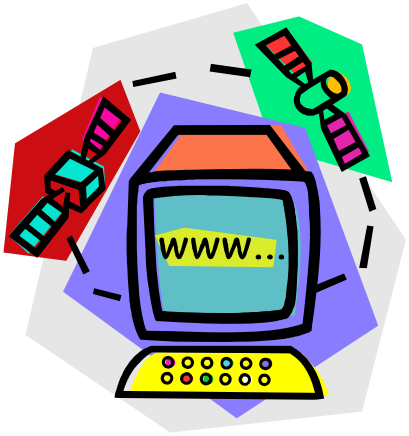
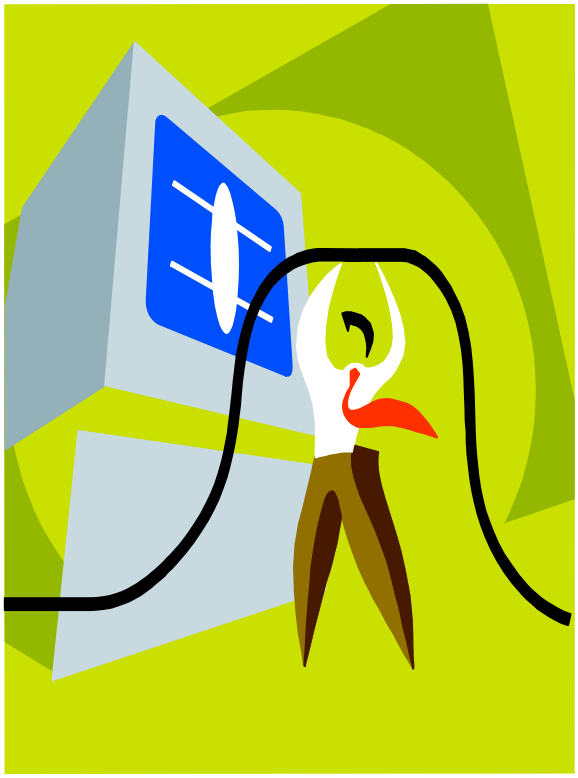
“LA TECNOLOGÍA Y LA INTIMIDAD PERDIDA”

TESINA





UNIVERSIDAD NACIONAL DE GENERAL SAN MARTIN (UNSAM)

FUNDACIÓN DE ESTUDIOS SUPERIORES E INVESTIGACIÓN (FUNDESI)

CARRERA DE POSGRADO: ABOGADO ESPECIALISTA PARA LA MAGISTRATURA

TESINA

“LA TECNOLOGÍA Y LA INTIMIDAD PERDIDA”

Tesista: Dra. María Lucía ANTUZ

Director de Tesis: Doctor en Derecho y Ciencias Sociales, José Daniel CESANO

Asesora Metodológica: Magister Sc., Delia Elena VERA BARROS

AÑO 2010

Neuquén

República Argentina.

INDICE

INTRODUCCIÓN

Las cuestiones que se abordarán en este trabajo se encuentran relacionadas al crecimiento de Internet y de las redes sociales informáticas en los últimos tiempos, por la multiplicidad de fines que tienen hoy estas redes, que abarcan lo académico, cultural, empresarial, etc. y que implican un dinamismo sin fronteras, en tanto medio de comunicación de difusión mundial y los problemas que se plantean en relación a la libertad de expresión y la intimidad en este ámbito.

El desarrollo del tema se dividirá en cuatro tópicos. Así, en el primero se precisarán conceptos básicos en cibernética. En el segundo se caracterizarán los denominados derechos personalísimos -libertad de expresión e intimidad- que han renacido como consecuencia de las agresiones provenientes de la utilización de las técnicas electrónicas. Se analizará la protección civil de la intimidad en el art. 1071 bis del Código Civil, los aspectos más relevantes del instituto incorporado por dicho precepto legal, el bien jurídico que se trasluce en la protección de los datos personales, la evolución legislativa, y el derecho a la intimidad como objeto del habeas data. Frente a la insuficiencia legislativa imperante en la materia y a la necesidad del ser humano de controlar la información en todo el proceso destinado a obtenerla, se hará referencia al derecho a la autodeterminación informativa. En el acápite tercero se abordarán los fundamentos de la responsabilidad civil frente a un supuesto de conducta arbitraria en la interferencia al derecho a la privacidad o hecho ilícito informático. Aludiremos a los daños que puede causar a terceros el empleo de los sistemas avanzados de comunicación automatizada, el tratamiento de los datos por medio de la interconexión de los ordenadores y su ulterior divulgación en el medio social donde se aplican los sistemas magnéticos. El cuarto apartado estará destinado a efectuar consideraciones de carácter político-criminal y describir los nuevos delitos en la materia, introducidos por la Ley 26.388 al Código Penal. A modo de colofón se darán las conclusiones y reflexiones finales, intentándose proponer una solución concreta a tales contingencias y que resulte respetuosa del principio de legalidad.

Sin desmerecer los beneficios de los sistemas informáticos en general, pues brindan la posibilidad de acceder a sus contenidos de una manera más simple, favorecen el entendimiento entre culturas, el intercambio de experiencias y el avance de las distintas disciplinas científicas que pueden contribuir al interés general y al bien común,

es menester que se preste atención y regule el frecuente uso indebido de aquéllos, ya que puede derivar en la comisión de delitos de esta índole.

Internet es un instrumento útil a la hora de revisar, obtener información, desarrollar habilidades y relacionarse y ha posibilitado el auge de un inmenso mercado virtual a través del cual se celebran millones de contratos de consumo. Pero, Internet también es una pieza del movimiento postmoderno que muestra al mundo como un lugar siniestro bajo el dominio de cada aspecto de la vida por los sistemas de computadoras; o en la gran ciudad sin policía que es el ciberespacio facilita la expansión de la depravación; la proliferación de crackers, que mediante la interactividad utilizan en su provecho referencias de tarjetas plásticas o de passwords ajenos; la difusión de bancos de datos que ponen en jaque a la intimidad invadiendo en especial los datos sensibles. [Razón por la cual] el 24 de septiembre de 1998 el Consejo de Europa (98/560/EC) recomendó aplicar ciertos estándares, entre ellos dar clara información a los usuarios sobre los riesgos inherentes a los servicios on-line y reducir "los contenidos ilícitos ofensivos para la dignidad humana que circulan en servicios audiovisuales y on-line" y el uso indebido de las redes (art. 2.2.2.a).[1]

En mérito a que el comercio electrónico -mediante la red Internet- es un fenómeno nuevo, requiere de un marco jurídico pertinente para desarrollarse y consolidarse. La red se erige como un instrumento tecnológico -fruto de la revolución digital y del avance de las comunicaciones en general- que mejorará substancialmente las relaciones entre los países en general y comerciales, en particular. El carácter internacional de la red -que se expande por el ciberespacio- acrecienta la inseguridad jurídica devenida de la dificultad de cómo solucionar los problemas jurídicos -no sólo de índole contractual y comercial- que se produzcan en el espacio no regulado (aquí surge la idea de la "ley del ciberespacio").[2]

Cabe agregar en este introito, evocando a Gozaíni, que: “Las nuevas tecnologías de la información son un arma de doble filo: aumentan nuestras capacidades y nuestro poder, pero también hacen a sus usuarios más vulnerables a la vigilancia y a la manipulación. Ambos aspectos son inseparables: es precisamente lo que aumenta nuestras capacidades lo que nos hace más vulnerables. El ciberespacio no constituye

[1] ALTERINI, Atilio Aníbal, “Respuestas ante las nuevas tecnologías: Sistema, principios y jueces”, LA LEY 2007-F, 1338.
[2] CAFFERATA, Fernando J., “Utilización de la red de internet. La jurisdicción y el derecho aplicable para solucionar conflictos”, LA LEY 2001-B, 1281-LLP 2001, 801. Derecho Comercial Doctrinas Esenciales, Tomo II, 1237.

una excepción: navegar por la red nos permite nuevas formas de comunicación con personas de todo el mundo, pero también, puede significar que todas nuestras comunicaciones puedan ser interceptadas por terceros que, al mismo tiempo, nos localizan e identifican. Esto puede querer decir que otras personas o grupos están construyendo un perfil de nosotros mismos: qué direcciones visitamos, qué anuncios nos interesan, qué productos compramos, a qué periódicos nos suscribimos o con quién mantenemos correspondencia electrónica. Podría incluso ocurrir que personas totalmente desconocidas accedan al disco duro de nuestro ordenador personal, observen lo que guardamos en él, quizás decidan cambiar o borrar ciertos archivos o transmitirnos un virus. Desde luego, puede no ocurrirnos nada parecido; pero podría ocurrir".[3]

DESARROLLO DEL TEMA

I.- Definiciones conceptuales

Una *red* es un sistema donde los elementos que lo componen denominados ordenadores, son autónomos y están conectados entre sí por medios físicos o lógicos y que pueden comunicarse para compartir recursos. Las redes están formadas por conexiones entre grupos de ordenadores y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información. Los diferentes ordenadores se denominan *estaciones de trabajo* y se comunican entre sí a través de una línea cableada o inalámbrica conectada a los servidores, con funciones administrativas y están dedicados en exclusiva a supervisar y controlar el acceso a la red y a los recursos compartidos.

Otra herramienta utilizada en la red es el *modem* para permitir la transferencia de información convirtiendo las señales digitales a analógicas y viceversa. También existen en esta estructura los llamados *Hubs y Switches* con la función de llevar a cabo la conectividad de usuarios de la red desde lugares remotos. A este mundo

[3] GOZAÍNI, Osvaldo Alfredo, *Hábeas Data, Protección de datos personales*, Editorial Ribinzal-Culzoni, Santa Fe, 2001, pág. 9.

informático debemos agregar otro de menor alcance llamado *Intranet*, para el uso interno de una organización.

Los distintos tipos de servicios proporcionados por Internet utilizan diferentes formatos de dirección, o lo que es lo mismo Dirección de Internet. Uno de los formatos se conoce como decimal con puntos, por ejemplo 123.45.67.89; otro formato describe el nombre del ordenador de destino y otras informaciones para el encaminamiento, por ejemplo 'mayor.dia.fi.upm.es'. Las redes situadas fuera de Estados Unidos utilizan sufijos que indican el país, por ejemplo (.es) para España o (.ar) para Argentina. Dentro de Estados Unidos, el sufijo anterior especifica el tipo de organización a que pertenece la red informática en cuestión, que por ejemplo puede ser una institución educativa (.edu), un centro militar (.mil), una oficina del Gobierno (.gov) o una organización sin ánimo de lucro (.org).

El espacio cibernético se crea con la interconexión, en un ámbito mundial de muchas computadoras, que son máquinas que leen códigos. La interconexión de estos códigos, manejados por hombres, define la arquitectura del espacio cibernético. La configuración de Internet comenzó en 1969 a partir del programa militar denominado "Arpanet" que permitió que las computadoras que operaban las fuerzas militares, los proveedores de material bélico y algunas universidades que investigaban acerca de problemas de defensa, se pudieran comunicar aún cuando una de sus redes fuera dañada por un hecho de guerra. ("Reno v/ American Civil Liberties Union". 521 US 844, cit. p. 847).[4]

Una página *web* es un objeto cultural, o sea, hecho por el hombre; todo aquello de lo que se puede predicar algo, y desde que es obra del hombre. Ese objeto es inmaterial. La materia es definida como forma de energía que tiene los atributos de poseer una masa y una extensión en el espacio y el tiempo, por lo tanto una página web no es un bien material o, en otras palabras, no tiene materia. En una página web, el sustrato estará dado por los diferentes componentes (soportes de hardware y software) donde se almacenan la información y los datos, ideas que constituyen la obra en sí. La sigla "www" significa World Wide Web, comúnmente simplificada en el término "la web", conjunto de redes basadas en la arquitectura cliente/servidor.

[4] En citas COLAUTTI, Carlos E., "La libertad de expresión y el espacio cibernético", LA LEY 1999-E, 1329.

En la actualidad es casi imposible calcular los sitios web que existen y los servidores a los que tenemos acceso, dado que Internet ha tenido un extenso desarrollo, en gran parte motivado en fines comerciales de las empresas, por lo que de ser la red de investigación militar para lo que fue creada, pasó a transformarse en un negocio y como tal amplió su órbita de alcance.

El *word wide web* (www) es una red mundial compuesta por la sumatoria de los servidores conectados a ella. Así, la información se encuentra depositada en bancos de datos llamados *servidores de web* o *web servers* que concentran las distintas páginas (webpages) en formato multimedia (color, gráficos, audio y video). De acuerdo con estos conceptos, el *server* sería un lugar de almacenamiento de datos, que podría estar ubicado en cualquier lugar del mundo y podría recibir distintas páginas web.[5]

Otro servicio es el *host* u *hospedaje de página-web*. El *hosting* es un contrato por el cual el prestador del servicio concede a su co-contratante, gratuitamente o por el pago de un precio en dinero, el derecho al alojamiento de archivos informáticos en un servidor (que puede ser propio del prestador o sólo gozar de un derecho de uso sobre él) que quedan a disposición del público. Existen, por tanto, dos relaciones diversas: la del alojamiento del archivo (entre el prestador y el introductor de la página) y la de acceso a la información (del público al servidor), conectadas, pues al introductor le interesa la amplitud del público.[6]

Martínez Medrano, nos brinda una clasificación de *operadores de Internet*: A) Proveedores de contenido: autores, editores y otros titulares de derechos que ingresan sus obras en la red. Son los principales interesados, conjuntamente con las empresas de software, en una fuerte protección de los derechos de autor. B) Proveedores de Servicio: es la denominación común para dos tipos de sujetos denominados proveedores de acceso a usuarios y proveedores de servicios adicionales, los que además del acceso suministran determinados servicios, como por ejemplo contenidos, ya sea producido por ellos mismos o por terceros. C) Proveedores de Red: quienes proveen a los *access Provider* y *host service Provider* es decir las líneas de comunicaciones para bajar la información de la red. (vgr. Telefónica de España, British

[5] BALLONE, Mariano C. y GERMAIN, Pablo C, "Tributación en el comercio electrónico", LA LEY 2000-C, 1224.
[6] GALDOS, Jorge Mario, " Responsabilidad civil de los proveedores de servicios en Internet "Responsabilidad civil e internet: Algunas aproximaciones", LA LEY 2001-D, 953-Responsabilidad Civil Doctrinas Esenciales Tomo VI, 69

Teleconm, AT&T etc.). D) Usuarios: sujetos que acceden a la información y utilizan las diversas prestaciones de la red.[7]

Los buscadores gobiernan la información, comparan la palabra buscada por el usuario con un archivo índice de datos procesados previamente y almacenado en una ubicación determinada y en base a las coincidencias encontradas, publican los resultados de acuerdo a los criterios preestablecidos por cada buscador, determinan el procedimiento de carga de contenidos, a cuyo fin recorren periódicamente con programas informáticos las direcciones de todas las páginas web existentes en Internet, accediendo a su contenido, que es clasificado y almacenado para ser utilizado en las búsquedas.

Por otra parte, las *redes sociales online* consisten en servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en las que se plasman datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado. Mediante el envío de invitaciones a través de correos a sus conocidos, ofrece la posibilidad de unirse al sitio web.

Estos nuevos servicios se configuran como poderosos canales de comunicación e interacción, que permiten a los usuarios actuar como grupos segmentados: ocio, comunicación, profesionalización, etc, siendo que uno de los principales objetivos de la red social se alcanza en el momento en el que sus miembros utilizan el medio online para convocar actos y acciones que tengan efectos en el mundo offline.

Entre los años 2001 y 2002 surgen los primeros sitios que fomentan redes de amigos. Hacia 2003 se hacen populares con la aparición de sitios tales como Friendster, Tribe y Myspace. Google lanza en enero de 2004 Orkut apoyando un experimento que uno de sus empleados realizaba en su tiempo libre. En ese mismo año fue creada Facebook y en 2005 ingresan Yahoo 360º y otros.

Las herramientas que proporcionan en general las redes sociales en Internet son:

[7] GALDOS, Jorge, op.cit, pág. 1.

actualización automática de la libreta de direcciones; perfiles visibles; capacidad de crear nuevos enlaces mediante servicios de presentación y otras maneras de conexión social en línea.

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 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 y, por ende, del ámbito de la privacidad e intimidad de los usuarios.

Internet, entonces, es la resultante de la combinación de la informática con la telemática; la primera se ocupa del tratamiento automatizado de la información y la segunda de la transmisión de esa información tratada informáticamente a través de redes, que pueden ser abiertas -como lo es Internet- o cerradas. Por su estructura no es una empresa, sino un conjunto de servidores y redes de computadoras entrelazadas a través de los proveedores de conectividad (que brindan la infraestructura) que utilizan un protocolo único de comunicaciones. No es de nadie, no tiene propietario, ni organizador determinado. Se trata de un maravilloso instrumento socializador a un nuevo nivel que trasciende lo local o nacional, para ser un 'socializador global'. Pero, además, al menos en estos días, se trata de un socializador descentralizado y mínimamente sujeto a controles, en su mayoría autoimpuestos. En principio, se pretende -por un lado- que por su naturaleza misma, no es susceptible de regulación, pero también -otros sectores- piensan que debe sujetarse a normas y responsabilidades.[8]

[8] PARELLADA, Carlos A., “Responsabilidad por la actividad anónima en Internet”, LA LEY 2007-F, 1066.

II.- Derecho a la libertad de expresión y a la intimidad. Tutela legal. Habeas data.

La regulación de la red no debe buscar el control sino la garantía del desarrollo de la actividad en términos igualitarios, de eficacia y de universalidad del acceso. Asimismo debe ofrecer mecanismos reparadores ante las vulneraciones de los derechos de los particulares, que previamente han sido educados en las características del medio para que sepan protegerse de eventuales intromisiones. […] Es preciso conjugar, por un lado, libertad de expresión y comunicación, y, por otro, derecho al honor y la intimidad.[9]

Los sistemas de información basados en el procesamiento de datos pueden llegar a constituir -atento las características de los nuevos soportes magnéticos: almacenamiento de mayor cantidad de información y posibilidad de interconexión entre ellos- una invasión al derecho a la intimidad, por lo que resulta necesaria una adecuada protección de este derecho personalísimo frente al avance tecnológico. [10]

A la vez y por su propia naturaleza permite la expresión de ideas y opiniones, y la difusión de las mismas. En razón de sus posibilidades técnicas Internet transmite y difunde información en forma escrita, visual y auditiva.

El servicio de Internet, que permite exteriorizar el pensamiento humano como así también la búsqueda, recepción y difusión de información e ideas de toda índole, se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión, que como todo derecho debe ejercerse en forma razonable, regular y no abusiva considerándose tal, a aquél que contraríe los fines que la ley tuvo en mira al reconocerlos o al que exceda los límites impuestos por la buena fe, la moral y las buenas costumbres.

Nuestro máximo Tribunal nacional, sostuvo que la libertad de expresión es un derecho que es absoluto tan solo desde la perspectiva de que no puede someterse a censura previa, pero su ejercicio puede generar responsabilidad en caso de abuso, es

---

[9] FERNÁNDEZ RODRÍGUEZ, José Julio, *¿Regular Internet? Una reflexión sobre los límites del derecho y las funciones del estado, en Defensa de la Constitución Garantismo y Controles, Libro en reconocimiento al Dr. Germán J. Bidart Campos*; Víctor Bazán – Coordinador-, Ediar, Buenos Aires, 2003, pág. 470.

[10] CAMPANELLA DE RIZZI, Elena Margarita y STODART DE SASIM, Ana María, "Derecho a la intimidad e informática", LA LEY, 1984-B, p. 667.

decir, aquel reconocimiento no implica impunidad frente a la responsabilidad por los daños provocados en su ejercicio.[11]

Por otra parte, la irrupción de la informática en la sociedad ha replanteado la cuestión de la protección del derecho a la intimidad, en virtud del riesgo que para las personas implica la estructuración de los grandes bancos de datos de carácter personal, y particularmente la potencialidad del entrecruzamiento de la información contenida en los mismos, lo que plantea la necesidad de elaborar un modelo de concepto de la protección del derecho al intimidad, es decir, la necesidad de respuestas jurídicas que protejan los abusos de la manipulación de la información personal.[12]

La Declaración de los Derechos Humanos de la Asamblea General de las Naciones Unidas (1948, art. 12) expresa: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". Por su parte, la Convención Americana sobre los Derechos Humanos, norma que tiene idéntica jerarquía constitucional que el documento internacional anteriormente citado a partir de la reforma de 1994 (art. 75, inciso 22, 2ª cláusula, C.N.), en su art. 11, inc. 2º dispone que: "nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia ni de ataques ilegales a su honra o reputación". Son derechos y garantías inherentes al ser humano (art. 29 inc. c, C.A.DD.HH.), entre los que se encuentran aquellos que conciernen a la integridad espiritual (honor, intimidad, imagen y libertad).

Y, específicamente en cuanto al derecho a la privacidad e intimidad, la Corte Suprema de Justicia de la Nación ha establecido pautas valiosas para supuestos en los que el derecho a informar y ser informado se encuentre en conflicto con el derecho a la vida privada, destacándose que su fundamento constitucional se encuentra en el art. 19 de la Constitución Nacional y describe el ámbito de autonomía individual que protege (sentimientos, hábitos y costumbres, relaciones familiares, y genéricamente acciones, hechos y datos que de acuerdo con la forma de vida aceptada por la comunidad están reservadas al propio individuo).

[11] C.S.J.N., 11/12/1984, "Ponzetti de Balbín, Indalia c. Editorial Atlántida, S. A.", LA LEY, 1985-B, 120.
[12] AMAYA, Jorge Alejandro, *El habeas data: una garantía en dos dimensiones, en Defensa de la Constitución Garantismo y Controles, Libro en reconocimiento al Dr. Germán J. Bidart Campos*; Víctor Bazán – Coordinador-, Ediar, Buenos Aires, 2003 pág. 777.

En rigor, comprende no sólo la esfera doméstica, el círculo familiar y de amistad, sino otros aspectos de la personalidad espiritual y física de las personas tales como la integridad corporal o la imagen y nadie puede inmiscuirse en la vida privada de una persona ni violar áreas de su actividad no destinadas a ser difundidas, sin su consentimiento o el de sus familiares autorizados para ello y sólo por ley podrá justificarse la intromisión, siempre que medie un interés superior en resguardo de la libertad de los otros, la defensa de la sociedad, las buenas costumbres o la persecución de un crimen.

La intimidad, concretamente, se encuentra receptada en el artículo 19 de la Constitución Nacional que reza: “Las acciones privadas de los hombres que de ningún modo ofendan el orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exenta de la autoridad de los magistrados. Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe”.

El reconocimiento de la existencia de un derecho a la intimidad, como especie dentro de los derechos personalísimos, se encuentra contenido en el art. 1071 bis del Código Civil que establece: "El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres o sentimientos, o perturbando de cualquier modo su intimidad, y el hecho no fuere un delito penal, será obligado a cesar en tales actividades, si antes no hubieren cesado, y a pagar una indemnización que fijará equitativamente el juez, de acuerdo con las circunstancias; además, podrá éste, a pedido del agraviado, ordenar la publicación de la sentencia en un diario o periódico del lugar, si esta medida fuese procedente para una adecuada reparación".

Vale decir, que son requisitos para que resulte configurado el acto lesivo de la intimidad los siguientes: a) que exista un entrometimiento en la vida ajena, esto es, que el agente ejercite un acto que interfiera en el ámbito privado de otro; b) que dicha intromisión resulte arbitraria, en el sentido de que no se encuentre justificada por algún fin superior; c) que perturbe la intimidad del sujeto interferido, para lo cual la citada disposición legal contiene algunos ejemplos (publicación de retratos, difusión de correspondencia, etc.), pero cuya enunciación no es de ninguna manera taxativa, sino meramente ilustrativa; y, por último, un recaudo negativo: d) que el acto lesivo no

constituya un delito penal, pues si lo configura entrarían a funcionar los principios ordinarios de la responsabilidad civil.

En el art. 1071 bis se encuentra vislumbrada tanto la protección de la intimidad como el efectivo ejercicio de la libertad de los particulares en general e impide que tal intromisión se convierta en un abuso del derecho, frente a la falta de justificación de la conducta, con autonomía de que el hecho difundido sea verdad. Se busca la cesación de la perturbación a la intimidad, es decir una tutela inhibitoria, y persigue el resarcimiento del daño causado.

"La referida arbitrariedad del ataque a la intimidad, en la fórmula del artículo, no es otra cosa que la antijuridicidad, el actuar sin derecho.[13]

La reserva de la vida privada puede ser objeto de ataques de distintas naturaleza, siendo la enunciación contenida en la norma meramente ejemplificativa, verbigracia, quedarían comprendidos en ella, los adelantos tecnológicos en cuanto a los aparatos de escucha y obtención de imágenes, los avances en el campo de la información y la posibilidad de interconexión de bancos de datos.

En orden al elemento subjetivo, […] "la mayor parte de los autores entienden que el art. 1071 bis no introduce modificaciones al esquema general de responsabilidad del Código que se basa en el principio de culpa. En consecuencia, en el caso de ataques a la vida privada será menester que la víctima pruebe la culpa o dolo del agente (entre otros, Zavala de González). Mientras que para un sector minoritario en la doctrina (a la sazón, Mosset Iturraspe) la figura contemplada en el art. 1071 bis no requiere para su configuración la prueba de dolo ni de culpa en el agente, y constituye un caso de aplicación del abuso del derecho.

Por último en alusión al elemento negativo que refiere la norma que *el hecho no fuere un delito penal*, establecer en sede civil la ausencia de requisitos del tipo penal, en el caso concreto, en tanto que, no se establece en el art. 1071 bis una hipótesis de prejudicialidad. Así se ha sostenido que: "Si en el caso concreto, el hecho constituye delito penal, se debe esperar el juzgamiento del caso en sede penal, en tanto si el hecho

[13] ZABALA DE GONZÁLEZ, Matilde, *Derecho a la intimidad*, 1982, p 116 y ss, et.al., en BUERES y HIGHTON, op.cit., pág. 137.

constituye delito penal, se aplicarán las reglas generales de la responsabilidad civil, de lo contrario, será de aplicación el artículo en comentario".[14]

El invasor de la intimidad ajena responde cuando actúa en forma arbitraria, cualquiera sea el modo de perturbación. De allí que el requisito de la arbitrariedad exigido por el art. 1071 bis, del Código Civil, para configurar un ataque a la esfera de la vida privada, debe interpretarse como referido a la antijuridicidad de la conducta lesiva, y estará a cargo de los jueces fijar la indemnización equitativamente, de acuerdo a las circunstancias, deviniendo procedente la publicación de la sentencia a pedido del interesado.

El profesor Miguel A. Ekmekdjian, lo ubicó [al derecho a la intimidad] como uno de los contenidos del derecho a la dignidad y lo definió como "la facultad que tiene cada persona de disponer de una esfera, ámbito privativo o reducto infranqueable de la libertad individual, el cual no puede ser invadido por terceros, ya sean particulares o el propio Estado, mediante cualquier tipo de intromisiones".[15] El reconocido jurista también nos trae la definición que sobre el mismo aporta Cooley, el cual lo ha definido como: "the right to be let alone" (el derecho que tiene un hombre a ser dejado en la soledad de su espíritu).[16]

Con otros fundamentos, Humberto Quiroga Lavié reflexiona que: "[…] en el concepto de intimidad palpita la idea de exclusión de los demás del ámbito de lo estrictamente personal, aclarando que sólo en caso de hipótesis de delito se podrá ingresar válidamente en el ámbito de la privacidad personal y lo define como el respeto a la personalidad humana, del aislamiento del hombre, de lo íntimo de cada uno, de la vida privada, de la persona física, innata, inherente y necesaria para desarrollar su vida sin entorpecimientos, perturbaciones y publicidades indeseadas". Y continúa el citado autor diciendo que: "Es el derecho personalísimo que permite sustraer a las personas de

[14] FERREIRA RUBIO, Delia, *El derecho a la intimidad. Análisis del artículo 1071 bis del Código Civil*, 1982, p. 146 ss, et.al., en BUERES y HIGHTON, op.cit., pág. 139.
[15] EKMEKDJIAN, Miguel A., *Derecho a la Información*, Ed. Depalma, 2ª ed., Buenos Aires, 1996, ps. 72 y sigtes.

[16] EKMEKDJIAN, Miguel Ángel, Tratado de Derecho Constitucional, tomo I, Ed. Depalma, 1993, p. 568. cf. también el Manual de la Constitución Argentina, ed. Lexis Nexis. Depalma, quinta edición, 2002, p. 96.

la publicidad o de otras turbaciones a su vida privada, el cual está limitado por las necesidades sociales y los intereses públicos."[17]

A la par del derecho a la intimidad existe un reconocimiento por parte de la doctrina mayoritaria del derecho a la información, siendo Ekmekdjian quien distingue entre el "derecho a informar" y el "derecho a informarse", tanto en lo que se refiere a las ideas cuanto a la difusión de noticias.

Tales derechos –intimidad y libertad de informacion-, como derivación o especie de la libertad de expresión, tienen fundamento constitucional. En efecto, el art. 14 de la Carta Magna establece que: "Todos los habitantes de la Nación gozan de los siguientes derechos [...] de publicar sus ideas por la prensa sin censura previa..."; el art. 32 de la citada norma prescribe: "El Congreso Federal no dictará leyes que restrinjan la libertad de imprenta o establezcan sobre ella la jurisdicción federal" y el art. 42 del mismo ordenamiento legal preceptúa: "Las autoridades proveerán a la protección de [...] los derechos de los usuarios y consumidores...", con la finalidad de garantizar el bienestar general.

El pacto de San José de Costa Rica, que contiene la Convención Americana de Derechos Humanos, ratificada por la Argentina mediante la ley 23.054, en su art. 13 inc. 1, contempla el derecho de toda persona a la libertad de pensamiento y expresión, declarando como comprensiva de aquélla "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 otro procedimiento de su elección".

En 1923 la ley de propiedad intelectual 11.723 (Adla, 1920-1940, 443) había requerido el consentimiento expreso de los interesados para que el retrato fotográfico de una persona fuera puesto en el comercio (art. 31).

En la década de los años '50 la computación se extendió por el Mundo y llegó a la Argentina. En 1998 la ley de propiedad intelectual incluyó a "los programas de computación fuente y objeto" en la protección del derecho de autor (art. 1 según ley 25.036 -Adla, LVIII-E, 5040-).

En el año 2001 la ley 25.506 (Adla, LXII-A, 6) asumió la necesidad de reglas legales para la nueva tecnología, a cuyo fin estableció la equivalencia entre el

[17] QUIROGA LAVIÉ, Humberto, *Derecho a la Intimidad y Objeciones de Conciencia*, Universidad del Externado de Colombia, p.10

documento digital y el documento escrito (art. 6) y previó un procedimiento matemático de firma digital para los casos en que la ley requiere una firma manuscrita (art. 3).

La comercialización en masa de productos y servicios de consumo generó en 1993 la ley 24.240 de defensa del consumidor, que -de acuerdo con lo que se entendía generalizadamente- estableció en su art. 40 la responsabilidad objetiva, y en ese aspecto fue vetada. En 1998 la disposición revivió mediante la ley 24.999 (Adla, LVIII-C, 2929), pero entretanto "el veto del Poder Ejecutivo a esa norma resultó irrelevante" en razón de la communis opino doctrinaria y jurisprudencial.

La ley 24.240 (Adla, LIII-D, 4125) (art. 3) se integra con las leyes de defensa de la competencia (ley 22.262) y de lealtad comercial (ley 22.802) (Adla, XL-C, 2521; XLIII-B, 1346). La comercialización tiene íntimas conexiones con la publicidad, que ocupa el papel de "primer ministro en el reino de la cultura de masas"; las leyes de defensa de la competencia y de lealtad comercial ahora se entienden desde la perspectiva de protección de los consumidores. Los derechos del consumidor y la defensa de la competencia fueron garantizados por los arts. 42 y 43 de la Constitución Nacional, tras la reforma de 1994.

Como tutela a los derechos de las personas a conocer sus datos y en consecuencia solicitar medidas sobre el registro que de ellos constan en bancos públicos o privados proveedores, en el ámbito constitucional la referida reforma incorporó la garantía del Habeas Data en el art. 43, 3er. párrafo, concibiéndola como una especie de la acción de amparo que se complementa con las acciones previstas en la ley 25.326 de protección de datos personales (Adla, LX-E, 5426).

El art. 43, 3er párrafo de la CN reza: "Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ellos referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".

La norma de mención permite en una primera etapa el ejercicio de la acción por la persona afectada tendiente a "tomar conocimiento de los datos a ella referidos y de su finalidad". Es decir que el accionante puede conocer no solo qué datos se tienen sobre una persona, sino también con qué objetivo ellos están en el mismo. La toma de

conocimiento implica el ejercicio del "derecho de acceso a la información". Este derecho de acceso tiene por finalidad permitir al individuo el control sobre la información que le concierne, que es en esencia uno de los objetivos principales del habeas data. [18]

Cabe señalar que "...el origen del habeas data se explica en virtud del desarrollo del llamado "poder informático"; quienes "hacen" informática (el productor, el gestor y el distribuidor de datos) tienen generalmente protección constitucional de su actividad, en las reglas que tutelan la libertad de comercio, trabajar, propiedad, inviolabilidad de los papeles privados, etc. La situación no es la misma para los "registrados" en los archivos o bancos de datos, ya que éstos pueden contener información equivocada, antigua, falsa, o con potenciales fines discriminatorios, o lesiva del derecho a la intimidad de las personas; de ahí, que el promotor del habeas data tendrá que alegar, para tener buen suceso, que los registros del caso incluyen información que es inexacta, o que pueden provocarle discriminación.[19]

La garantía constitucional de marras se encamina a que la vida privada de los hombres no se vea invadida por el almacenamiento y difusión de datos personales, sin la previa autorización del titular o de quien detente su representación. Así aflora la autodeterminación informática o libre disposición de los datos personales “libertad informática”, es decir poner límites y control a esa libertad. El fundamento está en la libertad de resolver el destino que se pretende dar a los datos y, en su caso, se autoriza o no el acopio informativo de ellos. La tutela a la intimidad es su sustento y supone dar privilegio a la libertad de las personas para disponer o resolver qué aspecto de su vida permiten que se hagan público y así la sola intromisión en la vida privada o en la esfera de la intimidad implica la afectación al derecho a la intimidad, sin que sea necesario indagar dónde se encuentra la lesión individual.

Sin duda, la garantía de habeas data y, a través de la misma el derecho a la protección de los datos personales -entendida como la rama del derecho que protege la autodeterminación informativa de las personas- aparece como un punto de partida que marcará para siempre un hito en la regulación de la informática y las comunicaciones. Y agrega Basterra que la gran mayoría converge en que el habeas data tutela el derecho

[18] PALAZZI, Pablo Andrés, “El Habeas Data en el Derecho Constitucional Argentino”, en *La Defensa de la Intimidad y de los Datos Personales a través del Habeas Data. Ley 25.326.* Coordinado por Osvaldo Alfredo Gozaíni. Ediar, Buenos Aires, 2001, pág. 52.

[19] CNCiv., sala F, 6/7/95, "Branchi de Sáenz, Delia A. c. Sanatorio Greyton S.A. s/ amparo", LA LEY 1996-C, 473.

a la intimidad, pero no en forma genérica sino como una especie de intimidad: la intimidad informática o autodeterminación informática y a través de ella el derecho a la imagen o el propio perfil.[20]

El derecho a la autodeterminación informática consagra el conjunto de facultades y actividades que reconocen al individuo, auténtica garantía frente a las intromisiones que pudieran producirse a través de la informática en la vida privada de las personas.

Víctor Bazán reconoce que el derecho a la autoderminación informativa ofrece una textura que resulta más acorde con los modernos desafíos informáticos, puesto que al abordar el concepto de intimidad en su faz negativa, permite avanzar hacia una fase activa del proceso de circulación de la información personal brindando protagonismo al interesado, al permitir ejercer un adecuado control para la preservación de la libertad informática.[21]

El derecho a la intimidad como género que caracteriza la defensa de la privacidad, del honor, la imagen, la reputación, la identidad, entre otros de los derechos, es el fundamento del hábeas data. Y habida cuenta de los nuevos peligros y amenazas que el tratamiento informático trae consigo, se sugiere una conceptualización del derecho a la autodeterminación informativa a través de una extensión de su protección frente al uso ilícito o abusivo de la informática a cualquier información personal que represente una amenaza para la persona en "manos de terceros"; la interpretación no consentida de la información debe controlarse y limitarse sin detenerse a averiguar la índole íntima o no de la información.[22]

Es por ello que los titulares de la información que se almacena en esos bancos o registros de datos que estuvieran autorizados por la ley, y más aún en aquéllos que carecen de autorización, deben tener garantizado el derecho de acceder a esos datos a los efectos de tomar conocimiento de su exactitud, para requerir la correspondiente modificación, corrección o rectificación. Incluso para que los datos o las informaciones sean suprimidos de los registros, cuando ellos fueren inexactos u obsoletos, cuando implicaran discriminación por razones de raza, religión, ideología u otra circunstancia

[20] BASTERRA, Marcela, "Habeas Data: Derechos Tutelados", Doctrina Judicial, 1999-3; p.77.
[21] BAZÁN, Víctor, "El Hábeas Data y sus particularidades frente al amparo", en Revista de Derecho Procesal, N°4 – I, Rubinzal-Culzoni, Santa Fe, Argentina, 2000, p. 261.
[22] HERRÁN ORTÍZ, Ana Isabel, *La violación de la intimidad en la protección de datos personales*, Dykinson, Madrid, 1999, pág. 105

personal o de grupo, salvo que el registro estuviera especialmente habilitado para realizar una constatación de esa naturaleza, cuestión que debe considerarse excepcional, en especial teniendo en cuenta que los datos sensibles deben quedar exentos de todo registro. El derecho a la libre disposición de los datos personales supone recrear un derecho fundamental que, derivado del derecho a la vida privada del hombre, le permite resolver por sí mismo el tratamiento que quiera asignar a los datos que sobre su persona se almacenen con destinos diferentes.

La ley de protección de datos personales 25.326, aporta la claridad necesaria al tema para interpretar que es una acción distinta del amparo común. Ella comienza delimitando su objeto (art. 1), el que se acota a la faceta personal del habeas data. Introduce definiciones legales sobre conceptos claves (art. 2) que servirán como criterio de interpretación a la hora de su aplicación. Regula la organización y funcionamiento de los archivos; ellos deben estar registrados, los datos archivados deben ser veraces, adecuados y pertinentes; no pueden ser recolectados por medios desleales; se debe respetar la finalidad para la cual fueron almacenados (arts. 3 y 4). Se ocupa de la necesidad del consentimiento como condición de licitud del tratamiento de datos (art. 5); de la recolección de los datos sensibles (arts. 7 y 8); de los deberes de informar al titular de los datos (art. 6); de la seguridad (art. 9), y de la confidencialidad (art. 10). […] de diversas especies de habeas data aplicables a todo el territorio (arts. 13/16), registradas todas por el principio de gratuidad (art. 19). Se respeta el instituto del olvido o caducidad del almacenamiento con fines posibles cuando cese el movimiento que justificó su almacenamiento (art. 23.3) y de los datos económicos-financieros al fijar un plazo (art. 26.4), llegando incluso a disponer el blanqueo de morosos que hubieran cancelado sus deudas al momento de entrada en vigencia de la ley (art. 47 y último, vetado por el Dec. 995/2000 invocando la protección de los dadores de créditos). Asimismo se crea un órgano de control con atribuciones específicas (art. 29.1), cuya autonomía funcional (art. 29.2) fueron también observados por el citado decreto presidencial con el solidario argumento de no incrementar erogaciones presupuestarias.[23]

Es la propia ley la que ratifica el mandato constitucional contemplando la posibilidad que se acceda al conocimiento de datos personales y a la finalidad que se

[23] QUIROGA LAVIÉ, Humberto, et.al., *Derecho Constitucional Argentino*, segunda edición actualizada por Humberto Quiroga Lavié, Tomo I, Editorial Rubinzal-Culzoni, 2009, págs. 600/601.

dará a los mismos (arts. 33 y 37). La acción de hábeas data es una acción de protección de los datos personales específicamente ordenada a la defensa de la intimidad de los datos, el derecho a la autodeterminación informativa y a la propia imagen, aún cuando no estén dadas las condiciones de arbitrariedad o ilegalidad del acto cuestionado. Es la misma norma constitucional la que establece que podrá interponerse el hábeas data "para tomar conocimiento de los datos a la persona referidos" sin supeditar la legitimación a la existencia de arbitrariedad o ilegalidad. Esta prescripción de la propia Constitución, da cuenta que no es requisito la procedencia de la arbitrariedad o ilegalidad manifiesta a que se referían los tribunales inferiores en el caso.[24]

Por su parte la ley 26.032 establece: "La búsqueda, recepción y difusión de información e ideas de toda índole, a través del servicio de internet, se considera comprendido dentro de la garantía constitucional que ampara la libertad de expresión...".

Según los fundamentos del proyecto, "la importancia que en las sociedades modernas tiene el servicio de internet reside en que es una herramienta válida para que toda la ciudadanía pueda tener acceso a información sin censura, a enviar y recibir información y en especial a expresar sus opiniones en todo tipo de temas: políticos, religiosos, económicos, sociales, culturales, etc.".

En el año 2007, la ley 26.285 modificó la ley de propiedad intelectual permitiendo la libre reproducción y difusión de obras para no videntes editadas en formato digital.

Pero lo cierto es que Argentina, a diferencia de otros países, se encuentra en un vacío legislativo y, mientras no exista en nuestro país una ley de tratamiento de datos, el habeas data pude servir preventivamente para evitar la difusión de comentarios hirientes o mal intencionados que persigan agredir el respeto personal o la fama profesional que se tenga; como también ante la falta de una regulación específica pueden aplicarse al medio de comunicación que presenta la red no sólo los principios generales de la responsabilidad civil sino también los principios generales del Derecho, con la apropiada consideración de las circunstancias del caso (art. 16, Cód. Civil), ya que éstos últimos pueden cumplir una función interpretativa.

[24] BASTERRA, Marcela I., "Aspectos procesales y sustanciales del habeas data en un fallo de la Corte Suprema de Justicia de la Nación", LA LEY 2005-B, 741.

Y es que el sistema jurídico se caracteriza como una entidad orgánica autosuficiente, con capacidad de expansión para reglar jurídicamente cualquier hecho o situación que pertenezca a esa rama de modo coherente, es una totalidad ordenada con coherencia entre sí, y constituye un bloque sistemático, que impone a los jueces que juzguen los casos que les son sometidos aunque las leyes adolezcan de silencio, oscuridad o insuficiencia (art. 15, Cód. Civil) a cuyo fin, colocados en la misma hipótesis del legislador, deben acudir al espíritu de la ley, a los principios de leyes análogas -sea por *analogía legis* o por *analogía juris*-, ante la inexistencia en nuestro país –como se expresara retro- de demasiadas disposiciones legislativas ni de fallos judiciales que versen sobre los temas polémicos que Internet puede llegar a ocasionar.

Los principios que protegen la privacidad en Internet son:

• La información: es fundamental notificar al usuario en forma previa, clara y detallada, que la entidad o empresa recopilará información personal, el uso que se le dará, el medio en que ésta se acopiará, y si los consumidores deberán ser requeridos para hacer uso de ella.

• El principio de opción: el cual permite al usuario decidir si la información recolectada de sí mismo será utilizada para propósitos distintos del que le fue señalado y aceptado originalmente.

• El concepto de acceso: se refiere a la facultad individual del consumidor para acceder a la información de sí mismo recolectada por el servidor, de manera tal de poder constatar su existencia, corregirla o complementarla y/o eliminarla, si así lo desea.

• El principio de seguridad: se refiere a la obligación de quien acopia la información personal de protegerla ante un acceso, uso y exhibición no autorizados, como asimismo respecto de su pérdida o destrucción.

• La exigibilidad: para el cumplimiento sustantivo de los principios antes mencionados, está dada por la regulación jurídica y el régimen sancionador que la autoridad pública debe aplicar en esta materia.

La regla es que tenemos el derecho a expresarnos, pero dentro de sus límites y bajo la responsabilidad de quien lo ejerce. 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 justificaría su responsabilidad es que ha creado el riesgo y ha posibilitado el daño. […] Ahora, lo que se nos plantea es cuál es el alcance que queremos darle a la evitación de los daños. Descartamos la censura, pues la República Argentina ha declarado su intención de mantenerse al margen de la conversación global, lo que nos lleva a pensar que el Derecho Argentino no propugna ni la censura pública ni la privada, pero ello no implica garantir la elusión de las responsabilidades provenientes de los excesos que desorbitan el derecho de expresión. El Estado Argentino ha reconocido el valor de la Red en orden al lugar ideal para el derecho de informar y 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 (Adla, LVII-E, 5667), 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... 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, INTERNET se merece la mayor protección ante cualquier intromisión gubernamental" (C.S.J. EE.UU, junio 26-1997 in re "Reno Attorney General of United States et al. v. American Civil Liberties et al.", N° 96-511).[25]

Una posible solución para evitar la existencia o difusión de contenidos ilícitos en internet es la existencia de medios técnicos -filtros- que, en la práctica, limiten o impidan el acceso sólo a dichos contenidos, y que los usuarios pueden contar con esos programas, para así se viabilice la libre circulación de la información reclamada por la libertad de expresión y el respeto a las preferencias personales, en tanto siempre serán mejores los filtros selectivos que las censuras generalizadas.

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

[25] PARELLADA, Carlos A., "Responsabilidad por la actividad anónima en Internet", LA LEY 2007-F, 1066.

perfiles de amigos, lo que puede suponer otro riesgo para la protección de la privacidad, además de dificultar el proceso de eliminación de su información en Internet.

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.

III.- Responsabilidad civil en las relaciones informáticas

La realidad de un mundo globalizado nos aconseja delimitar la problemática de la responsabilidad en Internet en tanto de ella nos servimos la mayoría de los sujetos que tenemos acceso a un ordenador que, como fundamento, tiene como actividad la transmisión de información en todos los ámbitos, ya sea académicos, culturales, de esparcimiento, etcétera.

Dicha actividad informática, comprende todos los procesos de tratamiento de la información, en cuanto se desenvuelve mediante el uso de computadoras y lleva consigo un riesgo social que, en el caso de concretarse en daños a usuarios o terceros, hace aplicables las reglas del sistema actual de responsabilidad civil, contractual y extracontractual, según exista vínculo o no entre el ofensor y la víctima.

Ello en virtud de que la responsabilidad emergente de la informática, no es más que un nuevo capítulo especial de la responsabilidad civil. Por ende, las situaciones generadoras de obligaciones entre los sujetos interesados: constructores, asesores en informática, proveedores de servicios, usuarios, etc., no puede escapar de sus lineamientos generales.

De manera tal que el fundamento de dicha responsabilidad se encuentra en el deber genérico de no dañar *alterum non laedere*, consagrado en el art. 19 de la Constitución Nacional. Ella se basa en la conducta antijurídica de un sujeto de derecho realizada con dolo o culpa en los supuestos de responsabilidad subjetiva o cuando exista responsabilidad objetiva en los casos que ella proceda, o cuando exista un mandato legal

en el supuesto de omisiones, todas hipótesis que además deben producir daño para que exista acción civil.

Y en base a las prescripciones del art. 16 del Código Civil si una cuestión no puede resolverse ni por las palabras, ni por el espíritu de la ley se atenderá a principios de leyes análogas; como así también si aún la cuestión fuese dudosa, se resolver por los principios generales del derecho, teniendo en consideración las circunstancias del caso; en tanto que, siguiendo tal directriz, el art. 15 establece que los jueces no pueden dejar de juzgar bajo el pretexto de silencio, oscuridad o insuficiencia de las leyes.

Prevalece la postura de responsabilizar a los operadores de redes y proveedores de acceso al servicio de alojamiento y provisión de datos cuando en la publicación de información de terceros se demuestre que habiendo conocido directamente los contenidos ilícitos, siendo posible técnicamente, no se bloqueó la información. De igual manera cabe atribuir responsabilidad al autor o editor de una obra que, a título oneroso o gratuito, ingresa a un sitio -con el consentimiento del responsable del servicio- un contenido ilegal, por los daños causados por sus opiniones que generan dañosidad, es decir perturbación ilegítima del ámbito privado alcanzada por el art. 1071 bis del Cód. Civil, concurrentemente con la del dueño del sitio.

La vida privada protegida por el artículo 1071 bis es el conjunto de datos, hechos o situaciones reales, desconocidos por la comunidad y reservados al conocimiento bien del sujeto mismo, bien de un grupo reducido de personas.[26]

La mayor parte de los autores entienden que el art. 1071 bis no introduce modificación alguna al esquema general de responsabilidad del Código que se basa en el principio de culpa. En consecuencia, en el caso de ataques a la vida privada será menester que la víctima pruebe la culpa o el dolo del agente.[27]

En la órbita contractual, la relación jurídica obligacional que surge de la prestación del servicio entre la empresa titular del sitio web y el usuario, es un contrato por adhesión. Tales instrumentos contractuales son aquellos en los cuales el contenido ha sido determinado con prelación, por uno solo de los contratantes, al que deberá adherir el co-contratante que desee formalizar la relación jurídica obligatoria, sin poder modificarlo. Envuelve un consentimiento sin deliberaciones previas al aceptarse una fórmula pre establecida.

[26] FERREIRA RUBIO, Delia, *El derecho a la intimidad. Análisis del art. 1071 bis, del Código Civil*, 1982, pág. 102.
[27] ZABALA DE GONZÁLEZ, Matilde, *Derecho a la intimidad*, 1982, p. 137 y ss., en especial p. 140.

El usuario al realizar el proceso de registración en cualquier sitio web que preste este tipo de servicios, tales como Facebook, Hi5, Orkut, debe obligatoriamente aceptar y prestar conformidad a los términos y condiciones del sitio y políticas de privacidad impuestas unilateralmente. La naturaleza jurídica del contrato que rige la relación, llamados comúnmente *Términos de Uso*, *Términos y condiciones*, *Políticas de Privacidad*, es -como ya se expresó- la de un contrato por adhesión.

En este vínculo contractual (art. 1107, Cód. Civil), la solución no puede ser otra que admitir -como lo ha hecho la doctrina- la existencia de una obligación tácita de seguridad a cargo del locador.[28] Esta obligación de seguridad consistiría en el deber del programador, de confeccionar un programa cuya utilización no acarrea una información defectuosa, con fundamento en el art. 1198 del Cód. Civil en cuanto establece que los contratos deben celebrarse, interpretarse y ejecutarse de buena fe y de acuerdo con lo que verosímilmente las partes entendieron o pudieron entender obrando con cuidado y precisión.

La información inexacta es aquella que no concuerda con la verdad y es "no verdadera" por ser: -falsa (es decir, engañosa, fingida o simulada para dar una apariencia distinta de la realidad) o -errónea (es el resultado de un concepto equivocado que en la mente del informante difiere de la realidad); mientras que la información falsa es la trasmitida deliberadamente con el propósito de engañar, revela dolo o mala fe y genera responsabilidad; la información errónea es el resultado de un acto no consciente, que no se quiere y no genera responsabilidad si el error es excusable, para lo cual se deben ponderar los cuidados y diligencia puestos para obrar cautelosamente y evitarlo. La información agraviante, independientemente de ser exacta o no, afecta la dignidad de las personas, su honor, reputación, decoro, de que goza ante los demás.[29]

La obligación de seguridad en cuanto al contenido, exactitud y periodicidad del suministro de las informaciones, da lugar a una responsabilidad objetiva contractual, pues tal obligación sería de resultado, y no se admite como excusa la

---

[28] LLAMBIAS, Jorge, *Tratado de derecho civil. Obligaciones*, t. IV-B, p. 169, núm. 2844, Ed. Perrot, Buenos Aires, 1980; BUTAMANTE ALSINA, ob. cit., p. 484, núm. 1502.

[29] BUSTAMANTE ALSINA, Jorge, *Teoría general de la responsabilidad civil*, 7ª ed., Ed. Abeledo Perrot, 1992, p. 245.

prueba de la falta de culpa, de manera que el que se considera responsable deberá acreditar la ruptura del nexo causal entre su conducta y el incumplimiento.

Si bien el daño derivado de la información deficiente es sólo una consecuencia inmediata del incumplimiento de la obligación del vendedor de proveer una cosa exenta de vicios, es una consecuencia inmediata del incumplimiento de la obligación de seguridad consistente en proveer una cosa no dañina. En consecuencia, el proveedor del ordenador responderá en su caso, por las consecuencias dañosas inmediatas derivadas de la información defectuosa (art. 520, Cód. Civil), sin perjuicio de que pueda acreditarse el dolo, caso en el cual su responsabilidad se extenderá a las consecuencias mediatas (art. 521, Cód. Civil).

Las relaciones en esta materia vienen marcadas por una notable dependencia mutua entre las partes, para la adecuada consecución del propósito negocial. Ello, en virtud del enorme desequilibrio en el nivel de conocimientos técnicos, por lo que el usuario debe confiar ampliamente la operatoria a la decisión, consejos y actividad del prestador. Pero además, éste requiere que el propio usuario defina claramente cuáles son sus necesidades, a fin que puedan ser fielmente interpretadas, en la ejecución de la tarea.

De todas maneras, la situación en torno al grado de confianza depositada en el prestador, debe conducir necesariamente hacia una serie de formas de reacción jurídica. Asume un deber de resultado, y para eximirse de responsabilidad, debe acreditar causas exógenas a su radio de previsibilidad.

Resulta necesario intensificar el control judicial sobre las cláusulas de exoneración de responsabilidad, incorporadas por el empresario en los contratos con contenido por él mismo predispuesto y a los que el usuario presta adhesión.

La culpa del usuario deberá ser apreciada con criterio restrictivo, teniendo en cuenta su situación de inferioridad en cuanto al conocimiento de la técnica informática, que se caracteriza por su complejidad y evolución continua.

En efecto, muchas veces, los defectos de conducta en que incurre el usuario en la utilización del ordenador, pueden ser una consecuencia del incumplimiento, por parte del proveedor, de su deber de informar y aconsejar al cliente. En consecuencia, el usuario podrá a su vez demostrar que su error de conducta es excusable (art. 929, Cod. Civil), e indicativo a la par del incumplimiento de un deber del proveedor, con lo cual la eximente invocada por este último quedará desvanecida.

En todos los casos, se impone la declaración de invalidez parcial de tales estipulaciones que deberá declararse de pleno derecho si se trata de dispensa de la culpa grave del predisponente, o bien, previa apreciación judicial, cuando aún refiriéndose a su mera culpa grave, el pacto fuera igualmente abusivo por vulnerar el orden público, la regla moral o el principio de buena fe y justo equilibrio de las prestaciones.[30]

Tratándose del ámbito extracontractual, el factor de atribución en el ámbito del Derecho Informático es subjetivo, y en consecuencia para la disciplina del art. 1109 del Cód. Civil se requiere la comprobación de culpa de quien opera el sistema automatizado como requisito necesario de la obligación de indemnizar; es decir un obrar negligente de los buscadores para atribuirles responsabilidad. Aquí también es posible afirmar que sobre el proveedor de servicios de Internet, quien tiene la capacidad técnica y recursos suficientes, pesa una obligación de seguridad. La carga de la prueba se invierte y es él quien se encuentra precisado a acreditar los extremos exculpatorios que variarán según sea el caso.

Sobrino, Waldo Augusto Roberto señala que: a) Las empresas de *Information service providers* son responsables en forma objetiva por el hecho de haber incorporado informaciones a sus páginas o sitios; pero, siempre y cuando los autores de las notas y/o artículos y/o los *links* (de primer grado) también resulten responsables. Y, estos últimos serán responsables en forma subjetiva, debiendo distinguirse, si las informaciones versan sobre personas "públicas" (en cuyo caso, se aplicará la teoría de la real malicia en traslación al derecho argentino de los criterios dirimentes sobre responsabilidad de la prensa), o si se trata de personas no públicas (donde la responsabilidad surgirá por el sólo hecho de haber actuado con culpa). b) Las empresas de Internet *Service Providers (I.S.P.) Hosting service providers* tendrán una responsabilidad subjetiva, derivada de su falta de diligencia del control de las páginas o sitios.[31]

Jorge Bustamante Alsina entiende que corresponde adoptar el sistema de presunción de culpa del art. 1113, 2º párr., 1ª parte del Cód. Civil, como supuesto de

---

[30] STIGLITZ, Rubén - STIGLITZ, Gabriel, "Contratos por adhesión, cláusulas abusivas y protección al consumidor", Ed. Depalma, Buenos Aires, 1985, ps. 141 y sigts.

[31] SOBRINO, Waldo Augusto Roberto, “Argentina: Responsabilidad de las Empresas Proveedoras de Servicios de Internet”, http://www.alfa-redi.org/rdi-articulo.shtml?x=538

hecho del hombre con las cosas (se refiere a las computadoras y no a la información computarizada misma) como instrumento del hecho del hombre.[32]

Gabriel y Rosana Stiglitz, consideran que la información computarizada es una forma de energía "notoriamente riesgosa", desde que se encuentra en un "permanente estado de peligro potencial de ocasionar daños" dado que la capacidad de control es limitada, por lo que se convierte en "causa autónoma del daño". De allí que propician la aplicación del art. 1113, 2° párr., 2° parte.[33]

Una parte importante de la doctrina nacional argentina estima que la actividad realizada por los proveedores de Internet quedan receptadas en la órbita del art. 1113 del Código Civil -actividades riesgosas-, o sea, aquéllas que "por su propia naturaleza (esto es, por sus características propias, ordinarias y normales) o por las circunstancias de su realización —v.gr., por algún accidente de lugar, tiempo o modo—, genera un riesgo o peligro para terceros".[34] Ello ante la hipótesis de anonimato del propietario de la página web.

La complejidad creciente de los sistemas informáticos y el manejo de grandes volúmenes de información en reducidos tiempos, importa a la postre que errores e imperfecciones queden fuera de alcance de toda supervisión del hombre, convirtiéndose la información computarizada (energía) en causa autónoma del daño (derivado de su riesgo o vicio).

En materia de responsabilidad objetiva por riesgo creado debe aplicarse el régimen predeterminado de imputación de consecuencias que prevé el Código Civil para los daños causados por ilícitos culposos.

La exoneración de responsabilidad por daño extracontractual, requiere la acreditación del caso fortuito externo al propio sistema de información computarizada o a las cosas que le sirven de soporte material; o de cualquiera de los extremos que obstaculizan el nexo causal, previstos en el art. 1113 del Cód. Civil.[35]

En definitiva, es la justicia y no el buscador, quien debe decidir sobre la licitud o no del contenido de un sitio de Internet. Así, ante la violación de derechos por

---

[32] BUSTAMENTE ALSINA, Jorge, "La informática y la responsabilidad civil", LA LEY 1987-B, p. 892.

[33] STIGLIZ, Gabriel A.; STIGLITZ, Rosana M., “Responsabilidad civil por daños derivados de la informática”, LA LEY 1987-E, 795

[34] PIZARRO, Ramón Daniel, “glosa al art. 1113 del Cód.Civil”, en BUERES, A. J (Dir.) - HITHONH, E. I. (Coord.), *Código Civil y normas complementarias. Análisis doctrinario y jurisprudencial*, T° 3-A, Hammurabi, Bs. As. 1999, pág. 556.

[35] STIGLITZ, Gabriel A.; et.al., ob.cit.

parte de un sitio web, el damnificado debe recurrir a la justicia para que en caso de corresponder, sea un juez quien ordene al buscador eliminar de su índice los sitios de Internet cuestionados o adoptar las medidas que correspondan al respecto. Si el buscador incumple la orden judicial, entonces si habrá culpa y –consecuentemente- responsabilidad de su parte.

Es decir que antes del reclamo de un particular requiriendo el bloqueo de contenido supuestamente lesivo disponible en Internet, es claro que ninguna negligencia existe por parte del buscador, por lo que no puede atribuírsele culpa -y consecuentemente, tampoco responsabilidad- por el contenido cuestionado. Si bien después de recibido el reclamo la cuestión parece más discutible, el buscador no está obligado a remover los contenidos a menos que reciba una orden judicial en tal sentido.

Los daños que la información nominativa ilícita o antijurídica puede causar a terceros, afectarían en algunos casos el patrimonio del encuestado perjudicándole por la frustración de una ganancia legítimamente esperada o, la pérdida de una chance ya sea por un negocio lucrativo en gestión, o por el desempeño de una actividad pública o privada o el ejercicio de una profesión.

En lo atinente a la determinación de la indemnización del daño cabe subrayar que las consecuencias de la responsabilidad contractual o de la responsabilidad extracontractual son, por lo general, las mismas, sin embargo, la distinción entre las dos hipótesis tienen su razón de ser y su importancia práctica bajo varios aspectos sobre todo en lo concerniente a la obligación de la prueba. […] En los casos de responsabilidad contractual basta que el demandado pruebe el hecho jurídico (contrato) del que deriva su crédito; es el deudor quien si se quiere liberar, tiene el deber de demostrar que el incumplimiento depende de causas que no le pueden ser imputables. Por el contrario, en los casos de responsabilidad extracontractual, el demandado tiene el deber de probar no sólo el hecho que originó la obligación, sino también la imputabilidad, por culpa o dolo, del hecho mismo del deudor (ars. 1073 a 1095, 1109, 1113, parte 2da., 1114 a 1117, 1119 y 1124 a 1131, cód.civil).[36]

La conducta antijurídica del proveedor también puede causar daño moral por los padecimientos que sufra la víctima en la órbita de su patrimonio moral subjetivo y aún en el aspecto objetivo o social de su reputación lesionando el honor que es otro

[36] DALL'AGLIO, Edgardo Jorge, "Aspectos de la Responsabilidad Civil Emergente de las Relaciones Informáticas", El Derecho, Jurisprudencia General, Tomo 117, Buenos Aires, 1986.

valor distinto de la intimidad, pero que goza también de la protección jurídica como derecho de la personalidad.

Si el daño moral existe, la víctima podrá requerir un resarcimiento, pues menoscaba su espiritualidad un ataque a su persona tanto como cuando proviene de un hecho humano, imputable a título de dolo o culpa, como cuando es causado por el riesgo creado por una cosa o por una actividad desplegada (art. 1113 del Código Civil).[37]

Para completar el esquema de la responsabilidad civil es necesario probar la relación de causalidad adecuada entre el daño ocasionado y la acción del operador del sistema automatizado, de tal manera que el perjuicio haya sido causado por la información nominativa como producto del procesamiento de los datos.

La relación de causalidad permite establecer la autoría del daño a los fines de la atribución de responsabilidad, y también para determinar la extensión del resarcimiento, habida cuenta que se responde de los daños que sean consecuencia inmediata y de aquéllos que sean consecuencia mediata previsible del hecho dañoso.

Es obvio que la consecuencia inmediata del procesamiento ilícito, esto es, la información nominativa falsa, errónea o desviada de su finalidad específica, no causa perjuicio económico por sí misma, sino en cuanto entrando en conexión con otro hecho distinto, como lo sería las relaciones jurídicas patrimoniales de quien es objeto de la información, ocasiona a éste un perjuicio en ese ámbito como consecuencia mediata del hecho informático. En efecto, la consecuencia inmediata ha de ser la interrupción de una relación laboral o profesional, el fracaso de un negocio en gestión o la rescisión de un contrato en perjuicio de quien resulta víctima del ilícito informático, lo cual ocasionará a su vez como consecuencia mediata un detrimento patrimonial por el ataque a los bienes materiales susceptibles de valor económico o por la privación de una ganancia o la pérdida de una chance. Vale decir que el hecho ilícito informático no recae directamente en el patrimonio sino en un derecho de la personalidad, lo cual al producir un desmedro de la identidad de la persona implicada causa eventualmente una repercusión patrimonial negativa.

En cuanto a la reparación de los daños ocasionados, ésta debe ser integral, aplicándose al respecto las reglas generales en materia de responsabilidad. Se agrega

[37] BUERES, Alberto J.-HIGHTON, Elena, *Código Civil y normas complementarias. Análisis doctrinario y jurisprudencial*, T° 3-A, Hammurabi, Bs. As. 1999, pág. 547.

como reparación mixta la eventual condena a publicar la sentencia a costa de la parte que hubiera causado el perjuicio.

Bustamante Alsina, sintetiza lo expuesto en relación a la informática y la responsabilidad civil, en las siguientes premisas:

a) Sólo cae en el ámbito de la responsabilidad civil por daños a terceros, el hecho ilícito informático.

b) El ilícito informático consiste en un uso incorrecto o abusivo de la información nominativa.

c) La información nominativa es aquélla que permite la identificación de las personas mediante el procesamiento de datos individuales y su acumulación en centros o bancos de información.

d) El uso incorrecto de la información nominativa consiste en el procesamiento de datos falsos o erróneos u obtenidos por medios fraudulentos o en el abuso de ellos desviándolos de los fines para los cuales fueron recogidos.

e) La responsabilidad civil del operador del sistema se configura cuando de ese uso incorrecto o abusivo de la información nominativa, deriva daño patrimonial o moral para la persona encuestada como consecuencia de la violación del deber de preservar la identidad de los terceros.

f) Si existe contrato entre el operador del sistema y el damnificado, la responsabilidad es contractual por violación del deber de seguridad fundado en la buena fe de las partes (art. 1198, Cód. Civil).

g) Si no existe relación jurídica anterior, la responsabilidad es extracontractual. La ilicitud genérica tiene fundamento en el art. 1109 del Cód. Civil y la ilicitud específica resulta de la violación del art. 1071 bis del Cód. Civil por intromisión arbitraria en la vida ajena atentando contra la intimidad.

h) El factor de responsabilidad es subjetivo y consiste en la culpa presumida de quien causa daño con la cosa (art. 1113, Cód. Civil).

i) Los sistemas automatizados de información que emplean cosas o sea computadores y elementos magnéticos, no son cosas peligrosas que dañen por sí mismas, sino instrumentos que el hombre maneja o acciona a voluntad.

j) Se responde del daño patrimonial que es consecuencia inmediata o mediata previsible del hecho pues el ilícito informático recae sobre un derecho de la personalidad (identidad) y repercute indirectamente en el patrimonio del damnificado.

k) De *lege ferenda* debe promoverse el dictado de una ley que prevenga el uso incorrecto o abusivo de la información nominativa. [38]

IV.- Política criminal y delitos informáticos

Teniendo en cuenta que el Derecho siempre va detrás de los acontecimientos, circunstancia que se patentizada en el caso de Internet, por su evolución permanente, implica un necesario crecimiento del Derecho Penal para justificar la persecución de delitos relativos a la problemática de la informática, so riesgo de lesionar el principio de legalidad.

El referido principio comporta una de las garantías de mayor trascendencia para el individuo frente al poder punitivo estatal, pues si existe una conducta que no está prohibida, no podrá ser penado por haberla cometido hasta que ella haya sido efectivamente sancionada como delito en la ley.

La expansión desmesurada que -en forma constante y aproximadamente a partir de la década de los años noventa del siglo que se fue- viene experimentando la legislación penal, constituye una característica arquetípica de nuestras sociedades". [39] Se trata, sin duda, de un fenómeno global, del cual, la República Argentina, no ha escapado.[40]

La realidad social exige un aggiornamiento y, por tanto también en la intervención penal, pero siempre que esa intervención aparezca como razonable. Para ello, resulta necesario desmantelar la estructura ideológica de la emergencia continua y programar líneas político-criminales que encuentren un firme basamento en

[38] BUSTAMANTE ALSINA, Jorge, "La informática y la responsabilidad civil", LA LEY 1987-B, 892, Responsabilidad Civil, Doctrinas Esenciales, Tomo VI, 21-LLP 1987, 631.

[39] SILVA SÁNCHEZ, Jesús María, La expansión del Derecho penal. Aspectos de la política criminal en las sociedades post industriales, 1ª edición, Ed. Civitas, Madrid, 1999.

[40] CESANO, José Daniel, "Discursos de emergencia y política criminal: tendencias de la política criminal argentina en los albores del siglo XXI", *Cuadernos de Política criminal*, 2ª época, Centro de Estudios Superiores de Especialidades Jurídicas, N° 86, Madrid, 2005.

investigaciones de carácter empírico criminológico que podrían proporcionar al legislador información previa a optar por la criminalización de una determinada conducta.

Riquert antes de las reforma introducidas al Código Penal en materia de criminalística informática predecía que: "Para algunas ramas del derecho puede resultar una fértil idea la señalada por Gregorio Badeni, cuando manifiesta que frente a tales adelantos es necesaria una razonable interpretación dinámica de las leyes para que, sin necesidad de acudir a su reforma, se pueda evitar que queden a la zaga de la realidad social (su columna de opinión titulada "La interpretación dinámica de la ley", p. 35, diario Clarín del 13/4/99). […] En consecuencia, si estamos socialmente convencidos de que complementando la protección de nuestro ámbito de privacidad es necesario que ella tenga nivel penal, será preciso para concretarla que el legislador modifique los tipos penales pertinentes pues es el único modo en que la garantía constitucional que es el principio de legalidad no sea afectada." [41]

Desde el inicio de este siglo, la política criminal Argentina se ha caracterizado por sumarse a esta tendencia generalizada hacia la expansión penal. Así se han operado reformas en la materia aquí tratada, por caso, en la ley 25.326 (2/11/2000), destinada a la protección de los datos personales (y por tanto vinculada con el artículo 43, 3° párrafo de la Constitución Nacional, que consagra el *Hábeas Data*), introdujo dos nuevas figuras al Código Penal: a) por una parte, el artículo 117 bis, en cuyo párrafo primero se consagraba una suerte de falsedad ideológica, que sólo se distinguía del delito previsto por el artículo 293, por el limitado objeto de protección (ya que no se trataba de cualquier documento sino de las constancias de los datos personales contenidas en el correspondiente registro) [texto, según veremos, derogado por la ley 26.388] y b) por otra, el artículo 157 bis que prevé los tipos de acceso ilegítimo a un banco de datos personales y de revelación ilegítima de la información registrada en los mismos. En la ley 25.506 (14/12/2001), de régimen legal de la firma digital, que incorporó el art. 78 bis al Código penal, ampliando la significación de los conceptos

[41] RIQUERT, Marcelo A., "Nuevas tecnologías, ataques a la privacidad y sus repercusiones penales", LA LEY 1999-E, 70.

suscripción, firma y documento, a los digitales (texto también derogado por la ley 26.388). [42]

Un delito informático, es una conducta en contravención con las leyes, que se efectúa al utilizar como medio un equipo informático. Afecta la seguridad informática, pues se obtienen datos que involucran la privacidad de personas, instituciones o empresas, se viola correos electrónicos, se roba la identidad, etc. Varían desde lo que se conoce como ciberporno, piratería, falsificación de documentos mediante una computadora, lectura, sustracción o copiado de información confidencial, uso no autorizado de programas de cómputo, acceso a áreas informatizadas en forma no autorizada, difamación por Internet o hasta los temibles virus informáticos.

Como consecuencia de la necesidad de modificar ciertos aspectos de los tipos penales ya contemplados en el Código Penal y receptar así las nuevas tecnologías como medios comisivos para su ejecución, se sancionó la Ley 26.388, en junio del 2008 (Adla, LXVIII-C), que si bien no contempló ni previó algunos tipos penales que pueden materializarse a través de la informática como medio comisivo, entre otros, hurto, delitos contra la propiedad intelectual, régimen penal cambiario, y que puede traer aparejado la atipicidad de estas conductas cuando fueran perpetradas bajo la modalidad de la criminalidad informática, en aras del principio de principio de especialidad, puede afirmarse que la referida normativa, en su generalidad, resulta cuidadosa en los conceptos y definiciones empleadas. No incorporó ningún tipo omisivo, ni doloso, ni culposo, lo cual debe destacarse en un Estado de Derecho, respetuoso del principio de reserva de los ciudadanos.

La reforma instaurada al Código Penal en materia de criminalidad informática, por la citada ley, se encargó inicialmente de efectuar una modificación al art. 77 del Código Penal, brindando precisiones acerca de los términos *documento, firma, suscripción, instrumento privado y certificado*, sumándolos -junto con sus significaciones jurídicas- al ya mencionado artículo. Agregó para ello tres párrafos al final de dicho artículo y derogó el artículo 78 que ya establecía los conceptos de *firma digita y suscripción.*

[42] CESANO, José Daniel, "La política criminal Argentina: ¿últimas imágenes del naufragio?", Sup. Penal 2009 (mayo), 1-LA LEY 2009-C, 1099.

Como se expresara retro no se crearon nuevos tipos penales, sino que se modificaron ciertos aspectos de los ya existentes para receptar las nuevas tecnologías como medios comisivos para su ejecución. Los tipos penales previstos en ella son: el Ofrecimiento y Distribución de Imágenes relacionadas con Pornografía Infantil (artículo 128 C.P.N), Violación de Secreto y Privacidad (artículos 153, 153 bis, 155, 157, 157 bis C.P.N), Estafa y otras Defraudaciones (artículo 173, inciso 16, C.P.N.), Daño o sabotaje informático (artículos 183 y 184, C.P.N.), Interrupción de Comunicaciones (Artículo 197 C.P.N.), Alteración de pruebas electrónicas (artículo 255 C.P.N.).

El aumento de casos de pornografía infantil por medio de la web hizo necesario la modificación del anterior artículo 128, no sólo introduciendo nuevas modalidades típicas, sino también incorporando los medios electrónicos como formas de comisión. El nuevo texto especifica como destinatario de la norma a los menores de 18 años, omitiendo al igual que la redacción anterior, otorgar protección a los incapaces mentales. El bien jurídico protegido es la protección del menor. El objetivo de este nuevo tipo penal reside en reprimir la explotación de niños en la producción de cualquier representación suya en actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales.

Se agregó el Capítulo III, del Título V, del Libro II del Código Penal, intitulado "Violación de Secretos". La mención del bien jurídico "Privacidad" en el que no sólo protegen datos "secretos" como sinónimo de intimidad de los individuos exige una protección más intensa que su vida privada, dadas las debilidades técnicas de los sistemas informáticos y la mayor intervención estatal.

La ley de marras incluye dentro del concepto amplio de "correspondencia" a las comunicaciones electrónicas, solucionando por vía legislativa las controversias generadas en la doctrina y la jurisprudencia sobre la posibilidad de asimilar el correo electrónico ("e-mail") a la correspondencia tradicional. Pena a aquél que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

La ausencia de una definición precisa del concepto [comunicación electrónica], conllevará a su constante reformulación en virtud de los incesantes avances tecnológicos. Por ello, creemos que la jurisprudencia deberá precisar los alcances de este elemento normativo del tipo penal recurriendo a tal fin a la función reductora del bien jurídico. Por ejemplo, el acceso sin autorización del titular de la cuenta de correo electrónico de un mail basura o "spam" no podrá entenderse típico pues en modo alguno se lesiona la privacidad del sujeto pasivo.[43]

En el mismo capitulo se reprime con multa a aquél que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros. Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

Asimismo se castiga al funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos, introduciendo aquí la ley la palabra "datos" con lo cual amplía el objeto de protección penal.

El artículo 157 bis, en su inciso 1°, reprime con prisión de un mes a dos años al que a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales.

Es sujeto activo del delito quien accede a sabiendas (dolo directo) de cualquier forma a un banco de datos personales, enunciando la ley dos modalidades comisivas específicas: acceder "ilegítimamente" o "violando sistema de confidencialidad y seguridad de datos"; es decir, en ambos supuestos debe tratarse de un acceso sin autorización del titular o de la ley.

El objeto de protección penal son los archivos de datos personales, o sea, el conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento electrónico o no, cualquiera fuere la modalidad de su formación, almacenamiento, organización o acceso (art. 2°, ley 25.326). El bien jurídico protegido

[43] FILLIA, Leonardo César; MONTELEONE, Romina; NAGER, Horacio Santiago; ROSENDE, Eduardo E.; SUEIRO, Carlos Christian, “Análisis a la reforma en materia de criminalidad informática al Código Penal de la Nación (ley 26.388)”, Sup. Penal 2008 (agosto), 15-LA LEY 2008-E, 938.

es la privacidad, que se vería afectado cuando los datos estén contenidos en servidores públicos atento a las limitaciones propias del estado de la capacidad de almacenamiento conforme a la ley de Habeas Data.

La ley 26.388, establece además, en su artículo 9° una incorporación al artículo 173, el inciso 16, como supuesto de defraudación informática o fraude informático. Elabora como verbo típico el acto de manipular algún elemento. La manipulación que el tipo requiere, es decir la alteración del normal funcionamiento, es el abuso de la confianza depositada, la frustración de expectativas y buena fe o posturas elusivas ante reclamaciones de la contraparte.

Esta norma distorsiona el concepto de defraudar recogido en todo el capítulo, toma quizá de manera solapada la última de las acepciones gramaticales que se asimila al acto de apoderarse propio del hurto (que es en definitiva lo que está legislando, esto es, un hurto sofisticado pero hurto al fin), y que aún con todo ello, de manera confusa y poco respetuosa del principio de estricta legalidad, fuerza un concepto para elevarlo punitivamente a la categoría de defraudación sin caracteres óntico-ontológicos a nivel de la conducta descripta, que se diferencien del apoderamiento ilegítimo de lo ajeno ya contenido en el artículo 162 de la ley de fondo.[44]

El artículo 12 sustituye el artículo 197 del Código Penal, refiriéndose al que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida. El bien jurídico protegido es entonces la comunicación, que en lo que respecta al tipo penal no necesita estar en curso de ejecución. Se garantiza la posibilidad de comunicarse por parte de la ciudadanía, mediante los sistemas de mensajería instantánea, voz sobre ip, los protocolos sobre los cuales corren los servidores de correo, telefonía celular, mensajería de texto, radio unilateral y bilateral, las redes internas, así como las redes privadas virtuales u otro sistema que de cualquier forma permitan el diálogo o la transmisión de información entre dos o más personas.

El art. 13 sustituye al 255 del Código Penal, reprimiendo al que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia

[44] FILLIA, Leonardo César, et.al., op.cit.

de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

La alteración debe ser en un aspecto medular del documento, registro u objeto calificado como elemento de prueba o confiado en su custodia por razones de interés público.

La presente modificación legal al sistema penal ha tenido el propósito fundamental de ajustar las disposiciones penales tradicionales a las nuevas formas de comunicación y al empleo de sistemas tecnológicos, recurriéndose para ello a una nueva definición del concepto de documento y de cosas pasibles de protección, extendiéndose la tutela del ordenamiento penal a aquellos objetos intangibles como el correo electrónico, las comunicaciones provistas por los sistemas de mensajería electrónica, el software, las páginas creadas y colocadas en internet, la información almacenada en soportes magnéticos o electrónicos, y otras aplicaciones surgidas a partir del incesante avance cibernético.[45]

Con el lógico desarrollo de las tecnologías continuará también la materialización de nuevas previsiones legislativas que harán lo imposible por abarcar conductas delictivas cometidas vía Internet.

De las reformas introducidas al Código Penal a partir del año 2000, la mayoría de ellas responden a transformaciones securitarias. Con excepción de las leyes 25.326, 25.506, 26.364 y 26.388 que importan modificación en el catálogo de bienes jurídicos protegidos (criminalidad informática [o aspectos a ella vinculada – firma electrónica, *hábeas data*-] y trata de personas), entre otras, dada la problemática tratada en este trabajo. “Hemos dicho que uno de los rasgos que caracterizan a la política criminal argentina actual es la de expandir el ámbito de la intervención penal a sectores que, tradicionalmente, no fueron abarcados. Esto hace decir gráficamente a Cancio Melía (2000:147) que los legisladores encuentran bienes jurídicos *hasta debajo de las piedras*. Y en tal sentido, consideramos que uno de los factores que podrían evitar este degenerado y anárquico crecimiento, estaría representado por un mayor conocimiento de estas cuestiones empíricas. Es que si no se conoce esta realidad, la legislación irremediablemente vulnerará principios elementales que, la creación del Derecho penal

[45] TAZZA, Alejandro O. y CARRERAS, Eduardo, “La protección del banco de datos personales y otros objetos de tutela penal”, LA LEY 2008-E, 869.

debiera resguardar; concretamente: a) *in dubio pro libertate*, b) tolerancia, c) ponderación de daños y ventajas al momento de decidir una intervención penal y d) practicidad procesal. En otras palabras la decisión de criminalización sólo debe producirse después de constatar la inexistencia de un medio menos lesivo de resolución del problema y después de concluir que los beneficios esperados con esa criminalización superan los costes que ésta puede comportar".[46]

CONCLUSIONES Y REFLEXIONES FINALES

Parece claro que el derecho a la protección de datos es una reacción, una defensa frente al avance de la informática. Su estructura conceptual actual está concebida en la era tecnológica. A ella le debe su existencia, y en disputa con ella, pretende devolver al individuo la dimensión de su privacidad amenazada, y en muchos casos arrebatada. [47]

Siguiendo al maestro Morello, cabe sugerir que debemos abocarnos a dictar una ley que regule Internet y que en materia de responsabilidad civil, contemple principios tales como: que el proveedor de servicios demuestre la real imposibilidad del control del contenido nocivo y de identificar al autor del material dañino, para lo que sería necesario crear un registro de web que permita individualizar al proveedor de una noticia o información. El proveedor de servicios, para no incurrir en censura, podría notificar al autor conocido de un material dañino anoticiándolo que procederá a su supresión. Que en caso de dudas sea el prestatario de información quien requiera al proveedor del contenido que acredite la veracidad de sus afirmaciones aunque ellas contengan denuncias de posibles ilícitos y, demostrada la verdad de la información, la suprima o asuma el juicio de reparación civil por los daños que promoverá el damnificado. En los casos de autores anónimos a los identificados, se transfiera por vía de principio la responsabilidad civil al autor. Que ante un material dañoso el damnificado pueda reclamar al proveedor su eliminación y este último actúe, de ser técnicamente posible, acogiendo esa petición. No perder de miras que el usuario celebra

[46] CESANO, José Daniel, op. cit., pág. 17
[47] EKMEKDJIAN, Miguel Ángel y PIZZOLO, Calogero (h), *Habeas data, El derecho a la intimidad frente a la revolución informática"*, Editorial Despalma, s/d, pág. 21

un contrato con su proveedor de información, y los conflictos jurídicos entre ambos se rigen por el sistema convencional o negocial de responsabilidad, mientras que pertenecen a la órbita de la responsabilidad civil extracontractual las restantes cuestiones. Ello sin perjuicio de la eventual invalidez de las cláusulas abusivas impuestas por la empresa predisponente. Es necesario que converjan los esfuerzos tendientes a sumar las vías instrumentales para la evitación y reparación del daño: códigos de conducta, sistemas de filtrados en la base para la protección de los menores, identificación de los operadores de la red e incluso de los usuarios por medio de la encriptación, sistemas alternativos de solución extrajudicial rápida y eficaz de las disputas, acciones de cesación del daño. El operador jurídico debe armonizar los tres principios en que se soporta el orden jurídico: legalidad, seguridad jurídica y razonabilidad.[48]

La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, pues, resulta evidente que las categorías contenidas en algunas leyes fueron desarrolladas sin imaginar qué nivel de exposición generaría Internet, ni las herramientas de búsqueda que hoy existen.

Esta regulación tiene que buscar, no el control y la represión sino la facilidad de acceso, la igualdad y el fomento del uso de la red, que es una herramienta útil para el desarrollo de las modernas sociedades. Se deben ir superando las diferencias territoriales, garantizar el acceso a todos los ciudadanos a la red que se logrará con el consenso de variables de diversos tipos y no sólo jurídicas, labor de universalización a la que están llamados los poderes públicos.

Sin detenimiento y en forma creciente se están construyendo vidas virtuales a través de usuarios en redes sociales, comentarios en foros, cuentas de mensajería, dirección de correos electrónicos, entre otras formas que amplían la influencia de terceros en nuestras vidas y por ende en nuestra intimidad.

La información que contiene la Red nos sobrevive. Así la pregunta que surge *a priori* es ¿Qué sucede con los datos incorporados al ciberespacio?

[48] MORELLO, Augusto M., "El proceso justo y las garantías jurisdiccionales" en "*Derechos y garantías en el siglo XXI*", dirs.: Aída Kemelmajer de Carlucci y Roberto M. López Cabana, 1999, Ed. Rubinzal-Culzoni, p. 386. En el mismo sentido Morello, Augusto M., "El principio de la seguridad jurídica", JA 1992-IV-886; Kemelmajer de Carlucci, Aída "Seguridad y justicia", JA 1993-I-813.

Lo que verdaderamente importa es que nuestros *bits* nos sobreviven y pueden ser mantenidos de forma artificial o no, por tiempo indefinido. Más allá de ello es importante que existe la posibilidad de salvaguardar la información, pues las proveedoras de servicios electrónicos –Google, Gmail, Hotmail, entre otras- nos permiten acceder a las cuentas para obtener los contenidos de los mensajes enviados o recibidos. Otro tanto sucede con las redes sociales –a modo de ejemplo Facebook- donde muchas personas comparten sus vidas convirtiéndose en verdaderos y gigantescos álbumes o baúles de recuerdos. Al fallecer un usuario estas redes sociales no desactivan la cuenta, sino que pasan a tener otro estado en el que eliminan información privada y sólo el círculo íntimo del occiso –confirmación de por medio- puede tener acceso a ella.

En la actualidad existen sitios que se encargan de mantener segura la información de sus usuarios mediante el pago de un canon locativo y, en el desafortunado caso que expiremos, se obligan a enviar esos datos a las personas que designen como responsables y que heredan dicha información, evitando así el olvido.

El peligro potencial es que los datos se pierdan en la posibilidad de traducción de formatos, teniendo en cuenta la variabilidad de estos últimos hoy en día. La solución es la implementación de formatos con estándares abiertos, para su evolución sin riesgos. La privacidad se destruye no por la información en sí misma, sino por su transmisión disfuncional sobre la que el afectado pierde toda posibilidad de influir.

Lo cierto es que todas las cuentas que tenemos en el espacio virtual son personales y la decisión de exhibir la información *on line* u ocultarla e incluso mantenerla después de muertos es nuestra, por tanto resulta indispensable plantearse este problema para que el progreso de Internet no nos pase en forma desapercibida.

BIBLIOGRAFÍA GENERAL CONSULTADA

AGOGLIA, Marta M., et. al., "Responsabilidad civil por daños causados por el procesamiento electrónico de datos personales", JA 1991-I-879.

ALTERINI, Atilio A, - "Cultura y derecho privado", L.L., del 12-IV-1996
- "Respuestas ante las nuevas tecnologías: Sistema, principios y jueces", LA LEY 2007-F, 1338.

AMAYA, Jorge Alejandro, "El habeas data: una garantía en dos dimensiones", *en Defensa de la Constitución Garantismo y Controles, Libro en reconocimiento al Dr. Germán J. Bidart Campos*; Víctor Bazán – Coordinador-, Ediar, Buenos Aires, 2003 pág. 777.

ANDORNO, Luís, La informática y el derecho a la intimidad, LA LEY 1985-A, 1100- Responsabilidad Civil Doctrinas Esenciales, Tomo VI, 3.

ARMAGNAGUE, Juan F., *Derecho a la información, habeas data e Internet*, Buenos Aires, La Rocca, s/d.

BALLONE, Mariano C. y GERMAIN, Pablo C, "Tributación en el comercio electrónico", LA LEY 2000-C, 1224.

BASTERRA, Marcela I., - "Habeas Data: Derechos Tutelados", Doctrina Judicial, 1999-3; p.77.
- "Aspectos procesales y sustanciales del habeas data en un fallo de la Corte Suprema de Justicia de la Nación", LA LEY 2005-B, 741.

BAZAN, Víctor, - "El Hábeas Data y sus particularidades frente al amparo", en Revista de Derecho Procesal, N°4 – I, Rubinzal-Culzoni, Santa Fe, Argentina, 2000, p. 261.
- Defensa de la Constitución, Garantismo y Controles. Libro en reconocimiento al Dr. Germán J. Bidart Campos. Coordinador. Ediar, Buenos Aires, 2003.

BIANCHI, Alberto B., "Habeas data y Derecho a la privacidad", ED, 161-866.

BIDART CAMPOS, J. Germán, *Teoría General de los Derechos Humanos*, Ed. Astrea, 1991, pág. 71.

BORDA, Alejandro, "La responsabilidad extracontractual por ilicitudes informáticas", en las jornadas en homenaje a Jorge Bustamante Alsina, ED 139-936.

BUERES, Alberto J. y HIGHTON, Elena, *Código Civil y normas complementarias. Análisis doctrinario y jurisprudencial* - 3 A, Editorial Hammurabi, Bs. As., 1999.

BUSTAMANTE ALSINA, Jorge, - "La informática y la responsabilidad civil", LA LEY 1987-B, 892
- *Teoría general de la responsabilidad civil*, 7ª ed., Ed. Abeledo Perrot, 1992.

CAFFERATA, Fernando J., “Utilización de la red de internet. La jurisdicción y el derecho aplicable para solucionar conflictos”, LA LEY 2001-B, 1281-LLP 2001, 801. Derecho Comercial Doctrinas Esenciales, Tomo II, 1237.

CAMPANELLA DE RIZZI, Elena Margarita y STODART DE SASIM, Ana María, “Derecho a la intimidad e informática", LA LEY 1984-B, p. 667.

CASTRILLO, Carlos V., “Responsabilidad civil de los buscadores de Internet”, LA LEY 11/01/2010, 1.

CESANO, José Daniel, - “Discursos de emergencia y política criminal: tendencias de la política criminal argentina en los albores del siglo XXI”, *Cuadernos de Política criminal*, 2ª época, Centro de Estudios Superiores de Especialidades Jurídicas, N° 86, Madrid, 2005.
- La política criminal Argentina: ¿últimas imágenes del naufragio? Sup. Penal 2009 (mayo), 1-LA LEY 2009-C, 1099.

CHIRINO SANCHEZ, Alfredo, "Algunas reflexiones acerca de la tutela penal de la autodeterminación informativa. El caso del Proyecto de Código Penal costarricense de 1995". Nueva Doctrina Penal, Vol. 1997-A, Editores del Puerto, Buenos Aires

CIFUENTES, Santos, - *Derechos Personalísimos*, Buenos Aires, 1995.
- "Protección inmediata de los datos privados de la persona. Habeas data operativo", LA LEY 1995-E, p. 293.
- "La moral y los riesgos en las jornadas de Junín. Los medios masivos de comunicación", JA 1995-I, p. 798.

COLAUTTI, Carlos E., - “La libertad de expresión y el espacio cibernético”, LA LEY 1999-E, 1329.
- “El largo camino de la abolición de la censura", LA LEY 1992-E, 1149.

DALL’AGLIO, Edgardo Jorge, “Aspectos de la Responsabilidad Civil Emergente de las Relaciones Informáticas”, El Derecho, Jurisprudencia General, Tomo 117, Buenos Aires, 1986.

DELPIANO ASCENCIO, Héctor M., “Algunas reflexiones acerca del VI Congreso Iberoamericano de Derecho e Informática”, JA 1999-II-1053.

ECO, Umberto, *Cómo se hace una tesis, Técnicas y procedimientos de investigación, estudio y escritura*, Editorial Gedisa, Barcelona España, 1996.

EKMEKDJIAN, Miguel A., - *Tratado de Derecho Constitucional*, tomo I, Ed. Depalma, 1993.
- *Derecho a la Información*, Ed. Depalma, 2ª ed., Buenos Aires, 1996.

- Manual de la Constitución Argentina, ed. Lexis Nexis. Depalma, quinta edición, 2002, p 95.

EKMEKDJIAN, Miguel Ángel y PIZZOLO, Calogero (h), *Hábeas Data. El derecho a la intimidad frente a la revolución informática*, Ediciones Depalma, Buenos Aires, 1998.

FERNANDEZ DELPECH, Horacio, *Internet: su problemática jurídica*, Bs.As., Abeledo Perrot, 2001, cap. IV ap. I, pág. 50/51.

FERNÁNDEZ RODRÍGUEZ, José Julio, "¿Regular Internet? Una reflexión sobre los límites del derecho y las funciones del estado", *en Defensa de la Constitución Garantismo y Controles, Libro en reconocimiento al Dr. Germán J. Bidart Campos*; Víctor Bazán – Coordinador-, Ediar, Buenos Aires, 2003, pág. 470.

FERREIRA RUBIO, Delia, *El derecho a la intimidad. Análisis del art. 1071 bis, del Código Civil*, 1982, pág. 102.

FERNÁNDEZ SEGADO, Francisco, "La dignidad de la persona como valor supremo", ED 166-907.

FILLIA, Leonardo César; MONTELEONE, Romina; NAGER, Horacio Santiago; ROSENDE, Eduardo E.; SUEIRO, Carlos Christian, "Análisis a la reforma en materia de criminalidad informática al Código Penal de la Nación (ley 26.388)", Sup. Penal 2008 (agosto), 15. LA LEY 2008-E, 938.

FORMARI, María Julia – LAVALLE COBO, Jorge, "El derecho a la intimidad y su relación con las comunicaciones electrónicas", LA LEY 2007-F, 1307.

FRENE, Lisandro, "Responsabilidad de los 'buscadores' de Internet", LA LEY 2009-F, 1219.

GALDÓS, Jorge M., GALDOS, Jorge Mario, " Responsabilidad civil de los proveedores de servicios en Internet "Responsabilidad civil e internet: Algunas aproximaciones", LA LEY 2001-D, 953-Responsabilidad Civil Doctrinas Esenciales Tomo VI, 69

GALINDEZ, Maricel, "Acceso ilegítimo a sistemas informáticos. La informática y el derecho a la intimidad. Necesidad de una reforma", ED del 7/10/1999.

GARONE, Guillermo, "Delitos cometidos vía Internet. El nuevo art. 128 del Código Penal", LA LEY 2010-A, 1151.

GIANFELICE, Mario C., "Responsabilidad civil emergente de la informática", LA LEY 1987-D, 1186.

GINI, Santiago Luís, "Internet, buscadores de sitios Web y Libertad de Expresión", LA LEY, Sup. Act. 23/10/2008.

GOLDENBERG, Isidoro, "La tutela jurídica de al vida privada", LA LEY 1976-A-581.

GONZÁLEZ PONDAL, Tomás Ignacio, “Facebook: Reflexiones sobre el derecho a la intimidad”, Sup. Act. 26/05/2009, 1, LA LEY Online

GOZAÍNI, Osvaldo Alfredo, - *El Amparo. Los Nuevos Derechos y Garantía del Art. 43 de la Constitución Nacional, 2da. Edición, Corregida, ampliada y actualizada*, Ediciones Depalma, Buenos Aires, 1998

- *Hábeas Data. Protección de datos personales. Doctrina y jurisprudencia*, Editores Rubinzal-Culzoni, Santa Fe, 2001.

GRATTON, Pierre: "Protección informática", Editorial Trillas, 1° Edición, México, 1998.

HERRÁN ORTÍZ, Ana Isabel, *La Violación de la Intimidad en la Protección de Datos Personales, Editorial Dukinson, Madrid 1998.*

HOERSTER Norbert, "Acerca del significado del principio de dignidad humana", p. 92, en SAGÜES, Néstor Pedro, "Dignidad de la persona e ideología constitucional", JA 1994-IV-904.

KEMELMAJER DE CARLUCCI, Aída, "Seguridad y Justicia", JA, 1993-I-813.

LEMON Alfredo, "La dignidad de la persona desde la Constitución Nacional", ED 168-875.

LLAMBIAS, Jorge, *Tratado de derecho civil. Obligaciones*, t. IV-B, Ed. Perrot, Buenos Aires, 1980

LLOVERAS DE RESK, Maria Eugenia, "La intrusión a la intimidad a través de la informática", JA 1989-II-916.

MASCIOTRA, Mario, *El Hábeas Data, La garantía polifuncial*, Librería Editorial Platense, La Plata, 2003.

MOLINA QUIROGA, Eduardo, - "Autodeterminación informativa y habeas data", JA 2/4/97.

- "Internet y libertad de expresión. A propósito de la ley 26.032", JA 2005 - III, p. 865.

MORELLO, Augusto M., - "El principio de la seguridad jurídica" JA, 1992-IV-886;

- "El proceso justo y las garantías jurisdiccionales" en *Derechos y Garantías en el Siglo XXI*, Dir.: Aída Kemelmajer de Carlucci - Roberto M. López Cabana, Ed. Rubinzal-Culzoni, Santa Fe, 1999, pág. 386

- "Los contenidos de la pretensión procesal penal y de la garantía de `hábeas data´". LA LEY, 1998-F, 369.

MOSSET ITURRASPE, Jorge y PIEDECASAS, Miguel A., *Código Civil Comentado, Responsabilidad Civil, Doctrina-Jurisprudencia-Bibliografía*, Editores Rubinzal-Culzoni, Santa Fe, 2003.

PALAZZI, Pablo Andrés, *"El Habeas Data en el Derecho Constitucional Argentino"*, en *La Defensa de la Intimidad y de los Datos Personales a través del Habeas Data. Ley 25.326.* Coordinado por Osvaldo Alfredo Gozaíni, Ediar, Buenos Aires, 2001, pág. 52.

PARELLADA, Carlos A., - "Causalidad y actos omisivos (o conducta inerte)", en Revista de Derecho de Daños, Ed. Rubinzal y Culzoni, To. 2003-2, pág. 103

- "Responsabilidad por la actividad anónima en Internet", LA LEY 2007-F, 1066.

PIZARRO, Ramón Daniel, "glosa al art. 1113 del Cód. Civil", en BUERES, A. J (Dir.) - HITHONH, E. I. (Coord.), *Código Civil y normas complementarias. Análisis doctrinario y jurisprudencial*, T° 3-A, Hammurabi, Bs. As. 1999, pág. 556.

QUIROGA LAVIÉ, Humberto, *Derecho a la Intimidad y Objeciones de Conciencia*, Universidad del Externado de Colombia, p.10

QUIROGA LAVIÉ, Humbero, BENEDETTI, Miguel Ángel, CENICACELAYA, María de la Nieves, Derecho Constitucional Argentino, Segunda edición actualizada por Humberto Quiroga Lavié, Tomo I, Editores Rubinzal Culzoni, 2009.

RIQUERT, Marcelo Alfredo: - "Informática y Derecho Penal Argentina", Editorial Ad-Hoc, 1° Edición, Buenos Aires, 1999.

- "Algo mas sobre la delincuencia informática en el MERCOSUR a propósito de la modificación al Código Penal Argentino por Ley 26388" http://www.ciidpe.com.ar/areas_especial_dpe.php

RIVERA, Julio César, "Los derechos a la intimidad y el honor frente al derecho a la información" (de Ponzetti de Balbin a Campilla, Colección de Análisis Jurisprudencial Derecho Civil) - Parte General - Editorial LA LEY 2003, 13.

RODRIGUEZ HAUSCHILDT, Victoria M.M., *Derecho Informático*, Editorial Aplicación Tributaria S.A., Buenos Aires, 2007.

SAGÜES, Néstor P., "Amparo, habeas data y habeas corpus en la reforma constitucional", LA LEY 1994-D, 1151.

SILVA SÁNCHEZ, Jesús María, *La expansión del Derecho penal. Aspectos de la política criminal en las sociedades post industriales*, 1ª edición, Ed. Civitas, Madrid, 1999.

SOBRINO, Waldo Augusto Roberto, "Argentina: Responsabilidad de las Empresas Proveedoras de Servicios de Internet", http://www.alfa-redi.org/rdi-articulo.shtml?x=538

STIGLITZ, Gabriel A. y STIGLITZ, Rosana M., "Responsabilidad civil por daños derivados de la informática", LA LEY 1987-E, 795.

STIGLITZ, Rubén - STIGLITZ, Gabriel, "Contratos por adhesión, cláusulas abusivas y protección al consumidor", Ed. Depalma, Buenos Aires, 1985, ps. 141 y sigts.

TAZZA, Alejandro O. y CARRERAS, Eduardo, “La protección del banco de datos personales y otros objetos de tutela penal”, LA LEY 2008-E, 869

TOBIAS, José W.; FELDMAN, Paula, “Derechos personalísimos. La tensión entre el derecho a la intimidad y la libertad de información. Los derechos personalísimos y las personas fallecidas. La causa "Ponzetti de Balbín", Colección de Análisis Jurisprudencial Derecho Civil - Parte General - Director: José W. Tobías, Editorial LA LEY 2003, 291.

UICICH, Rodolfo Daniel, *Los Bancos de datos y el Derecho a la Intimidad*, Editorial Ad-Hoc SRL, Buenos Aires, 1999

VIBES, Federico Pablo, "Internet y privacidad. La difusión en Internet de imágenes lesivas de la intimidad, el honor y otros derechos personalísimos", LA LEY 2000-D.

WEGBRAIT, Pablo, "La responsabilidad de los proveedores de servicios de Internet por violaciones al derecho de autor", LA LEY 2000-F, 1143.

ZAVALA DE GONZÁLEZ, Matilde, - *Resarcimiento de daños a las personas*, Editorial Hammurabi, 1994.

- “El derecho de daños. Los valores comprometidos”, LA LEY 1996-E, 1190. Responsabilidad Civil Doctrinas Esenciales Tomo I, 287

JURISPRUDENCIA

-C.S.J.N., 11/12/1984, “Ponzetti de Balbín, Indalia c. Editorial Atlántida, S. A.”, LA LEY 1985-B, 120.

- C.S.J.N., 03/02/2009, “Solaro Maxwell, María Soledad c. Yahoo de Argentina S.R.L. y otro” Publicado en, La Ley Online; Cita Fallos Corte: 332:47

- C.Cont.Ad. y Trib. Ciudad Bs.As., sala 2ª, 30/4/2002, "J. A." 2003 - IV, p. 65, con nota de Carranza, Luís R. y Palazzi, Pablo A. "Derecho de acceso a la información pública y derecho de acceso a la información privada (hábeas data): Semejanzas y diferencias".

-CNCiv, Sala F, 6/7/1995, J.A. 1996 - II, p. 397 y LA LEY 1996-C, 473.

-CNCiv, sala E, 25/11/2005, R., H. c. Ediciones Paparazzi S.A., DJ, 2006-2-197.

-CNCiv. y Com. Fed., Sala 1, 14/11/2006, Capristo, Maria X. v. Yahoo de Argentina S.R.L. y otro, LA LEY Online.

-CNCiv, Sala I, 20/02/2007, Z., S. K. c. Yahoo de Argentina S.R.L. y otro, LA LEY Online.

-CNCiv, Sala J, 10/05/2007, Partes: K., A. P. v. Yahoo de Argentina S.R.L., LA LEY Online

-CNCiv, Sala H, 05/06/2008, G., J. C. c. Arte Radio Televisivo Argentino S.A. y otros, LA LEY, Online.

-CNCiv, Sala L, 18/06/2009, Mazza, Valeria Raquel c. Yahoo de Argentina S.R.L. y otro, LA LEY, Online.

CNCiv. y Comercial Federal, Sala I, 10/02/2009, Unteruberbacher, Nicole c. Yahoo de Argentina S.R.L. y otro, LA LEY 16/07/2009

-Juzgado Nacional de 1a Instancia en lo Civil Nro. 75, D.C., V. c. Yahoo de Argentina S.R.L. y otro, 29/07/2009, LA LEY, Online

Dra. MARIA LUCIA ANTUZ[*]

[*] SECRETARIA DE CÁMARA. CON FUNCIONES EN EL DEPARTAMENTO DE DOCUMENTACIÓN DEL PODER JUDICIAL DE NEUQUÉN