas redes les fueron sucediendo otras, como Orkut, o Small World, y también comenzaron a aparecer redes especializadas (verticales) que ya veremos más adelante lo que son.

En la práctica el funcionamiento de estos servicios de redes sociales comporta que cada usuario ponga a disposición de otros, con los que no tiene por qué tener una relación de confianza, multitud de información personal. Generalmente en las redes sociales se denomina "amigo" a alguien que simplemente nos ha hecho llegar una tarjeta de presentación o que conforme a las reglas del portal "es amigo de un amigo". El empleo de expresiones del tipo "amigo", "seguidor", ofrecen una falsa imagen de privacidad para lo que, si no se conoce el funcionamiento de la red social acaba siendo público y disponible para cualquier persona. De hecho, si se utilizan las configuraciones por defecto, lo habitual es que la información sea completamente disponible para cualquier tercero, incluidos los buscadores.

Entonces, las ideas centrales en las redes sociales son tres: crear, compartir y consumir. Los usuarios comparten contenido de toda índole con sus "amigos" mediante diversas aplicaciones delineadas por cada red social. El usuario de la red se convierte en una especie de "Prosumidor", un usuario que consume y que produce contenidos en la red.

Cabe destacar que hay dos tipos de redes sociales. Por un lado las horizontales, que son redes sociales de comunicación, genéricas, sin usuarios y temáticas definidas. Un ejemplo de ellas podría ser Facebook o bien Twitter. Por otro lado están las redes sociales verticales, que son redes especializadas, creadas en base a una temática común. Dentro de ellas están las profesionales, como LinkedIn, las de ocio como Wipley (videojuegos) o Last.FM (Música), o bien las mixtas como Yuglo (creativos) o Unience (inversores).

Entre las actividades más comunes en estas redes sociales se encuentran la de compartir o subir fotos, enviar mensajes privados, comentar las fotos de los amigos, actualizar el perfil, enviar mensajes públicos, etiquetar amigos en fotos, videos o

publicaciones, descargar aplicaciones, buscar amigos, etc. Estas funciones típicas de las redes sociales tienen sus oportunidades y ventajas, pero también conllevan riesgos. Es decir, las redes sociales horizontales, genéricas o de ocio cuentan con un nivel de riesgo superior a las verticales o profesionales, dado que los usuarios exponen no sólo sus datos personales de contacto o información profesional o religiosa, sino que se pueden exponer de manera pública las vivencias, gustos, intereses, ideología y experiencias del usuario, lo que conlleva que la cantidad de datos de carácter personal puestos a disposición del público es mayor que en las redes verticales.

Existen distintos tipos de posibles riesgos para los datos personales en las redes sociales: entre ellos que el tipo de datos solicitados en el formulario de registro sean excesivos, que el grado de publicidad (exposición) del perfil del usuario sea demasiado elevado, que la finalidad de los datos no esté correctamente determinada, que haya una publicación excesiva de información personal, la instalación y uso de cookies sin consentimiento del usuario (almacenan determinada información sobre el usuario y su tipo de navegación a través de un sitio web), la suplantación de identidad de los usuarios de la red social, la recepción de comunicaciones comerciales electrónicas no solicitadas (spam), o bien la imposibilidad de realizar la baja efectiva del servicio (una vez efectuada la baja, los datos se mantienen a disposición de los responsables de la red social).

Las redes sociales ofrecen medios de interacción basados en los perfiles personales y contenidos que generan sus propios usuarios registrados. Esto supone un peligro a la privacidad de estos usuarios, ya que sus datos personales están siendo accesibles de forma pública y global. La gran problemática que se surge es por la acumulación ilimitada de información, y por la posibilidad de utilización ilícita de los datos de los usuarios. Para que este tratamiento de datos personales sea lícito se debe garantizar el consentimiento libre, expreso e informado del usuario en cuestión. Sumado a esto, los proveedores de servicios de redes sociales deben informar quienes son los que poseen los datos personales de los usuarios y con qué finalidad. Así entonces, los usuarios deben contar con el derecho a oponerse a esa posición y uso de sus datos.

Concientización de la sociedad

"*El papel del Derecho en el avance y aparición de novedades tecnológicas es el de servir como elemento disciplinador del proceso*". Así lo explica el autor del libro "El derecho a la intimidad y la informática", Luis Manuel C. Meján (1994).

Los principales problemas que surgen debido al uso de webs 2.0 y redes sociales son la revelación de datos personales que deben permanecer en la esfera de lo privado. Pero este hecho de que haya riesgos e incertidumbres no debe hacernos temer a las redes sociales. Ya que la gran mayoría de los jóvenes tiene una valoración positiva de las mismas. Por eso lo que nos falta aprender es a gestionar este nuevo paradigma. Ser conscientes de sus oportunidades, explotarlas, pero también saber que cada nueva oportunidad conlleva un riesgo. Por lo tanto hay que saber aprovechar las oportunidades, pero gestionando los riesgos. Para eso hay que educar en el tema, conocerlo bien, profundamente, para poder transmitírselo a los chicos y adolescentes que son los que más expuestos están en las webs 2.0 y redes sociales. El mensaje debe ser claro: los usuarios somos los que volcamos los datos personales en Internet, es importante ser conscientes de esto y pensar qué información hacemos pública.

Para concientizarnos al respecto, la familia y la escuela deben estar presentes en la socialización de los chicos en Internet. Padres, adultos y docentes juegan un rol fundamental para el aprendizaje del uso seguro de estas tecnologías por parte de los chicos. La toma de conciencia y la educación deber realizarse a través de Internet, y no eludiéndola. Para que los padres y las familias en general puedan acompañar a los chicos en el uso de las redes sociales, deben primeramente conocer qué es lo que verdaderamente son las redes sociales, los buscadores e Internet en general, qué funciones tienen y qué pueden hacer en ellas sus hijos. Un ejemplo claro que refleja la problemática actual es la que se da en cuanto a las amistades. En la vida real, los padres se preocupan por los amigos que tienen sus hijos. En cambio, en la vida virtual de las redes sociales, un padre no tiene ni idea las amistades con las que cuenta su hijo. Es clara la tendencia que existe en los jóvenes de aceptar a desconocidos en las redes sociales. Muchos lo hacen para ser "populares" y tener la mayor cantidad de contactos posibles. El rol del adulto, consiste en aconsejar respecto a que no es recomendable agregar a un desconocido, pero si se hace, es importante ajustar las configuraciones para no compartir con éstos nuestros datos personales.

Por otro lado, la escuela debe ser otro ámbito que eduque a los chicos en su uso de la herramienta informática. El Memorandum de Montevideo explica: "*El proceso educativo*

debe proveer de conocimiento sobre el uso responsable y seguro por parte de las chicos y adolescentes de las políticas de privacidad, seguridad y alertas con las cuales cuentan los instrumentos de acceso y aquellos lugares web en los cuales las niñas, niños y adolescentes son usuarios frecuentes como las redes sociales digitales". (2011). La escuela debe acompañar al niño en el proceso de creación de su identidad en el mundo digital. Y aquí no se trata de vigilar, sino más bien de dar orientaciones, modelos, de educar en la libertad de internet. Transmitir los cuidados de la vida real, a la vida virtual.

Se debe aprovechar al máximo el potencial comunicativo de las redes sociales y las webs 2.0, para abrir espacios de conexión, de encuentro, crear comunidades sanas (por ejemplo comunidades de alumnos de tal o cual colegio, o bien de intereses educativos o pedagógicos, o crear aulas virtuales de las asignaturas). Pero hay hacerlo siguiendo los criterios de privacidad y seguridad, evitando situaciones de riesgo (cerrando los grupos, restringiendo el acceso sólo a gente adecuada y no masificando las invitaciones, porque ahí surgen los problemas).

Existen varios tipos de abusos a los que se exponen los usuarios de las redes sociales o chats, a saber:

- Ciberbullying: Se da entre pares, y es cuando un menor amenaza, hostiga, humilla o molesta a otro a través de Internet.
- Grooming: Son prácticas online que realizan adultos a través de las cuales éstos se ganan la confianza del menor fingiendo empatía con ellos con fines meramente sexuales.
- Sexting: Consiste en el envío de contenidos de tipo sexual producidos por el remitente.

Lo importante es que los jóvenes tomen real dimensión de lo que implica subir contenidos en las redes sociales. Esto se logra identificando y disminuyendo los factores de riesgo relativos al uso de las nuevas tecnologías. Así, se podrá adquirir consciencia de que subiendo información a la web a través de publicaciones en Facebook o en Twitter formamos una identidad digital, una reputación online, un perfil de usuario. Por lo tanto quienes utilizamos estas nuevas tecnologías debemos pensar antes de hacer clic, ya que toda la información que subimos será muy difícil de borrar. Por eso es importante aprender a configurar la privacidad y seguridad de las cuentas en las redes sociales que se utilicen y así

saber quién tiene acceso a nuestros datos como fotos, videos, gustos o preferencias, ideología política, preferencia sexual, creencias religiosas, etc.

Bibliografía

-Brizzio, C. R. (2000*) La informática en el nuevo derecho*. (p.39) Buenos Aires: Abeledo-Perrot

-Debruelle, C. (1984 junio) *Problemas legislativos de la protección de datos. Ponencia presentada en la Conferencia Internacional de Madrid*, Madrid, España.

-Eco, U. (2012) *La estrategia de la ilusión.* Barcelona: Random House Mondadori.

-Frosini, V (1982) *Cibernética, derecho y sociedad.* Madrid: Tecnos

-Instituto de Investigación para la Justicia e Instituto Federal de Acceso a la Información y Protección de Datos, *Protección de Datos Personales en las redes sociales digitales: en particular de niños y adolescentes. Memorandum de Montevideo* (2011). Buenos Aires: IFAI y IIJusticia.

-Meján, L. M. C. (1994*) El derecho a la intimidad y a la informática*. México D.F: Porrúa

-Messía de la Cerda Ballesteros, J. A. (2003) *La cesión o comunicación de datos de carácter personal*. Sevilla: Civitas Ediciones S.L

-Palazzi, P (2000) *Breve ensayo sobre el derecho a controlar la información personal*. En E. Ruiz Martínez *Derechos y nuevas tecnologías* (p.72) Buenos Aires: Ad-Hoc

-Palazzi, P (2000) *El modelo informático desafía al derecho antitrust*. En R. Chacón de Albuquerque *Derecho y nuevas tecnologías* (p.43) Buenos Aires: Ad-Hoc

-Palazzi, P (2000) *La protección de la propiedad intelectual en la sociedad de la información*. En G. Martínez Medrano, *Derechos y nuevas tecnologías* (pp.19-21). Buenos Aires: Ad-Hoc

-*Perez Luño, A. E. (2010) Derechos humanos, estado de derecho y constitución.* (p.383) Madrid: Tecnos.

-Puccinelli, O. (1999) *El habeas data en indoiberoamérica*. Bogotá: Temis.

-Riquert, M. A. (2003) *Protección penal de la intimidad en el espacio virtual.* Buenos Aires: Ediar.

- Agencia Española de Protección de Datos (2011), *Guía de recomendaciones a usuarios de Internet.*