El derecho a la Intimidad y el caso Facebook

Iommi Alejandro

Abogado, recibido en el año 2011 de la Facultad de Derecho de la Universidad de Belgrano. Procurador en estudio jurídico Amz & Asociados. aleiommi@gmail.com

Abstract Español. La Intimidad está hoy en día, más vulnerable que nunca y esto se da en particular, a causa de las redes sociales (siendo el Facebook la red más popular en nuestro país y por lo tanto el objeto de mi trabajo). Los problemas que causa, compartir en exceso la información privada son de una gravedad considerable y teniendo en cuenta que el acceso al perfil privado de un usuario es algo relativamente sencillo, el daño puede llegar a ser notorio. Considerando que en la actualidad, la intimidad pasó a ser un bien prescindible y sin demasiada importancia (más que nada entre los jóvenes), las prevenciones son desoídas y la reacción más frecuente es la indiferencia. El objeto de este trabajo es analizar la problemática del tema, los recaudos a tomar y los pasos a tomar para evitar la invasión a nuestra intimidad dentro de las redes sociales.

Keywords: intimidad, red social, Internet, facebook, privacidad, web 2.0, delito informático.

Introducción

El Derecho a la Intimidad es un derecho imprescindible para el ser humano en sociedad. Ya desde su nacimiento - en la jurisprudencia de los Estados Unidos - fue creado con el objetivo de limitar la invasión de la prensa en la vida íntima de las personas. Desde su creación hasta la actualidad, este derecho fue evolucionando paulatinamente y adaptándose a los cambios de la sociedad. En nuestro ordenamiento se encuentra especialmente protegido por el art. 19 de la C.N., el cual predica que las acciones privadas son discrecionales mientras que no se afecte a un tercero o a la moral pública y aparte es complementado por el art. 18 que prohíbe la invasión al domicilio privado y a las comunicaciones personales, a menos que una ley especial permita su allanamiento en casos excepcionales. Por lo tanto ya en la Ley Fundamental el derecho a la intimidad es claramente protegido, debido a su importancia fundamental en la vida de las personas.

Luego en el Código Civil se establecen sanciones al que violare la intimidad de otra persona y la posibilidad de demandar al responsable por daños y perjuicios, también la intimidad es protegida en el derecho internacional, ya que el art. 11 de la Convención Americana sobre Derechos Humanos lo contempla expresamente.

Por otro lado, el Código Penal tipifica como delito la invasión de la correspondencia y papeles privados de las personas y mediante la Ley 26.388 se abarca también a la información informática, actualizándose el código a la nueva realidad.

También hay que mencionar la acción de Habeas Data, que nace del art. 43 de la C.N., la cual confiere acceso a la información de datos personales en registros o archivos que sean susceptibles de ser difundidos y que previamente a ser reglamentada ya era reconocida por la jurisprudencia.

Los llamados delitos informáticos son algo relativamente novedoso y a pesar de existir varias maneras de denunciarlos, se dificulta bastante el tema de la prueba, algo fundamental en todo tipo de proceso.

En el año 2000 fue sancionada la Ley 25.326 que protege esencialmente la información sensible de las personas y prohíbe la divulgación de los mismos. Además establece que los datos cedidos solo pueden ser utilizados con el consentimiento de su titular y con un fin previamente tolerado por este. El registro nacional de bases de datos fue otro avance en post de la protección de la información, teniendo como objetivo la regulación de las bases por medio de la inscripción en dicho registro y por lo tanto lograr un control, del uso de dicha información.

La llegada de Internet marcó un antes y un después en cuanto al derecho a la intimidad, ya que posibilitó el debilitamiento del mismo mediante programas invasivos tales como virus, Spyware, cookies y formularios destinados a obtener información personal con fines ocultos.
Facebook fue otro logro de la llamada web 2.0, logró el cambio del usuario del modo pasivo al activo, ya que facilitó herramientas para que todos los usuarios tengan la facultad para producir su propia información. Las redes sociales consiguieron algo insólito, que las personas hagan pública su vida privada y que la intimidad pase a ser un bien prescindible.

Para poder realizar este trabajo no solo se investigo en los textos jurídicos clásicos, como la Constitución Nacional, Códigos, Leyes, Manuales y Tratados sino que se incluyo también información seria obtenida en Internet, el medio más valioso y vasto de la actualidad. Al ser un tema tan actual la mayor parte de la información se encuentra en dicho medio y el valor de la misma se acredita por su propio origen.

CAPITULO 1: INTERNET Y LAS REDES SOCIALES

1. Problemática

Los datos personales y la información sensible deben ser protegidas por cada persona y por lo tanto no es para nada aconsejable su divulgación en forma irresponsable. "La mejor manera de proteger sus datos personales es evitar suministrarlos en forma indiscriminada". A modo de anticipo de la conclusión se recomienda:

- No complete formularios al azar. Muchos formularios que se ofrecen en la vía pública o a través de Internet, y que se relacionan con concursos, premios y obsequios, son excusas para obtener sus datos personales y utilizarlos, en el mejor de los casos, para realizar ofertas de productos. **Evite completar estos formularios si no confía en la seriedad de quien los ofrece. No suministre su información personal a menos que sea estrictamente necesario.**

- No entregue más información personal que la necesaria. La Ley 25.326 establece que sólo se podrá guardar la información personal necesaria para cumplir con el fin para el cual se recolectó la información. Es decir que no se puede guardar información por el mero hecho de tenerla, sino que debe estar justificada su obtención. Así, para concretar una operación de compra, podrá solicitarse los datos para la facturación, como nombre, dirección, pero no la dirección de correo, por ejemplo**. Si se la solicitan, exija la justificación y el destino que se dará a esa información adicional. Y niéguese a entregarla si no lo satisfacen las explicaciones.**

- Proteja a sus hijos. Converse con sus hijos acerca de los peligros que puede entrañar brindar información propia o de familiares. Adviértales que los datos podrían ser utilizados tanto para una publicidad, como para nuevas modalidades delictivas, tales como los secuestros virtuales, donde los criminales utilizan información obtenida para simular el secuestro de una persona**. La educación sobre el uso responsable de los datos personales debe comenzar en la niñez."**[1]

Hay que ser cauteloso a la hora de completar formularios con nuestros datos, ya que muchas veces solo son un medio para obtener información personal con fines publicitarios. La ley 25.326 exige que todo almacenamiento de información personal debe estar justificado y su finalidad debe ser conocido por la persona involucrada.

[1] Ministerio de Justicia, Seguridad y Derechos Humanos. (Página consultada el 21 de Septiembre de 2010). Presidencia de la nación, [On-line]. Dirección URL: http://www.jus.gov.ar/datos-personales/recomendaciones/proteja-sus-datos.aspx

En la actualidad Internet es una fuente importantísima de información, aunque también tiene sus peligros y riesgos, por lo que es imprescindible conocerlos para evitar daños en nuestra intimidad.

"Internet es una herramienta de mucha utilidad y el uso descuidado, como por ejemplo el acceso a páginas de dudosa procedencia, puede provocar daños en su PC y a su privacidad.

Esto se realiza por medio de programas maliciosos que se introducen al sistema. Estos programas se dedican al robo de datos personales y a cuentas de crédito, mientras que otros son utilizados con fines publicitarios. Estos ingresan por diferentes medios y los antivirus tradicionales no suelen detectarlos. Para eliminarlos se requieren programas especiales."[2]

El uso de Internet debe ser siempre de forma prudente, ya que de lo contrario se corre un alto riesgo de sufrir invasiones a la propia privacidad.

"La Dirección Nacional de Protección de Datos personales ofrece la siguiente información sobre los peligros de la web y las recomendaciones para que usted pueda navegar mas seguro por internet, con el objeto de contribuir a la protección de su privacidad y sus datos personales:

Software malicioso: son programas también conocidos como malware. Puede ser un virus que parece inocente, con alguna imagen en la pantalla que aparece y desaparece, hasta un virus que destruya toda la información. Este software es muy peligroso para las empresas, porque algunos programas fueron creados con propósitos criminales, tales como las transferencias de dinero, espionaje industrial, etc..
Software espía o spyware: registra todo lo que el usuario hace con el propósito de conocer sus preferencias y enviarle publicidad relacionada con su perfil."[3]
Conocer los peligros de Internet es el primer paso para evitar caer en un engaño, existen una serie de recomendaciones que podemos aplicar para que nuestra intimidad no sea violada.
"**Spam:** consiste en todo lo que el usuario recibe en su casilla de correo electrónico sin haberlo solicitado. Hay diferentes tipos de spam que pueden llegar a nuestra Bandeja de Entrada. Entre estos se destacan los mas perjudiciales como el Hoaxes, los Fraudes y los Scams."[4]

[2] Ministerio de Justicia, Seguridad y Derechos Humanos. (Página consultada el 18 de Septiembre de 2010). Presidencia de la nación, [On-line]. Dirección URL: http://www.jus.gov.ar/datos-personales/recomendaciones/uso-seguro-de-internet.aspx
[3] Ministerio de Justicia, Seguridad y Derechos Humanos. (Página consultada el 18 de Septiembre de 2010). Presidencia de la nación, [On-line]. Dirección URL: http://www.jus.gov.ar/datos-personales/recomendaciones/uso-seguro-de-internet.aspx
[4] Ministerio de Justicia, Seguridad y Derechos Humanos. (Página consultada el 18 de Septiembre de 2010). Presidencia de la nación, [On-line]. Dirección URL: http://www.jus.gov.ar/datos-personales/recomendaciones/uso-seguro-de-internet.aspx

Uno de los fraudes más conocidos y famosos es el Spam, que es toda información que llega a nuestro mail sin que nosotros la hayamos solicitado. Si se accede a este mail se corre el riesgo de que nuestra intimidad sea vulnerada.

Es imprescindible seguir ciertas recomendaciones para navegar en forma segura:

- **"Mantenga actualizado el software**. Es muy importante contar con un buen antivirus y un antispyware. También actualice cada 15 días su antivirus y su Sistema Operativo.
- **Utilice exploradores** que no tengan muchas fallas de seguridad.
- **Sea cuidadoso con los lugares que visita** y mucho más cuando esos lugares le hacen instalar programas especiales, por ejemplo "dialers" (marcadores telefónicos que, en algunos casos, pueden marcar números internacionales automáticamente) ofreciendo disfrutar del lugar con fotografías, música y videos. Como resultado de su visita puede tener instalado un espía en su máquina que va a informar al dueño de la página todo lo que usted hace minuto a minuto.
- **Sea cuidadoso con los correos que abre.** No basta conocer el emisor para abrir el correo con confianza, ya que no existe ningún mecanismo para autenticar el nombre del remitente. La persona que envía puede colocar en el campo "De" o "From" el nombre o la frase que desee, y este nombre es el que se muestra en el mensaje al recibirse. Cualquier correo, cualquiera sea el asunto que un mensaje tenga, puede ser contaminante (es sencillo para un programador emitir mensajes con el mismo contenido malicioso y cientos de asuntos distintos).
Si la redacción del mail no concuerda con lo que habitualmente suele recibir del remitente, no lo abra.
Verifique por e-mail o teléfono si realmente esa persona amiga/conocida le mandó ese mail y, sólo una vez verificado que no existen problemas, proceda a abrirlo.
O en caso contrario elimínelo rápidamente para evitar cualquier contratiempo."[5]

Lo primero y principal es contar con un antivirus confiable, un navegador eficiente y también prestar atención a los sitios que se visitan y a los correos que se abren.

"**Salvo circunstancias muy especiales no se haga partícipe de cadenas de mails**, ni crea en frases que le incentivan a participar en las mismas diciendo algo así como: "Atención: no es una broma, funciona. Entonces, date gusto, regálate…", etc.
Utilice la opción "copia oculta" para enviar mails. Le evitará problemas a los destinatarios ya que el mail, en camino a su destinatario pasa por equipos intermedios que tienen acceso al contenido del mensaje, y pueden utilizarse para recopilar direcciones para después utilizarlas para enviar correo SPAM.

Si usted tiene contratada banda ancha, la cual no paga por tiempo de conexión, no la deje "conectada" en forma permanente las 24 horas del día, ya que el tiempo prolongado de conexión aumenta la probabilidad de éxito de un eventual atacante que

[5] Ministerio de Justicia, Seguridad y Derechos Humanos. (Página consultada el 18 de Septiembre de 2010). Presidencia de la nación, [On-line]. Dirección URL: http://www.jus.gov.ar/datos-personales/recomendaciones/uso-seguro-de-internet.aspx

encuentre su máquina al barrer, al azar, direcciones de Internet. Si el atacante tiene éxito, debido a vulnerabilidades no protegidas del sistema, puede instalar en la máquina programas maliciosos o incluso utilizarla como iniciante de otros ataques dirigidos a terceras máquinas.

Solamente llene formularios en la WEB en los que se esté utilizando el protocolo https:// (utiliza un Servidor Seguro con encriptación -ilegible para alguien que lo "atrapa" en el medio e intenta leer- de datos entre el Servidor y su máquina), en lugares que le merezcan confianza, y solamente en los casos en los que el llenarlo le proporcione un real beneficio (por ejemplo, acceso a información que usted necesita consultar).

Recomiende a sus hijos que no den ninguna clase de dato respecto a su propia persona ni de ningún familiar directo y que el uso que le den al Chat sea el mismo tanto en presencia de los padres como en ausencia de los mismos. Considere seriamente, también, la ubicación de la PC en un área "pública" de la casa (un lugar donde la pantalla esté siempre a la vista de los padres). **Instale programas para evitar que sus hijos accedan a páginas prohibidas.**

No confíe ciegamente en lo que está publicado en INTERNET. Cualquiera puede publicar lo que quiera y no existe un órgano fiscalizador que controla que lo que está publicado en la WEB no sea malicioso ni que sea verdadero. Procure seleccionar lo que consulta tratando de quedarse con aquello que sea realmente confiable. Sea crítico al analizar el contenido, y deseche páginas o "sites" completos donde observe errores, inexactitudes, superficialidad u otro atributo que le hagan perder confianza en lo allí publicado.

NIC (Network Information Center), es el organismo que administra y registra los dominios en argentina y el mundo. Usted puede visitar www.nic.ar y ver quienes son los responsables de los sitios que usted visita, en Argentina."[6]

Es importante evitar las cadenas de mails, enviar los mismos con copia oculta (para no divulgarlos), tampoco llenar formularios de cualquier pagina ni divulgar datos con información personal y por sobre todo no confiar plenamente en lo que esta publicado en Internet.

2. La web 2.0

"La Web 2.0 se refiere a una nueva generación de Webs basadas en la creación de páginas Web donde los contenidos son compartidos y producidos por los propios usuarios del portal. El término Web 2.0 se utilizó por primera vez en el año 2004 cuando Dale Dougherty de O'Reilly Media utilizó este término en una conferencia en la que hablaba del renacimiento y evolución de la Web.Si hay una Web 2.0 necesariamente debe existir una Web 1.0 de donde evoluciona la primera. La Web 1.0 es la Web tradicional que todos conocemos y que se caracteriza porque el contenido e información de un *site* es

[6] Ministerio de Justicia, Seguridad y Derechos Humanos. (Página consultada el 18 de Septiembre de 2010). Presidencia de la nación, [On-line]. Dirección URL: http://www.jus.gov.ar/datos-personales/recomendaciones/uso-seguro-de-internet.aspx

producido por un editor o *Webmaster* para luego ser consumido por los visitantes de este *site*. En el modelo de la Web 2.0 la información y contenidos se producen directa o indirectamente por los usuarios del sitio Web y adicionalmente es compartida por varios portales Web de estas características." [7]

La diferencia fundamental entre la Web 1.0 y la Web 2.0 es que en esta última, la información es producida por los usuarios.

"En la Web 2.0 los consumidores de información se han convertido en "prosumidores", es decir, en productores de la información que ellos mismos consumen. La Web 2.0 pone a disposición de millones de personas herramientas y plataformas de fácil uso para la publicación de información en la red. Al día de hoy cualquiera tiene la capacidad de crear un blog o bitácora y publicar sus artículos de opinión, fotos, vídeos, archivos de audio, etc. y compartirlos con otros portales e internautas.La Web 2.0 ha originado la democratización de los medios haciendo que cualquiera tenga las mismas posibilidades de publicar noticias que un periódico tradicional. Grupos de personas crean blogs que al día de hoy reciben más visitas que las versiones online de muchos periódicos. La Web 2.0 ha reducido considerablemente los costes de difusión de la información. Al día de hoy podemos tener gratuitamente nuestra propia emisora de radio online, nuestro periódico online, nuestro canal de vídeos, etc. Al aumentar la producción de información aumenta la segmentación de la misma, lo que equivale a que los usuarios puedan acceder a contenidos que tradicionalmente no se publican en los medios convencionales." [8]

La Web 2.0 facilitó las herramientas para que todas las personas tengan la capacidad de producir su propia información.

3. Las redes sociales. El caso Facebook

"La seguridad en Internet no existe, es una sensación, y Facebook no es la excepción a esa regla", asegura **Miguel Sumer Elías**, especialista en nuevas tecnologías, Profesor Titular de Derecho Informático en la Universidad de Belgrano (UB) y responsable del sitio www.informaticalegal.com.ar. Y agrega: "Lo que uno puede hacer es minimizar los riesgos. Por eso, los expertos recomiendan tener presente que todo lo que se sube a la red quedará expuesto a los ojos del mundo entero. No hay que olvidar que los sistemas de seguridad, programados por seres humanos, están lejos de ser infalibles. Y que el propio fundador de Facebook, Mark Zuckerberg, fue víctima de ataques virtuales en los que piratas informáticos accedieron a toda su información. "Si uno quiere estar relativamente seguro en Facebook, debe ser muy consciente de lo que publica y configurar con gran cuidado las opciones de privacidad", afirma Daniel Monastersky, abogado, CEO del sitio www.identidadrobada.com y docente universitario en Derecho Informático." [9]

[7] Javier Gosende, responsable área marketing digital y promoción online de Human Level Comunnications. (Página consultada el 29 de Junio de 2010). Microsoft, [On-line]. Dirección URL: http://www.microsoft.com/business/smb/es-es/internet/web_2.mspx/

[8] Javier Gosende, responsable área marketing digital y promoción online de Human Level Comunnications. (Página consultada el 29 de Junio de 2010). Microsoft, [On-line]. Dirección URL: http://www.microsoft.com/business/smb/es-es/internet/web_2.mspx/

[9] Miguel Sumer Elías, Abogado en Derecho Informático, Internet y Nuevas Tecnologías de Información. (Página consultada el 07 de Julio de 2010).[On-line]. Dirección URL:

El Facebook es una nueva herramienta que si no se usa con cuidado y cautela, puede llegar a ser peligroso para sus usuarios.

"Publicar todo, en todo momento y con pocas precauciones. Por ahí pasa la moda hoy. "Para los jóvenes, Facebook es la principal puerta de entrada a la Web. Acceden unas seis veces por día. Y, de ese modo, van construyendo una suerte de relato audiovisual colectivo de la vida social", explica Roberto Igarza, docente e investigador de la Universidad Austral, especializado en nuevas formas de consumo en la cultura. Para él, una parte de ese fenómeno radica en que la gran mayoría de los usuarios comparte todo con todos, sin crear grupos según niveles de confidencialidad y dejando su información personal "en un campo que no está para nada delimitado".Por su parte, **Elías** agrega: "Estamos cambiando hacia una generación indiferente respecto de su privacidad, donde la tendencia a mostrar se instala como un estilo de vida. Esto se complica cuando hablamos de chicos que juegan a mostrarse sin ser conscientes de las consecuencias"."[10]

En la actualidad, la juventud tiene un afán de mostrar toda su vida privada en forma pública, por lo que la intimidad dejó de ser importante y pasó a ser un bien prescindible.

"En principio, Facebook no permite el acceso a menores de 13 años. Y les recomienda a los padres que "juzguen si es necesario supervisar a sus hijos mientras utilizan el sitio". Luego, los anima "encarecidamente" a hablar con ellos sobre los riesgos del uso de Internet."Hay que hablar con los chicos –recomienda **Elías**– y decirles lo mismo que nos decían nuestros padres cuando íbamos a jugar a la plaza: 'no hables con extraños', sólo que en una versión adaptada a Internet". En su opinión, no es bueno prohibirles el acceso a Facebook, porque la curiosidad los llevará a ingresar en forma oculta, lejos de los ojos paternos. Por el contrario, aconseja mantenerse cerca de ellos y hablarles sobre los peligros en un lenguaje que puedan entender. "Educarlos y darles confianza para que, en una situación de peligro, no se queden callados por pensar que serán castigados".[11]

No se le debe prohibir a los menores el uso del Facebook, sino que se los debe educar y explicar en forma clara, los peligros potenciales que poseen las redes sociales.

"El problema es que, para que los padres puedan dialogar, primero necesitan instruirse. Por lo menos, tener un perfil en Facebook y saber de qué se trata. "Sino, los chicos perciben ese desconocimiento y no consideran a sus padres como autoridades en la materia", afirma Monastersky. "Quizás, la solución sea incorporar conocimientos sobre Internet y el uso responsable de las redes sociales en un espacio público como es la escuela, compartido por padres, hijos y docentes", sugiere Igarza. O tal vez, los padres, sin perder el vínculo padre-hijo, figuren como amigos de sus hijos en Facebook, con el

http://www.informaticalegal.com.ar/2009/12/02/facebook-el-peligroso/

[10] Miguel Sumer Elías, Abogado en Derecho Informático, Internet y Nuevas Tecnologías de Información. (Página consultada el 07 de Julio de 2010).[On-line]. Dirección URL: http://www.informaticalegal.com.ar/2009/12/02/facebook-el-peligroso/

[11] Miguel Sumer Elías, Abogado en Derecho Informático, Internet y Nuevas Tecnologías de Información. (Página consultada el 07 de Julio de 2010).[On-line]. Dirección URL: http://www.informaticalegal.com.ar/2009/12/02/facebook-el-peligroso/

fin de ingresar a su actividad online. “Hay muchas medidas de ese tipo que se pueden tomar, pero lo fundamental es que los padres logren entender lo que está sucediendo, cosa que no siempre pasa”, concluye el experto.”[12]

Es de fundamental importancia que se les informe a los menores sobre los peligros de Internet y las redes sociales, desde espacios públicos como las escuelas, hasta en el propio hogar de cada familia.

“Los especialistas consultados coincidieron en ciertos criterios que deberían guiar un uso consciente, responsable y seguro de Facebook:

- No tener un millón de amigos. “Debemos ser muy selectivos y no agregar a alguien porque chateamos una vez o porque nos parece que lo conocemos. Está en juego nada menos que el acceso a información muy valiosa sobre nuestra vida”, advierte **Elías**. Según el experto, son 150 o 200 los contactos que una persona puede, razonablemente, conocer.
- No subir contenidos que puedan perjudicarnos. “No publiques nada en tu perfil que no te sientas cómodo adjuntando a un currículum o solicitud de beca”, recomienda Facebook. Monastersky es enfático al respecto: “Hoy en día, tu currículum es Internet. Y, por cómo funciona la Web, una vez que algo se sube ya nadie puede borrarlo; de ahí la importancia de pensar varias veces antes de publicar algo”.
- No divulgar datos personales delicados. Con el nombre completo y la dirección de correo electrónico es más que suficiente. No incluir domicilio, teléfono, ni situación sentimental. “No subir fotos de la familia ni de la casa, o información sobre las rutinas y actividades diarias… usar el sentido común pensando que alguien, eventualmente, podría acceder a esos datos con voluntad de hacer daño”, recomienda **Elías**.
- No usar aplicaciones desconocidas. Al hacerlo, el usuario comparte información valiosa sobre sí mismo y sobre sus contactos con los creadores de esos programas. ¿Qué hacen ellos con los datos? Quizás nada malo… pero quizás sí. “El usuario no tiene forma de comprobarlo. Además, es un hecho que gran parte de esas aplicaciones instalan virus y espías en las computadoras”, agrega Monastersky.
- Tener un perfil. A los que no están interesados en Facebook, Monastersky les recomienda que se registren y se contacten con sus conocidos, aunque después no usen la cuenta con frecuencia. “De lo contrario –sostiene–, le están dando, a quien quiera usurparles la identidad, una gran oportunidad de ser los primeros en generar un perfil falso y agregar a sus conocidos”.”[13]

Para evitar futuros problemas, es necesario seguir una serie de recaudos a la hora de utilizar el Facebook, como evitar la publicación de información personal delicada, no utilizar aplicaciones desconocidas y por último, no agregar contactos desconocidos.

[12] Miguel Sumer Elías, Abogado en Derecho Informático, Internet y Nuevas Tecnologías de Información. (Página consultada el 07 de Julio de 2010).[On-line]. Dirección URL: http://www.informaticalegal.com.ar/2009/12/02/facebook-el-peligroso/

[13] Miguel Sumer Elías, Abogado en Derecho Informático, Internet y Nuevas Tecnologías de Información. (Página consultada el 07 de Julio de 2010).[On-line]. Dirección URL: http://www.informaticalegal.com.ar/2009/12/02/facebook-el-peligroso/

Lo que se debe hacer al utilizar una red social, según el Ministerio de Justicia, Seguridad y Derechos humanos es:

"**Privacidad.** Ajuste sus opciones de privacidad para mantener su información fuera del dominio público.
Crear. Los padres pueden crear sus propias cuentas y "añadir" a sus hijos como contactos para monitorear sus actividades en línea.
Cuidado. Tenga cuidado con correos electrónicos que dicen provenir de su sitio de contactos sociales. No entregue información personal en respuesta a un correo electrónico.
Revisar. Para evitar fraudes, revise la dirección de URL en la parte superior de la pantalla antes de ingresar su nombre de usuario y clave en un sitio de contactos sociales - existen sitios impostores cuyo propósito es conseguir esta información, por lo que debe asegurarse de estar donde cree que está.
Reportar. Si se encuentra con algo sospechoso, repórtelo al sitio, o a una autoridad."[14]

Mantener la privacidad, monitorear a los más chicos, no confiar en cualquier correo que dice llegar de una red social, controlar la dirección de la red social antes de ingresar a la misma y denunciar toda conducta sospechosa.

Al contrario, lo que no se debe hacer es lo siguiente:
"**No poner fotos de otros sin su consentimiento**, sobretodo de menores de edad.
Intentar **evitar colgar fotos privadas** incluso de uno mismo.
No suministrar datos personales como dirección, teléfono ni la ubicación (donde se encuentra).
No admitir a desconocidos dentro de la red.
No permitir la recepción automática de comentarios de cualquier persona.
No responder a comentarios o e-mails mal intencionados o de personas desconocidas que hacen preguntas personales."[15]
No subir fotos de otras personas sin su aprobación, ni tampoco fotos privadas de uno mismo. No es recomendable divulgar datos personales, ni admitir a personas desconocidas o responder comentarios de desconocidos sobre temas estrictamente personales.

4. Como denunciar un delito informático

"Si Ud. ha sido víctima de un delito informático, tiene varias opciones en Argentina:

[14] Ministerio de Justicia, Seguridad y Derechos Humanos. (Página consultada el 18 de Septiembre de 2010). Presidencia de la nación, [On-line]. Dirección URL: http://www.jus.gov.ar/datos-personales/recomendaciones/redes-sociales.aspx
[15] Ministerio de Justicia, Seguridad y Derechos Humanos. (Página consultada el 18 de Septiembre de 2010). Presidencia de la nación, [On-line]. Dirección URL: http://www.jus.gov.ar/datos-personales/recomendaciones/redes-sociales.aspx

1. En la Ciudad de Buenos Aires, denunciarlo en la cámara del crimen de la Capital Federal (Viamonte 1147 PB, de 7,30 a 13,30) o en el fuero federal (Comodoro Py 2002, de 7,30 a 13,30). En el interior puede ir al juzgado federal mas cercano.
2. Ir a una Fiscalía federal o de de instrucción (dependiendo de la jurisdicción) o Fiscalia o Justicia Contravenciaonal de la C.A.B.A. (si corresponde la competencia en Buenos Aires) para que le tomen la denuncia. Para presentar una denuncia en el Ministerio Público de la Ciudad de Buenos Aires debe ir a la sede de Combate de los Pozos 155, de 9 a 20 horas o vía mail a denuncias AT jusbaires gov ar (solo para delitos del art. 128 -pornografía infantil- o art. 183/184 -daño informático- del Código Penal).
3. Denunciarlo en Policia Federal (teléfonos 101 ó 911) o en la sección Delitos de Tecnología (calle Cavia 3350, Piso 1º, Capital Federal, Tel.4370-5899, en el correo electrónico: analisis_criminal@policiafederal.gov.ar).
4. Acudir a la Dirección Nacional de Protección de Datos personales, en Sarmiento 1118 Piso 5, si el delito está relacionado con la privacidad o sus datos personales.
5. Hable con el Arcert de Argentina, no toman denuncias pues se centran en el Estado, pero podrán ayudarlo. CABASE tiene también un CESIRT para incidentes.
6. Consultar un abogado para iniciar una querella o denuncia penal.
Formalidades .No exiten formalidades. Si lo hace por escrito, el texto debe contener un descripción de los hechos, lo mas precisa posible, indicando la prueba que posee y si sabe quién es la persona que lo realizó.
CUESTIONES PROBATORIAS: Lo primero y más urgente que deberá hacer es juntar la prueba acudiendo a un informático junto a un notario o escribano y levantar un acta notarial. Tambien imprimir copias de todo y guardarlo notarizando el contenido. **Recuerde que todo lo que está en Internet se puede borrar en segundos y dejará de ser prueba para su caso!!!. La mayoría de los delitos informáticos no tienen condena por falta de pruebas."**[16]
En nuestro país tenemos varias formas de denunciar un delito informático, el camino ha tomar depende de cada uno. El tema más importante es el de la prueba, ya que la información subida en Internet puede ser borrada de un segundo a otro y sin pruebas, el delito queda impune. Lo esencial es levantar un acta notarial para que la prueba no se desvanezca.

5. Práctica Judicial

En la actualidad hay numerosos casos sobre el tema, el derecho a la intimidad ha sido objeto de novedosos ataques por medio de la Internet. Hoy en día, este derecho está mas vulnerable que nunca y por esa misma razón debe ser protegido con nuevas normativas.

Un hijo denuncia a su madre por violar su privacidad en Facebook

En este caso en particular, el punto está en decidir que predomina mas, el derecho a la intimidad de un menor en las redes sociales o la preocupación de una madre ante el cambio radical del comportamiento de su hijo. Es un límite que solo puede dar el juez ante cada caso concreto, aunque hoy en día se está viendo una expansión del derecho a la

[16] Pablo Palazzi, abogado, especializado en propiedad intelectual, datos personales, delitos informáticos y nuevas tecnologías. (Página consultada el 14 de Noviembre de 2010). [On-line]. Dirección URL: http://www.delitosinformaticos.com.ar/blog/como-denunciar-un-delito-informatico/

intimidad, adaptandose el mismo a las nuevas situaciones. Las redes sociales son relativamente novedosas, por lo que los problemas van a ser cada vez más frecuentes y la interpretación va a variar de caso en caso. Lo que si es claro es que el derecho a la intimidad puede ser vulnerado y este abuso debe ser sancionado, para evitar que en el futuro, se cometan nuevas violaciones al mismo.

"Madre e hijo en los tribunales por culpa de las redes sociales. El chico de 16 años ha denunciado a su madre por violar su privacidad al meterse en su perfil de Facebook y cambiarle la contraseña.

Denise New estaba muy preocupada por su hijo Lane, de 16 años tras recibir una llamada de un amigo del chico advirtiéndola de que éste tenía comportamientos extraños a causa de la turbulenta relación sentimental que estaba viviendo.

Lane, de 16 años salió de casa para dar una vuelta con sus amigos y su madre, Denise New, aprovechó que su hijo se había dejado su cuenta de Facebook abierta para poder husmear y saber cuáles eran las razones de su cambio de actitud.

La madre se encontró con que su hijo había publicado un comentario en el que afirmaba que había conducido a 150 km/h tras discutir con su novia.

Es por esto que Denise New creyó oportuno cambiar la contraseña de la cuenta de Facebook de su hijo para que éste no se conectara más y así evadirle de estos problemas.

Pero antes de ello, esta madre estadounidense publicó dos posts en el Facebook de Lane criticando varios comentarios suyos.

Lane descubrió la hazaña de la madre y la denunció por violación de privacidad, según ha publicado el 'Huffington Post'.

La primera vista del juicio se celebrará el 12 de mayo y los jueces decidirán si prevalece la preocupación de una madre por su hijo sobre la privacidad de éste en las redes sociales."[17]

Por orden judicial, quitaron un perfil falso de Facebook
El uso abusivo de Facebook para crear perfiles falsos y dañar el derecho a la imagen e intimidad de una persona, fue sancionado por un juez. Mediante una orden judicial, se ordeno que se de baja a la falsa cuenta, debido a que se estaba ocasionando un perjuicio irreparable en el actor y además se ordenó a los principales buscadores, que eliminen de sus búsquedas al actor, cuando los resultados estén relacionados con los hechos en autos. En este caso, no solo fue intimada la red social, sino también los buscadores que arrojaban como resultado, el perfil falso del actor, lo que implica que la protección del

[17] Miguel Sumer Elías, Abogado en Derecho Informático, Internet y Nuevas Tecnologías de Información. (Página consultada el 10 de Noviembre de 2010).[On-line]. Dirección URL: http://www.informaticalegal.com.ar/2010/04/09/un-hijo-denuncia-a-su-madre-por-violar-su-privacidad-en-facebook/

derecho a la intimidad es cada vez más intensa y extensa. Hoy en día un perfil falso en una red social popular puede llegar a ocasionar serios problemas a la persona afectada, ya que estas redes poseen tan nivel de difusión que la "mala publicidad" afecta en concreto y en forma gravísima a la persona vulnerada. La mayoría de la gente toma como cierto o por lo menos relativamente cierto lo que ve en un perfil de facebook, por lo tanto este abuso no debe ser permitido y mucho menos quedar impune.

"Lo dispuso una jueza de Rafaela, Santa Fe. Fue ante la presentación de una persona, que había denunciado la existencia de una cuenta en esa red social con su nombre, que él no había creado y cuyo contenido afectaba su imagen e intimidad.

La jueza Susana Rebaudengo, a cargo del Juzgado Civil, Comercial y Laboral Tercera Nominación de Rafaela, Santa Fe, ordenó a Facebook Inc. de Argentina quitar un perfil de esa red social**.**

Fue en una causa iniciada por una persona, luego de ésta que tomara conocimiento de la existencia de un perfil falso en Facebook con su nombre y sus datos personales, y en donde se incluían detalles sobre su orientación sexual.

En la resolución, la magistrada asegura que *"existiendo un alto grado de certeza que alcanza una evidencia tal que no admite, prima facie, posibilidad de discusión como asimismo entendiendo que nos encontramos ante una situación de urgencia como se está generando un perjuicio irreparable, previa la constitución de fianza por la suma de $ 30.000, con justificación de solvencia, ofíciese a Facebook Inc. de Argentina a los fines de que dentro del término de tres días procesa a bloquear y cancelar la cuenta existente en la red social Facebook a nombre del actor y se abstenga en adelante de habilitar el uso de enlaces, blog, foros, grupos, sitios de fans en los que se menoscabe u ofenda la imagen e intimidad del actor***".**

Asimismo, envió oficio a los buscadores de Internet Google, Yahoo! y Bing, para que *"realicen los actos necesarios para la eliminación del nombre e imagen del actor de los resultados de búsqueda con los sitios detallados en autos"*."[18]

Como se ve en estos dos casos, las redes sociales y principalmente el Facebook (que es la más popular) pueden llegar a usarse en forma abusiva, dañando la imagen e intimidad de las personas. En estos casos es cuando la justicia debe intervenir para que estas conductas sean interrumpidas y enmendadas.

Conclusión

A pesar de que el derecho a la intimidad está ampliamente regulado, todavía existen casos en los que la ley no alcanza a cubrir todos los supuestos que se dan hoy en día; esto

[18] Miguel Sumer Elías, Abogado en Derecho Informático, Internet y Nuevas Tecnologías de Información. (Página consultada el 10 de Noviembre de 2010).[On-line]. Dirección URL: http://www.informaticalegal.com.ar/2010/08/11/por-orden-judicial-quitaron-un-perfil-falso-de-facebook/

se debe a que Internet se desarrolla con tanta velocidad y rapidez que es imposible para la ley seguirle el paso. El crecimiento de Internet es casi ilimitado y tan avasallante que muchas veces se cae en las famosas lagunas del derecho y los jueces en estos casos, se encuentran casi impotentes ante la nueva realidad. Pensemos que el derecho a la intimidad en sus orígenes nació para proteger a los particulares contra los abusos del Estado, de terceros y de la prensa y que la ley fue evolucionando a medida que la sociedad avanzaba, hasta que apareció Internet que lo revolucionó todo. La Ley tuvo sus progresos con la sanción de la 25.326 y con la creación del Registro Nacional de Bases de Datos y además nos ofrece la posibilidad de acudir a la Dirección Nacional de Protección de Datos personales en caso de un delito informático, por lo que la protección ante una invasión a nuestra intimidad es razonable. El tema de la prueba es como mínimo complicado, ya que la información que existe en Internet cambia constantemente y puede desaparecer de un segundo a otro y la única forma de probar la comisión de un ilícito es por medio de un acta notarial.

Lo esencial es tomar ciertos recaudos a la hora de navegar por Internet. Es recomendable no divulgar información personal, ni llenar formularios en forma indiscriminada, ya que muchas veces se utiliza esta información con fines ocultos (en el mejor de los casos solo para publicidad). Es indispensable navegar en forma segura, siendo conciente de donde se está entrando y que es lo que se está viendo o bajando. El principal blanco de ataque son los menores, por lo tanto sus padres deben interiorizarlos acerca de los peligros de Internet; la educación es clave para evitar futuros problemas. Los niños deben saber que no es conveniente suministrar información personal a desconocidos (ya sea por medio del chat o de redes sociales) y que deben ser extremadamente cautelosos a la hora de navegar por la web.

Otro riesgo de navegar sin precaución es el relacionado a los programas maliciosos que se dedican al robo de datos personales y que se introducen al sistema en forma engañosa. Es importante conocerlos para evitar problemas a futuro, ya que estos programas suelen venir camuflados por medio del email, de sitios en internet y hasta se encuentran también dentro de las redes sociales (accesibles mediante links externos). La Dirección Nacional de Protección de Datos Personales ofrece información clara sobre el tema y sugerencias para navegar en forma segura, con el objeto de proteger nuestra intimidad y nuestros datos personales.

El tema Facebook es aún más complicado, ya que al ser las redes sociales algo relativamente novedoso, la jurisprudencia es variada. El gran problema actual es que las personas tienen el afán de hacer pública su vida privada, sin saber los riesgos que corren al develar datos personales en forma masiva. En el caso de los menores, lo más productivo es educarlos y explicarles los riesgos que se corren al difundir información personal, ya que prohibirles el uso no suele ser efectivo. La educación es imprescindible para evitar futuros problemas, ya que los niños no suelen tener en cuenta las consecuencias de sus actos y con tal de “estar a la moda”, no se preocupan en lo más mínimo por los potenciales peligros que se esconden detrás de las redes sociales.

Los padres tienen que enseñarles a sus hijos que la intimidad es un bien preciado y que deben saber cual información deben compartir y cual no. También es necesario que la

escuela se ocupe de estos temas y que el problema no les sea ajeno, ya que los niños suelen ser la víctima más frecuente de robos de identidad y de datos personales.

El Ministerio de Justicia, Seguridad y Derechos humanos también ofrece recomendaciones a la hora de utilizar una red social, como no compartir información privada y sensible, no admitir a desconocidos dentro de la red, no responder comentarios de desconocidos y que los padres tengan a sus hijos como contactos para poder monitorear su actividad. Lo cierto es que en general los más chicos no conocen los peligros reales de las redes sociales y aparte los padres no suelen ocuparse del tema en forma seria y responsable, lo que trae como consecuencia la indiferencia por parte de los jóvenes.

Como bien ha resaltado la jurisprudencia en los fallos comentados en el presente trabajo; el uso abusivo del Facebook puede atentar contra la intimidad, el honor y hasta contra la propia imagen de la víctima del ilícito. Lo cual deja en claro que el tema es bastante delicado y el daño en la persona afectada puede llegar a ser de una gravedad considerable.

Para finalizar, a mí juicio sería conveniente una campaña pública seria en torno a los peligros de Internet y de las redes sociales, ya que en general por ignorancia o indiferencia la mayoría de la gente no toma los recaudos necesarios a la hora de navegar por la web. La escuela también debería ocuparse del tema, educando a los niños sobre los peligros reales del uso imprudente de las redes sociales. Por último los padres tampoco deben estar ausentes del tema, ya que sus hijos son las víctimas más frecuentes de los delitos informáticos y deben concientizarlos de los riesgos concretos que corren al no tomar en serio la propia privacidad. La intimidad dejo de ser un bien preciado y pasó a ser uno prescindible en la actualidad, cada vez se la valora menos y se le da muy poca importancia, por lo que a mi entender se esta produciendo un retroceso en torno a la valoración del bien en la sociedad y esto trae como consecuencia el aumento de delitos informáticos y de robos de identidad, algo que debería ser tomado en serio por el potencial problema que puede provocar en los personas.