# RESPONSABILIDAD EN REDES SOCIALES

Magister Abogada María Del Carmen Becerra

mcbecerra2008@gmail.com

Prof.Legislacion Profesional.-Fundamentos Profesionales y legales F.C.E.F. y N.Universidad Nacional de San Juan

El presente trabajo se enmarca en el Proyecto: Integración de Tecnologías Informáticas como Soporte para los Sistemas de Información Código: 21-E-819 proyecto_integracion_tics@yahoo.com.ar

**Abstract**: La atribución de responsabilidad civil por la actividad en las redes sociales y buscadores nos plantea hoy más que nunca el problema del anonimato y de la sobre exposición de los usuarios que los llevan a publicar sus datos personales en sitios públicos que les ocasionan múltiples riesgos entre los que se encuentran las nuevas formas comisivas de los delitos tradicionales contra el Honor y otros derechos fundamentales de las personas. En este trabajo se intenta discutir si las soluciones que se vienen adoptando en materia de responsabilidad son coherentes con los desarrollos actuales del derecho de Daños, de la reglas tecnicas y de las políticas públicas para seguridad de la información dispuestas por la Legislación ArgentinaSGP.

**Palabras Claves**: Responsabilidad Civil y Penal en redes y buscadores. Factor de atribución**.** Responsabilidad en las Redes Sociales desprotección de los datos personales.

## I. Introducción:

Tal cual lo expresa la doctrina[1] en cuanto a la responsabilidad civil en relación a Internet "Nuestra Constitución Nacional y nuestro Código Civil, son ricos en herramientas para resolver cuestiones de responsabilidad en la era de la nueva tecnología sin perjuicio de que sería muy importante contar con una legislación especial que se ocupe de reglamentar estos principios para evitar interpretaciones contradictorias. El fundamento de la responsabilidad se encuentra toda vez que es violado el deber genérico de no dañar alterum non laedere que estaría consagrado en el Art. 19 de la Constitución Nacional.

Distinto es el caso de la responsabilidad penal que se basa en la existencia de una conducta antijurídica de un sujeto de derecho realizada con dolo o culpa en los supuestos de responsabilidad subjetiva o cuando exista responsabilidad objetiva en lo casos que la proceda o cuando exista un mandato legal en el supuesto de omisiones.

Así desde el punto de vista jurídico podemos decir que Internet se caracteriza por[2]:

1. **Igualdad de acceso** (es una red abierta)

[1] Castrillo Carlos V. Responsabilidad civil de los buscadores de Internet. Revista Jurídica Argentina. Tomo "A".2010.

[2] Parellada Carlos "Responsabilidad por la actividad anónima en Internet". Publicado en Le Ley ISSN 0024-1636

Todos tenemos igual posibilidad de acceder a Internet. En torno a ello surgen múltiples preguntas:¿Cuál es la ley que nos rige y protege?, ¿La ley del país desde donde accedo?

¿...del país desde se origina la comunicación?,¿... de los países por los que atraviesa?

¿... las de los todos? Y lo que sin duda esta fuera de discusión que no importa el lugar donde esta hospedado el material, si el fin es que se lea en un determinado país, estará en la jurisdicción de ese país.

**2. Desde cualquier ubicación geográfica**

Basta tener electricidad y teléfono. Tras una década de universo digital el último estudio de IDC patrocinado por EMC se ha llegado a calcular la tasa de crecimiento de la información revela que la cantidad de información digital creo en el 2009 un 62% más que en el 2008 alcanzando unos 8000 Gigabytes (0.8) Zettabyte y que en el 2010 creada en 2010 es ya de l.2. Zettabytes. Esto nos evidencia la avalancha de información generada por los individuales pero que las empresas tienen la responsabilidad de almacenar y administrar.

**3. Intangibilidad de la información, a pesar de existir interactividad**

El usuario puede generar contenidos –a diferencia de lo que ocurre en la T.V. convencional-. Cada suscriptor aporta a la red, al ingresar su estilo de vida, su profesión y hasta creaciones artísticas. Un informe de Comscore[3] revela que para comprender verdaderamente el panorama de los medios digitales, es esencial obtener una visión detallada de los consumidores que usan la tecnología y cómo lo utilizan. Es de vital importancia para los vendedores y desarrolladores de productos entender no sólo lo que los consumidores compran sino cómo instalar el software que compran, cómo interactúan con diversas aplicaciones y la forma en que configurar sus equipos. comscore captura con gran alcance, los datos continuos de cientos de miles de PCs en todo el mundo para que se conozca este comportamiento.

**4. Conexión individual a través de un Proveedor de Servicio o Acceso (PSI)**

Cada usuario se vincula mediante un contrato de provisión del servicio con quien dispone de conexión a la Red. Este contrato es un contrato de consumo (*) de servicios. Tal cual lo expresaran los autores Lofeudo y Olivera[4] "Queda demostrado que dichos contratos adolecen de vicios e incurren en abusos en sus términos. El usuario pierde el control de la información relativa a su personalidad y a derechos personalísimos, viéndose impedido de ejercer un efectivo control sobre estos datos.

**5. Conexión del Proveedor del Servicio a la Red**

El PSI está a su vez conectado a la Red a través de las Redes Regionales contractualmente.

Este es un contrato entre empresas, con conexidad al de consumo.

**6. Permite realizar el derecho de informar y a la información** (art. 13.1 Convención Americana de Derechos Humanos)

[3] http://www.comscore.com/Press_Events/Press_Releases///comscore.com. Consulta realizada el 10 de mayo de 2010.

[4]Ismael Lofeudo y Noemí L. Olivera. Redes sociales y derecho. La cuestión vista desde la perspectiva de los principios jurídicos y el derecho argentino. SID 2009. 38ªJAIIO...

"Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir información e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier procedimiento a su elección"

Permite realizar el derecho de informar y a la información, dentro de sus límites (art. 13.2 Convención Americana de Derechos Humanos)

"El respeto de los derechos y la reputación de los demás"

"La protección de la seguridad nacional, el orden público o la salud o la moral públicas"

## II.-Factor de atribución para la responsabilidad civil

- **¿Cuál es el factor de atribución del proveedor de acceso?**

  El proveedor de acceso sólo se obliga a posibilitar el acceso del usuario, y es una obligación de resultado en cuanto a que el usuario tiene su acceso garantido por el proveedor. Ninguna responsabilidad tiene respecto a los contenidos.

- **¿Cuál es el factor de atribución del proveedor de contenidos?**

  El proveedor de contenidos responde por su culpa en la producción de contenidos ilícitos o difamatorios. Se trata de un hecho del hombre y responde por culpa y dolo. La Ley 25.326 establece la figura del responsable del tratamiento de datos personales y la Ley 26.388 fija la responsabilidad penal.

- **Cuál es el factor de atribución del proveedor de hostings**

  El proveedor de hosting, normalmente sólo provee un espacio para que el proveedor de contenido despliegue su software y esté a disposición de los navegantes que lleguen al server a través de los proveedores de acceso.

  Este proveedor de hosting es siempre técnicamente identificable, a diferencia de lo que sucede con el proveedor del contenido.

  El proveedor de hosting es responsable sólo si conoce la ilicitud del contenido

  Si ha sido advertido de la ilicitud del contenido, y no ha procedido con la diligencia debida al bloqueo técnico del contenido dañoso.

**¿Cuál es la tendencia?**

La tendencia inicial de la jurisprudencia norteamericana y europea, ha sido que los proveedores de hosting respondan por los daños que producían los usuarios al honor, la privacidad, los derechos intelectuales de terceros a través de las páginas que alojan.

Esa tendencia se advirtió en EEUU en el caso "Stratton c/Prodigy" (N.Y.S.C., mayo 24-1995)

También en Francia, en el conocido caso "Hallyday, Estelle c/Lacambre, Valentin" (febrero 10-1999, C.Apel.París,sala 14, publicado en la Rev. De Resp.Civil y Seguros, To. 1999 pág. 1392)

En el caso "Stratton c/Prodigy" (N.Y.S.C., mayo 24-1995)

Se argumentó que Prodigy realizaba recomendaciones acerca a los usuarios para que se abstuvieran de mensajes obscenos o difamatorios y que hasta había censurado algunos.

De allí que algunos autores sostengan que si el proveedor de hosting asume un control del contenido, entonces, debe responder por los daños que derivan de la conducta de los proveedores de contenido.

Esa doctrina tiene cierta incoherencia, pues responsabiliza a quien previene y no responsabiliza a quien no previene.

También resulta incoherente en cuanto si aceptamos que el control es imposible, por la cantidad de material a controlar, entonces ¿por qué responsabilizar a quien se le escapó un contenido dañoso en su quimérico intento?

En caso "Hallyday, Estelle c/Lacambre, Valentin" se trataba de una página web que contenía una serie de fotos en que Halliday aparecía desnuda y sin haber dado autorización para su publicación, la que afectaba su intimidad, el derecho a su propia imagen y su desempeño profesional como modelo.

La sala 14ª de la Cámara de París, sostuvo que el proveedor de hosting a personas anónimas no podía ser considerado un simple mensajero o intermediario.

El tribunal aplicó el riesgo de empresa o actividad como factor de atribución.

Valoró especialmente que se trataba de una actividad lucrativa o remunerada

Sin embargo, la tendencia legislativa expresada en la Communication Decency Act, estableció una regla de inmunidad para el proveedor de servicios al disponer que no puede ser tratado como un editor de información provista por terceros.

La misma orientación exhibió la llamada Ley Multimedia de Alemania, que sólo responsabiliza al proveedor de servicio de hosting cuando conoce la ilicitud del contenido.

También la Directiva Europea sobre Comercio electrónico del 4 de mayo de 2000 se enroló en un criterio tuitivo de las empresas de servicios, cuando dispone, en su art. 14, que no responde, salvo que tenga conocimiento de la ilicitud o si no actúa con prontitud a retirar los datos, cuando tenga ese conocimiento

En la misma orientación se proyecta el derecho argentino, que establece que el proveedor de servicios es intermediario y no tiene responsabilidad, salvo que

- Sea originante de la información o seleccione el destinatario
- Sea quien seleccione los datos o los modifique
- Que conozca el contenido de la información es ilícito y que no retire o bloquee el acceso inmediatamente de tomar conocimiento

**Crítica a la tendencia**

Ahora bien, si la decisión es ser tolerante con los proveedores de hosting, al menos creemos -con Cavanillas Mujica[5]- que se hace necesario consagrar la obligación de identificar a los almacenantes, pues de lo contrario se vuelve demasiado gravosa la situación de las víctimas de los daños

La tendencia legislativa a la inmunidad de los proveedores de servicios de hosting aparece avalada por el argumento del problema técnico del control del contenido y el consiguiente aumento de los costos de tales empresas, que es un argumento atendible, pero no definitorio

Ciertamente, los costos de la responsabilidad para las empresas de hosting en un sistema en que son responsables son grandes;

Pero no hay que olvidar que la inmunidad no evita el costo, sino que simplemente lo distribuye sobre un número indeterminado y aleatorio de víctimas.

De allí, que nos parezca más justo un sistema que abarque –al menos- los daños sufridos por los casos de anonimato.

Cuando el autor aparece cubierto por el modo de organización del sistema, el factor de atribución del riesgo de empresa, parece satisfacer mejor el ideal de justicia que el sistema de la inmunidad.

Desde el ángulo de la protección al consumidor, creemos que se nos abren algunas vías para la protección de los usuarios que resulten víctimas de daños producidos por la difamación, atentados al honor y a la intimidad de las personas.

En efecto, el art. 40 de la Ley 24.240 reza: "Si el daño al consumidor resulta del vicio o riesgo de la cosa o de la prestación del servicio, responderán el productor, el fabricante, el importador, el distribuidor, el proveedor, el vendedor y quien haya puesto su marca en la cosa o el servicio. … La responsabilidad es solidaria, sin perjuicio de las acciones de repetición que correspondan. Sólo se liberará total o parcialmente quien demuestre que la causa del daño le ha sido ajena"

**Cuando el servicio ha sido organizado de una manera tal que posibilite las lesiones a los intereses de terceros sin posibilidad de que nazca el crédito indemnizatorio por el anonimato, nos parece que no podría admitirse como excusa que la difamación o el atentado es causa ajena al organizador del servicio.**

En primer término, pues la jurisprudencia –incluso la norteamericana- ha establecido que el organizador del servicio no puede mantener reserva acerca de la identidad usuario dañador.

En efecto, cabe recordar que el principio de la reserva de identidad del usuario que ha difamado ha sido descartado en la jurisprudencia de los EEUU de Norteamérica. Nam Tai Electronics exigió a AOL que le facilitara la identidad de la persona que se escondía tras el nick 'scovey2' ya que entendía la había difamado. La empresa AOL (de la que era usuario el supuesto injuriante) se negó invocando la Primera Enmienda de la Const. de los EE.UU. La decisión fue adversa a la reserva de identidad

[5] CAVANILLAS MUJICA, Santiago, "La responsabilidad civil de los intermediarios en Internet en Ameal, O (Dir)-Gesualdi, Dora M. Derecho Privado, Libro Homenaje a Alberto Bueres".B.S.As, Hammurabi. Pág. 1719 y sgtes.

En segundo lugar, porque no parece razonable que sea más protegido el derecho de propiedad intelectual que los derechos de las personas. Y en tal sentido, creemos que no sería admisible la defensa del organizador del servicio de que la causa es ajena –defensa que en principio admite el art. 40 de la L.P.C.-

Y no lo sería, pues a la luz de la misma jurisprudencia norteamericana, resulta que se ha entendido que el organizador de un sistema que permite el atentado contra la propiedad intelectual es un infractor de segundo grado, que no puede escudarse en que no ha sido su propio hecho el que ha infringido las normas protectoras de la propiedad intelectual, sino los hechos de terceros.

Napster es un software que permite a sus usuarios buscar en el sitio la música que otro usuario del sitio posee en su propio ordenador y bajarla a la PC del que ha emprendido la búsqueda; Napster no reproducía ni ejecutaba la música, sino que simplemente permitía por su intermedio el intercambio que los usuarios producían entre sí.

El fallo de la Novena Corte de San Francisco que desestimó la defensa de Napster establece que "Napster es un infractor de segundo grado de las violaciones a los derechos de autor, ya que a través de su conducta ha amparado a sabiendas las infracciones por parte de los usuarios del sistema".

Crítica a la tendencia

Resulta –entonces- que si Napster es un infractor de segundo grado a la ley de protección del copyright, parece coherente sostener que quien organiza un servicio del cual resulta daños al honor y la intimidad de las personas, sea igualmente responsable de la posibilidad que brinda a la afectación impune de tales derechos.

Al desaparecer su carácter de dueño o guardián, entonces, ni siquiera las normas de la responsabilidad objetiva del art. 1113 del Código Civil Argentino, nos resulta eficaces para hacer efectiva la responsabilidad.

Para lograrlo deberíamos establecer tal como lo hace la norma del art. 48 de la Ley 24.051 que originante de un residuo peligroso no pierde el carácter de propietario o guardián por la transmisión de la propiedad ni por el abandono.

La misma solución debería extenderse al creador del virus.

Ahora bien, en la medida que las legislaciones no superen los problemas del anonimato e impongan ese deber de identificación a los usuarios y proveedores de contenidos, las víctimas serán sacrificadas sobre el falso argumento de la libertad de expresión.

Decimos falso argumento pues la libertad de informar y ser informado no es absoluta, como cualquier otra libertad, sino sujeta en cuanto a su ejercicio a sus justos límites.

Y entre los límites de la libertad de expresión, está la responsabilidad por los daños causados a terceros.

Sin lugar a dudas, Internet es el lugar ideal para lograr la vigencia efectiva del derecho a informar y ser informado consagrado por el art. 13.1 Convención Americana de Derechos Humanos, en cuanto dice: "Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir información e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier procedimiento a su elección"

Por ello, no alentamos ninguna forma de censura.

El Estado Argentino ha reconocido el valor de la Red en orden al lugar ideal para el derecho de informar y a ser informado, y ese reconocimiento –lamentablemente, por decreto, en lugar de haber sido una expresión del

Congreso de la Nación, está contenido en el Decreto No. 1279/97, que declara: "el servicio de INTERNET, se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión, correspondiéndole en tal sentido las mismas consideraciones que a los demás medios de comunicación social"
En ese mismo decreto, entre sus considerandos, ha recordado la decisión de la Corte Suprema de Justicia de los Estados Unidos de América al decir: "... no se debería sancionar ninguna ley que abrevie la libertad de expresión... la red INTERNET puede ser vista como una conversación mundial sin barreras. Es por ello que el gobierno no puede a través de ningún medio interrumpir esa conversación... como es la forma más participativa de discursos en masa que se hayan desarrollado, la red INTERNET se merece la mayor protección ante cualquier intromisión gubernamental."
El derecho a expresarse tal como está consagrado por la Convención Americana de Derechos Humanos, está limitado por:"El respeto de los derechos y la reputación de los demás" y "La protección de la seguridad nacional, el orden público o la salud o la moral públicas"[6]
Por ello, nos parece claro que no se trata de propugnar la censura; sino que el organizador es quien ha desnaturalizado el derecho de expresión al frustrar la posibilidad de identificación de quien traspasa los límites del derecho.
La regla es que tengo el derecho a expresarme pero dentro de los límites de ese derecho, y bajo la responsabilidad de quien ejerce el derecho.
El organizador no puede censurar, pero tampoco puede brindar el mecanismo para encubrir el ejercicio abusivo o excesivo del derecho, y del espíritu del ordenamiento jurídico surge la antijuridicidad de su conducta.
**Una razón que justifica su responsabilidad es que ha creado el riesgo y que es el propio del sistema organizado sobre la base del anonimato que, precisamente, ha posibilitado el daño.**

En nuestro país se dicto el año pasado el primer fallo relativo a la responsabilidad civil por la actividad de los buscadores de Internet.
La jueza Virginia Simari, titular del Juzgado Nacional en lo Civil Nº 75[7], hizo lugar una demanda presentada por la cantante Virginia Da Cuhna contra Google Inc. y Yahoo de Argentina SRL, por vincular e incluir en sus respectivos buscadores de Internet páginas de contenido sexual donde vinculaban su nombre, imagen y fotografías con esos sitios y actividades.
En razón de ello, Da Cuhna reclamó una indemnización como reparación del daño material y moral. Asimismo, solicitó el cese definitivo "del uso antijurídico y no autorizado de su imagen y de su nombre", así como "la eliminación de su imagen y nombre de los sitios de contenido sexual, erótico y pornográfico denunciados".

[6] art. 13.2 de la Convención Americana de Derechos Humanos
[7] www.cij.gov.ar/buscador.html

En el fallo recaído la jueza alega que la antijuricidad se la tiene por configurada con un criterio amplio cuando aparece violado el deber genérico de no dañar alterum non laedere que e halla consagrado en el art. 19 de la Constitución Nacional.

El factor de atribución lo encontró en los antecedentes fácticos y concretamente en la responsabilidad que se relaciona con actividades desplegadas por medio de sistemas informáticos y con sus consecuencias respecto de la tutela de la privacidad de los individuos.

Se fundó en lo dispuesto por los principios que gobiernan la responsabilidad civil en general, y en los Artículos 902 y sgtes, 1066 a 1069, 1072 a 1083, 1109 y 1113 del Código Civil pero antes de eso por la manda del Artículo 19 del que deriva el derecho a no ser dañado y en su caso a ser resarcido.

En consecuencia, la jueza ordenó a las compañías demandadas pagar una indemnización por el daño moral que le causó a Da Cuhna la situación denunciada.

En su demanda, Da Cuhna indicó que esa situación constituye un avasallamiento a sus derechos personalísimos al honor, al nombre, a la imagen y a la intimidad, al haber sido vinculada a páginas de Internet de contenido sexual, erótico y pornográfico y asimismo por la utilización comercial y no autorizada de su imagen.

La jueza Simari destacó que "los buscadores operados por las demandadas también son sitios de Internet, y sus autores y/o responsables deciden qué contenidos incluyen o no en los mismos".

Agregó que "su quehacer constituye un servicio que facilita la llegada a sitios que de otro modo serían de muy dificultoso acceso, y además, esa facilitación hace precisamente al núcleo de una de las actividades centrales que desarrollan".

"Así pues, nos hallamos en condiciones de afirmar que el buscador al contribuir al acceso a los sitios de Internet se encuentra en las mejores condiciones técnicas para prevenir la eventual generación de daño y de allí surge el perfil de los buscadores como responsables de su actividad facilitadora del acceso a sitios".

Con relación al daño causado, la magistrada consideró la circunstancia de que la accionante transite una actividad profesional que por esencia requiere la exposición pública de su físico y m s precisamente de su imagen, no legitima cualquier clase de exposición de su figura por terceros.

"El estándar para valorar un supuesto de afectación a la imagen, está conformado por el contexto en que las imágenes supuestamente atentatorias, hayan sido difundidas. En el caso, la presencia de la de la actora en páginas de contenido sexual, erótico, pornográfico no deja margen para la duda acerca de su entidad para afectarla"

.

## III.-El Anonimato.

Existe un anonimato relativo que dificulta establecer autoría. En las redes sociales se generan posibilidades de anonimato y en algunos casos se alientan estas conductas.

El anonimato obsta la responsabilidad, pues para que alguien sea responsable debe estar identificado. Por ello, es un principio la necesidad de identificación en la red; es necesario saber quienes son los que se ponen en contacto.

Existe un anonimato relativo que dificulta establecer autoría.El problema de la autoría se relaciona –en nuestra concepción- con el requisito de la relación causal Es el problema de establecer quién ha puesto la causa del daño. A quien le es imputable fácticamente la conducta dañosa.

La existencia de posibilidades de anonimato ha determinado que las directivas y leyes europeas imponen un deber a las proveedoras de servicios de Internet de identificar a los usuarios y a quienes se comunican a través de la Red.

El deber de identificación ha sido la solución que encontraron los europeos para que las víctimas tuvieran contra quien accionar en caso de daños

Pero nuestra problemática es la carencia de deber de identificación lo que dificulta la solución [3].

Existe un anonimato relativo, La doctrina[8] también ha expresado su preocupación sobre el problema del anonimato de los usuarios y de los contenidos ilícitos y nocivos que éstos puedan publicar en la Red

¿Quiénes interactúan en Internet?

■El usuario: Sin embargo aquí hay que aclarar que a fin de incorporarse a las redes sociales el usuario debe definir su perfil donde se va ha engolar un cúmulo de información que lo va a definir en la forma como se presenta en la sociedad. Hay usuarios de salas de chat, o foros.

■Los amigos: Son enlaces que vinculan perfiles y tienen por objeto propiciar las relaciones entre los sujetos [1].

■El proveedor de contenidos

■El prestador de servicio de almacenamiento (hosting)

■El proveedor de acceso que son quines brindan la infraestructura de telecomunicaciones y/o de cable distribución que permiten el transporte de la información digitalizada.

## IV.-Políticas de Estado.

Según las Políticas Públicas de seguridad de la Información dispuestas por la ONTI y adoptadas en Argentina por Decisión Administrativa 669/2002 y Resolución SGP 45/2005, los criterios básicos para clasificar y tratar la información están basados en los perjuicios que pueden ocasionarle a la empresa el incumplimiento de alguno de los valores generales de seguridad definidos en las políticas de seguridad de la información.

Conforme dichas políticas establecidas a nivel nacional el propietario de la información debe analizar la información a su cargo para proceder luego a su clasificación, basándose principalmente en los perjuicios que

[8] Parellada, Carlos. Obra citada.

pudiera ocasionarle al organismo y/o personas, el incumplimiento de alguno de los valores generales de seguridad definidos en la Política de seguridad de la información adoptada por la empresa.

A su vez las Políticas Públicas dividen la información en:

1. De acceso Público- De uso General
2. De acceso reservado (uso interno) y confidencial
3. De acceso Secreto
4. Propia de los Usuarios de los sistemas

Para la primera no es necesario establecer restricciones especiales, más allá de recomendaciones para su buen uso y conservación [2].

De acuerdo con las políticas Pública establecidas en nuestro país para la información de acceso Reservado se deben cumplir las siguientes consideraciones:

Autorización: Los usuarios que por la naturaleza de su trabajo se les permita el acceso a esta información, deben estar expresamente autorizados por los correspondientes propietarios de la información.

El acceso en los sistemas debe establecerse a través de un adecuado sistema automático de control de accesos.

El propietario de la información debe definir los tipos de permisos para que los usuarios puedan acceder a la información, ya sea de lectura, modificación y/o eliminación. El propietario de la información debe autorizar expresamente el uso de esta información con propósitos de prueba en el desarrollo y/o mantenimiento de sistemas.

Conservación: La información que hace al funcionamiento de la empresa, no debe conservarse en los equipos de procesamiento individuales, sino exclusivamente en los equipos de procesamiento centralizados.

Debe incluirse el tratamiento de la misma en os procesos habituales de generación de copias de respaldo y planes de recuperación de procesamiento.

Deben implementarse políticas de “escritorios vacíos” conservando todo documento impreso bajo llave.

Envío: Se debe asegurar la existencia de controles sobre la integridad, exactitud, confidencialidad e inviolabilidad de los datos transmitidos electrónicamente, que aseguren la correcta recepción del envío por parte del destinataria.

Impresión: Se debe evitar la impresión de documentos más allá de lo imprescindible para efectuar las tareas diarias y a través de impresoras colas de impresión de acceso restringido.

Divulgación a terceros:

Se deben instrumentar convenios de confidencialidad con terceros que necesariamente deban/puedan acceder a información de la empresa, ya sea directamente para desarrollar sus actividades o porque al efectuar sus tareas puedan acceder a información, por ejemplo personal de mantenimiento de equipos, de limpieza, etc.

No se debe transmitir información en forma verbal y/o escrita a personas externas a la empresa sin la autorización expresa del propietario de la información.

Se debe incluir en los contratos comerciales todos los requerimientos de control que requieran las políticas de seguridad de la empresa.

Destrucción:

Se debe destruir toda la información y sus correspondientes soportes lógicos/físicos cuando se considere en desuso.

Para la información de acceso secreto y que puede presentar riesgos importantes para la empresa, se deben cumplir las siguientes medidas adicionales de seguridad:

Se deben encriptar todos los archivos de datos sensibles tanto de producción como de cualquier otro ambiente en cualquiera de las siguientes situaciones:

- Procesamiento diario
- Conservación de sistemas
- Transmisión electrónica a través de redes
- Generación de copias de respaldo
- Conservación de logs de eventos.

El propietario de la información correspondiente debe conservar toda información clave para la ejecución de los procesos de encriptado y desencriptado. Para los reportes conteniendo información confidencial se deben utilizar impresoras dedicadas y de acceso físico restringido sólo a los usuarios autorizados.

Para la destrucción de los soportes impresos se deben utilizar trituradora de papel. No está permitido el uso de la información reservada y/secreta para propósitos de prueba en los desarrollos y/o implementaciones de sistemas, salvo expresa autorización del propietario de la información.

Para la información propia de los usuarios que este conservada en los equipos informáticos (archivos correos electrónicos residentes en los servidores de datos centralizados y/o estaciones de trabajo) de propiedad de la empresa y no de los usuarios que los operan, por lo que podrá ser administrada y/o monitoriada por la Subgerencia de Sistemas y la auditoría interna [4], de acuerdo a las pautas de seguridad definidas. En caso de que el usuario solicite una excepción, deberá estar debidamente justificada, ser autorizada por la autoridad pertinente e informada a quien corresponda.

Jerarquías de Clasificación de acuerdo a la óptica de la preservación o protección y según el nivel de confidencialidad e importancia de los datos se proponen las siguientes jerarquías [5].

a) Información Estratégica: Información muy restringida, muy confidencial

b) Información Restringida: Debe ser protegida siempre como información sensible y tratada como información crítica, reservada solo a sus propietarios.

c) Información de uso Interno: A disposición de todos los empleados

d) Información de uso general: Sin restricción para su uso.

Rotulado y manejo de información

La Norma [6] establece que es importante que se defina un conjunto de procedimientos adecuados para el rotulado y manejo de la información, según el esquema de clasificación adoptado por la empresa. Estos procedimientos deben incluir los recursos de información en formatos físicos y electrónicos. Para cada

clasificación, se deben definir procedimientos de manejo que incluyan los siguientes tipos de actividades de procesamiento de la información:

1. Copia
2. almacenamiento
3. transmisión por correo, fax y correo electrónico transmisión oral, incluyendo telefonía móvil, correo de voz, contestadores automáticos.

## V. Responsabilidad en las Redes Sociales por la desprotección de los datos personales:

En los últimos tiempos, los servicios de redes sociales han experimentado gran auge entre el público. Entre otras cosas, estos servicios ofrecen medios de interacción basados en perfiles personales que generan sus propios usuarios registrados, lo que ha propiciado un nivel sin precedentes de divulgación de información de carácter personal de las personas interesados (y de terceros).

Aunque los servicios de redes sociales aportan un amplio abanico de oportunidades de comunicación, así como el intercambio en tiempo real de todo tipo de información, la utilización de estos servicios puede plantear riesgos para la privacidad de sus usuarios (y de terceras personas): los datos personales relativos a las personas son accesibles de forma pública y global, de una manera y en unas cantidades nunca sin precedentes, incluidas enormes cantidades de fotografías y vídeos digitales, sin perjuicio de las distintas actividades delictivas que se pueden llevar a cabo usando estas redes como medios para la comisión de ilícitos (Delitos Informáticos, Delitos contra el Honor, contra la propiedad intelectual, industrial, etc.).

Por último, es importante tener en cuenta que en la gran mayoría de ocasiones, 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 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. En síntesis, el abanico de posibilidades de infracción a los derechos de intimidad y privacidad en las redes sociales es muy amplio, ya sean estos ilícitos cometidos por otros usuarios de las redes o por terceros.

En estos casos, la persona afectada podrá reclamar los daños y perjuicios ocasionados mediante una acción judicial.

Ley 25.326 de Protección de Datos Personales protege los datos personales en bases de datos ya sean de acceso público o privadas destinadas a publicar informes.

Esta ley no protege la autoría o propiedad de la base de datos en si, sino el derecho del titular de los datos (persona a quien refiere los datos) al acceso, honor, intimidad y correcto uso y tratamiento de los mismos según lo establece el artículo 43 de la Constitución Nacional.

Para esto la ley establece la obligatoriedad de la inscripción de la base de datos cumpliendo con ciertos requisitos y el incumplimiento de esta obligación resulta en infracción penada con multas y clausura de la base de datos.

Por otra parte, esta ley introdujo en nuestro Código Penal, penas de prisión de 6 meses a 3 años a aquella persona que brinde datos falsos a sabiendas a un tercero contenidas en una archivo de datos personales y si además se causa un perjuicio a alguna persona la pena se incrementa de un mínimo de 9 meses a 4 años y medio.

También reprime con la pena de prisión de un mes a dos años al que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

El órgano responsable de llevar el registro y control de estas bases de datos así como su protección es la Dirección Nacional de Protección de Datos Personales que depende del Ministerio de Justicia y Derechos Humanos.

Este organismo en su página web prevé una serie de recomendaciones:

"Consejos básicos para el uso de las redes sociales con Protección de Datos Personales" Facebook, HI5, y otros…

Las redes sociales generalistas o de ocio cuentan con un nivel de riesgo superior al de las redes sociales profesionales, dado que los usuarios exponen no sólo sus datos de contacto o información profesional (formación, experiencia laboral), sino que se pueden exponer de manera pública las vivencias, gustos, ideología y experiencias del usuario, lo que conlleva que el número de datos de carácter personal puestos a disposición del público es mayor que en las redes sociales de tipo profesional. Asimismo, se tratan datos especialmente protegidos, lo que supone un mayor nivel de riesgo para la protección de dichos datos personales y, por ende, del ámbito de la privacidad e intimidad de los usuarios.

Entre las principales situaciones, cabe señalar las siguientes:

• Existe un problema derivado de la falta de toma de conciencia real por parte de los usuarios de que sus datos personales serán accesibles por cualquier persona y del valor que éstos pueden llegar a alcanzar en el mercado. En muchos casos, los usuarios hacen completamente públicos datos y características personales que en ningún caso expondrían en la vida cotidiana como ideología, orientación sexual y religiosa, etc.

• Los datos personales pueden ser utilizados por terceros usuarios malintencionados de forma ilícita.

• Existe la posibilidad de que traten y publiquen en la Red información falsa o sin autorización del usuario, generando situaciones jurídicas perseguibles que pueden llegar a derivarse de este hecho.

• El hecho de que, a través de las condiciones de registro aceptadas por los usuarios, éstos cedan derechos plenos e ilimitados sobre todos aquellos contenidos propios que alojen en la plataforma, de manera que pueden ser explotados económicamente por parte de la red social.

## VI. Delitos Informáticos en las redes sociales.

La legislación argentina cuenta con una Ley específica sobre Delitos Informáticos, Ley 26.388.

En la misma, se encuentran regulados los siguientes:

• Pornografía infantil por Internet u otros medios electrónicos (art. 128 CP)

• Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º CP)

• Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP)

• Acceso a un sistema o dato informático (artículo 153 bis CP)

• Publicación de una comunicación electrónica (artículo 155 CP)

• Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP)

• Revelación de información registrada en un banco de datos personales (artículo157 bis, párrafo 2º CP)

• Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP; anteriormente regulado en el artículo 117 bis, párrafo 1º, incorporado por la Ley de Hábeas Data)

• Fraude informático (artículo 173, inciso 16 CP)

• Daño o sabotaje informático (artículo 183 y 184, Incisos 5º y 6º CP).

En este orden, bastaría solo dejar en claro que de acuerdo a estas modalidades delictivas descriptas arriba, entendemos que, según la situación, pueden ser cometidas tanto como por los mismos usuarios de la red social, personas ajenas a esta, o por la misma persona o empresa propietaria del sitio web.

## Conclusiones:

1) Internet presenta una arista que se muestra muy rebelde a la sujeción a la responsabilidad civil, que es el anonimato, en tanto, él dificulta hallar a los autores –de mensajes obscenos indecentes y de virus y espionaje electrónico-

2) El imperativo es la consagración del deber de identificación de los usuarios y proveedores de contenido a través de los servicios de acceso y provisión de espacios. También se torna impostergable la necesidad de identificar y registrar las bases de datos públicas y privadas que operan en las redes sociales.

4) Se deben establecer reglas claras sobre como actuar, compartir experiencias, difundir y educar y propiciar la creación de una Guía Latinoamericana para el uso de las redes sociales.

## Referencias:

[1]XCO-Community. Desconocidos en las redes sociales. 2008.-

[2]Becerra, María. Seguridad del Correo Electrónico. Revista “La voz del Foro”.Publicada por el Foro de Abogados de San Juan.2005.-

[3] www.mattica.com.

[4]NORMA IRAM ISO IEC 17799.Punto 6.Seguridad del Personal.Pag.26

[5]Becerra, Maria. Tesis “Metodologías de Clasificación y tratamiento de la Infomación”.Universidad Nacional de la Matanza. 2007.

[6] Normas ISSO IRAM 17.799