Universidad Siglo 21
Abogacía - Año 2010

El derecho a la intimidad en Internet

John Grover Dorado

RESUMEN

En los últimos años, las innovaciones científicas y tecnológicas han producido un cambio sustancial en todo el planeta. El contexto global actual, especialmente en el ámbito de las tecnologías de la información, resulta peculiar, pues ha derivado en la aparición de nuevos problemas jurídicos que resultaban inimaginables hasta hace tan sólo unos pocos años, y que el derecho debe intentar resolver. Internet, como una de las mayores aplicaciones de la Sociedad de la Información, requiere especial consideración por su carácter transnacional y su acelerado crecimiento tanto a nivel nacional como global.

En este orden de ideas, el presente Trabajo Final de Graduación estudiará la problemática relacionada con Internet y sus implicancias jurídicas en relación al derecho a la intimidad, entre las cuales se destacan: la afectación de la privacidad de los datos personales, el correo electrónico no solicitado o "*spam*", el monitoreo laboral del e-mail, las "*cookies*", las redes sociales, y, por último, la responsabilidad civil de los distintos sujetos que producen daños a través de la red.

ABSTRACT

During the last years, scientific and technological innovations have produced substantial changes all around the world. The current global context, especially in the field of technology of information, results unusual, because new legal issues that were unimaginable a few years ago have emerged, and law must try to solve them. Internet, as one of the largest applications of new technologies, requires special consideration because of its transnational characteristic, and its accelerated growth in both, global and national level.

This Final Graduation Project will study the problematic about Internet and its legal implications related to right to privacy. Among the main topics, there are included the following issues: the violation of individuals' personal data, junk mail or "spam", privacy of e-mail in labor scope, cookies, social networks, and, finally, liability of the various subjects that cause damages through the network.

AGRADECIMIENTOS

Quiero aprovechar estas primeras líneas para agradecer a todos y cada uno de aquellos que formaron parte de esta obra, directa o indirectamente:

A mis padres y hermana: gracias por acompañarme y alentarme en todo momento, y por el esfuerzo que realizan a la distancia.

A mis compañeros: sólo tengo para ellos palabras de gratitud por su entrañable amistad y compañerismo desde el primer día del cursillo de ingreso a la facultad. Gracias por compartir esta maravillosa e inolvidable etapa de mi vida.

ÍNDICE

CAPÍTULO III

EL DERECHO A LA INTIMIDAD

CAPÍTULO IV

PRIVACIDAD DE LOS DATOS EN INTERNET

CAPÍTULO V

PROBLEMAS JURÍDICOS DERIVADOS DEL CORREO ELECTRÓNICO

CAPÍTULO VI

RESPONSABILIDAD CIVIL

INTRODUCCIÓN

Las importantes innovaciones tecnológicas producidas en los últimos años - especialmente en el ámbito de las tecnologías de la información y la comunicación (TICs) - han generado un cambio sustancial en todo el planeta, ya sea a nivel económico, político, social y cultural en los individuos en particular y en las sociedades en general. Es así que, el contexto global actual resulta peculiar, pues han aparecido nuevos problemas jurídicos que resultaban inimaginables hasta hace tan sólo unos pocos años, y que el Derecho debe intentar resolver.

En este orden de ideas, dentro de los numerosos conflictos jurídicos planteados por el impacto de la informática y las telecomunicaciones en la sociedad actual, nos limitaremos a estudiar la problemática relacionada con Internet - como mayor exponente de las TICs - y sus implicancias en relación al derecho a la intimidad.

Creemos que el tema resulta de interés no sólo por su novedad y complejidad, sino principalmente por constituir un desafío para los juristas de la nueva era el hecho de intentar dar respuestas adecuadas a nuevas realidades.

Creemos, asimismo, que la cuestión no ha sido desarrollada de manera suficiente por la doctrina nacional, y esperamos que algunas de las consideraciones que se hagan en el presente Trabajo Final de Graduación puedan llegar a ser útiles para aclarar el incompleto panorama doctrinario.

Es por ello que, a lo largo de la obra, intentaremos no sólo describir las diversas situaciones que pueden afectar a la intimidad de los usuarios de Internet, sino que también abordaremos las distintas soluciones que desde la legislación y la jurisprudencia argentina resulten aplicables y/o se hubieren propuesto, todo ello, sin perder de vista las respuestas que se hubieren esbozado en el derecho comparado.

La estructura del presente trabajo constará de siete capítulos, que pasaremos a detallar a continuación.

En el capítulo I, esbozaremos algunas nociones básicas relativas a nuestro objeto de estudio; es así que se intentará dar un concepto de Internet, relatar su origen, como así su posterior evolución hasta el presente, dilucidar cuál es su naturaleza jurídica, y por último, exponer las distintas posturas acerca de la conveniencia o no de su regulación. Asimismo, abordaremos el concepto de "Sociedad de la Información", sus antecedentes, y el rol del derecho en la misma.

En el capítulo II, expondremos, aunque sea de manera breve, una problemática estrechamente relacionada con la intimidad: el derecho a la libertad de expresión en Internet. Consideraremos especialmente cómo influye el fenómeno de Internet en el concepto y la esencia misma de la libertad de expresión, poniendo atención en las libertades de contenido y de uso en Internet, la situación de la legislación y la jurisprudencia nacional en relación al tema, y, finalmente, la responsabilidad ulterior que surge del ejercicio abusivo de tales libertades, cuando se afectan otros derechos de igual o mayor jerarquía, entre los que se incluye al derecho a la intimidad.

En el capítulo III, nos referiremos al moderno significado que adquiere el concepto de derecho a la intimidad en la actualidad, desde el punto de vista del derecho constitucional y legal argentino, pero sin dejar de tener en cuenta la perspectiva que se tiene otros sistemas jurídicos más sofisticados, como lo son la normativa europea y estadounidense.

En el capítulo IV, trataremos el tema de la privacidad de los datos personales en Internet. Analizaremos las distintas formas de afectación a la privacidad de los datos personales de los usuarios, como así también expondremos las principales herramientas jurídicas con las que éstos cuentan para contrarrestar este problema. Nos referiremos particularmente a la aplicación de la ley 25.326 a las bases de datos publicadas u obtenidas a partir de la recolección de datos personales en Internet, a la captación y derivación de las comunicaciones en Internet, a las redes sociales como nueva modalidad de poner en riesgo la privacidad, y, por último, trataremos el tema de las "*cookies*" como herramienta de los navegadores de Internet para la recolección de datos personales.

En el capítulo V, estudiaremos las implicancias y conflictos jurídicos vinculados al derecho a la intimidad que el correo electrónico - como uno de los principales

servicios de Internet - puede ocasionar y cuál debería ser la legislación aplicable a las distintas situaciones que esta nueva herramienta genera. Expondremos principalmente tres cuestiones, a saber: la violación del e-mail como manifestación actual de la privacidad de la correspondencia, el correo electrónico no solicitado o *"spam"*, y las facultades del empleador de controlar el e-mail laboral de sus dependientes.

En el capítulo VI, analizaremos la responsabilidad de los sujetos que intervienen en los diversos servicios que ofrece Internet por los daños producidos como consecuencia de los distintos problemas jurídicos desarrollados en los capítulos anteriores. Vale decir, se tratarán las responsabilidades derivadas de la publicación de contenidos ilícitos y nocivos y de la afectación al derecho a la intimidad de los usuarios, desde la óptica del derecho civil argentino, excluyendo así el aspecto penal - los denominados delitos informáticos- y administrativo.

En el capítulo VII, a modo de colofón, reiteraremos ciertas conclusiones y propuestas dadas a lo largo del desarrollo de la presente tesis, reafirmando nuestra posición en cada uno de los temas tratados.

Por último, creemos necesario, dada la novedad y especificidad del problema, incluir un apéndice legislativo con las principales normas del derecho argentino que han sido objeto de análisis a través de la obra.

CAPÍTULO I

INTERNET EN LA SOCIEDAD DE LA INFORMACIÓN

A modo de introducción, y con el fin de lograr una mejor comprensión del problema jurídico que plantea Internet con relación al derecho a la intimidad, resulta imprescindible comenzar la presente obra esbozando algunas nociones básicas relativas a nuestro objeto de estudio. En esta primera parte, se intentará dar un concepto de Internet, relatar su origen, como así su posterior evolución hasta el presente, dilucidar cuál es su naturaleza jurídica, y por último, exponer las distintas posturas acerca de la conveniencia o no de su regulación.

En este orden de ideas, resulta imprescindible contextualizar nuestro objeto de estudio, vale decir, ubicar de manera temporal y espacial a la Internet. Para ello, se partirá del concepto de "Sociedad de la Información", pasando por sus antecedentes, hasta llegar a analizar el rol del derecho en la misma.

1. INTERNET: CONCEPTO

Puede definirse a Internet como "*una red de redes de alcance global que interconecta ordenadores autónomos entre sí, utilizando el protocolo de comunicación TCP/IP, con el objeto de compartir información, recursos y/o servicios*"[1].

De esta definición, deben hacerse las siguientes aclaraciones:

- Cuando se habla de una red de redes, se hace referencia a una red que no sólo interconecta ordenadores[2], sino que interconecta redes de ordenadores entre

[1] TREJO GARCIA, María del Carmen, "Investigación Parlamentaria sobre Regulación jurídica de Internet", 2006. Publicado en: http://www.diputados.gob.mx/cedia/sia/spe/SPE-ISS-12-06.pdf, consultado 09/09/2010.

[2] Se incluye dentro del término a todo tipo de computadoras, teléfonos celulares inteligentes, Asistentes Personales Digitales o PDA, y todo otro dispositivo idóneo para acceder a Internet.

sí, a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas telefónicas, etc.), con el objeto de compartir recursos.

- Internet sirve de enlace entre redes más pequeñas y permite ampliar su cobertura al hacerlas parte de una red global.

- Internet es una red descentralizada, caracterizada por la autonomía de cada máquina que forma parte de la misma, es decir, con la misma capacidad para enviar y recibir información entre ellas sin la intervención de un servidor o computadora central.

- Esta red global tiene la característica de que utiliza un lenguaje común que garantiza la intercomunicación de los diferentes partícipes; este lenguaje común o protocolo (un protocolo es el lenguaje que utilizan las computadoras al compartir recursos) se conoce como TCP/IP[3] (*Transfer Control Protocole/Internet Protocole*).

- En cuanto al objeto, si bien Internet en un principio se pensó con fines de intercambio de información, en la actualidad, la red resulta un medio versátil, pues puede ser utilizado con múltiples fines: permite ser empleado para leer periódicos con las últimas noticias, conversar con personas desconocidas o conocidas en tiempo real (*chat* y/o mensajería instantánea), hacer nuevos contactos en redes sociales virtuales, comprar y vender (*e-commerce*), operar en cuentas bancarias (*homebanking*), enviar y recibir texto, imágenes y videos con otros usuarios (*e-mail*), descargar música, software y películas, ver canales de TV de cualquier parte del mundo, entre otros servicios.

2. GÉNESIS Y EVOLUCIÓN

Internet tiene sus orígenes en años marcados por la Guerra Fría, específicamente en la década de 1960. En aquellos momentos, los organismos militares de los

[3] El protocolo que se adopta de manera uniforme para interconectar ordenadores a la red Internet, independientemente del servicio que se utilice, es el TCP/IP, el cual está formado por dos protocolos diferentes, unidos y acoplados:
"- TCP: el protocolo de control de transmisión define la manera en que la información será separada en paquetes y enviada a través de Internet, asegura de que cada paquete se recombine en el orden correcto, y los revisa para localizar posibles errores.
- IP: el protocolo de Internet es usado por computadoras especiales llamadas enrutadores (routers) para mover bits de información a través de la red. Cada paquete de información cuenta con la dirección IP tanto de la computadora que lo envió como de la que recibe el paquete."
Fuente: http://www.scribd.com/doc/11562881/Internet-Extranet-Intranet, consultado: 21/09/2010.

Estados Unidos intentaban buscar formas de comunicación alternativas que eliminaren cualquier tipo de autoridad central, debido a que, de existir una, sería el primer blanco ante un posible ataque proveniente del bloque soviético. Es así que nació ARPANET (*Advanced Research Projects Agency Network*), una red descentralizada formada por tres universidades y el Instituto de Investigación de Stanford. Para 1971, la red amplió su número de partícipes a quince, con la incorporación de otras universidades, centros de investigación, laboratorios y hasta organismos oficiales como la NASA. Dos años más tarde, ARPANET adquiere carácter internacional, con la adhesión de la Universidad *College of London* (Inglaterra) y del Centro de Investigación Sísmica de Noruega (NORSAR).

La historia de Internet se destaca en los años 80' con dos hitos, a saber: en 1982 se adopta el protocolo TCP/IP, y es allí cuando se comienza a usar la palabra Internet[4]; y en 1984 la Fundación para la Ciencia de los EEUU (NSF) da comienzo a una nueva red de redes: NSFNET, dedicada a la comunicación de la investigación y de la educación mediante nuevas y más rápidas conexiones. El desarrollo de dicha red en el incremento de la capacidad de transmisión de datos, hizo que la mayor parte de los miembros de ARPANET optaran por conectarse a esta nueva red y es en 1989 cuando finalmente se disuelve. NSFNET, junto a otras redes comerciales y de organismos estatales americanos y europeos, se constituyó así en la "columna vertebral" (*backbone)* de Internet a principios de los noventa[5].

Como se ve, en aquellos tiempos, a pesar de la gran evolución desde el punto de vista técnico informático, estas redes aún no eran comercialmente atractivas para el público en general, pues se utilizaban con fines administrativos, militares, educativos, o de investigación científica. Sin embargo, en el año 1991, el programador británico Tim Berners Lee definió una serie de reglas que hacen posible que todos los documentos incluidos en las distintas redes estén unidos en el ciberespacio, creando "HTML"[6] (*HyperText Markups Language*), que es el lenguaje de programa-

[4] Internet es la contracción de "*interconnected networks*", que significa redes interconectadas.
[5] Cfr. TRIGO ARANDA, Vicente; "Historia y evolución de Internet", publicado en página web de Autores Científico-Técnicos y Académicos (ACTA), http://www.acta.es, consultado: 09/09/2010.
[6] Según Trigo Aranda, HTML (*Hyper Text Markup Language* o Lenguaje de Marcado de Hipertexto) es el lenguaje de programación informático en el que se elaboran los sitios web. Asimismo, cuando hablamos de hipertexto, nos referimos a un texto con enlaces, es decir, referencias a otras partes del documento o a otros documentos. Hipermedio es una extensión del hipertexto, que permite incluir en los documentos

ción en que se escriben las páginas web[7]. Nace de esta forma la Gran Red Mundial (*World Wide Web*), formada por grandes servidores que almacenan documentos con extensión HTML, que permiten la combinación de texto con imágenes y videos, además de establecer vínculos (*links*) dentro y entre páginas web. Sin dudas que este hecho resultó trascendental, pues las posibilidades de la nueva Gran Red eran muy amplias, atractivas para el público en general, y redituables desde su explotación comercial por los proveedores de contenido.

Desde ese momento, Internet no ha parado de crecer, no sólo en cuanto a cantidad de servidores y recursos de infraestructura, sino principalmente desde su número de usuarios, que ha registrado un crecimiento exponencial a niveles inimaginables. Para graficar las palabras anteriores, un dato que es elocuente: al año 2010, aunque las estadísticas no son pacíficas, se calculan entre 1400[8] y 2000[9] millones de usuarios. En América Latina, la cifra de usuarios ronda los 187 millones de usuarios; y, finalmente, en Argentina, la cifra se acerca a los 20 millones de usuarios, con una penetración de casi la mitad de su población[10].

3. CONTEXTO ACTUAL

En este punto se intentará dar un sucinto panorama acerca de los principales lineamientos fácticos y jurídicos en los que desarrolla Internet en la actualidad. Para tal fin se tratarán brevemente el tema de la Sociedad de la Información, su recepción en diversos instrumentos internacionales, y, finalmente, los caracteres y el rol del derecho dentro de la misma.

3.1. LA LLAMADA "SOCIEDAD DE LA INFORMACIÓN". LA CMSI Y EL FGI

audio, video, imágenes, animaciones, mapas, entre otros medios. Por último, hay muchos otros lenguajes de programación (por ejemplo: JAVA, FLASH, MACROMEDIA) que en combinación con HTML hacen que las páginas de Internet sean más eficiente, rápidas y llamativas.

[7] Cfr. TRIGO ARANDA, Vicente, *ob. cit.*

[8] Según una estimación de Matthew Gray del Instituto de Tecnología de Massachusetts (MIT), publicada como "Growth and Usage of the Web and the Internet" en http://www.mit.edu, consultado: 09/09/2010.

[9] Según una estadística de la Internet Society publicada como "World Internet Users and Population Stats" en http://www.internetworldstats.com/stats.htm, consultado: 09/09/2010.

[10] http://www.internetworldstats.com/stats10.htm, consultado: 09/09/2010.

Internet como paradigma de las nuevas tecnologías de la información y las comunicaciones (TIC), ha transformado la vida de las personas, las sociedades y las economías en los últimos tiempos, dando lugar a la llamada "Sociedad de la Información". Se entiende por tal a *"una sociedad en la cual la creación, distribución y manipulación de la información forman parte importante de las actividades culturales y económicas"*[11].

Respecto de este concepto, cabe formular tres aclaraciones.

- En principio, esta noción presupone que los medios de generación de riqueza paulatinamente se han trasladado de los sectores industriales (o de productos tangibles) a los sectores de servicios e informáticos, y a su vez se reconoce con ello una profunda modificación en las estructuras socioeconómicas que caracterizaban a las sociedades modernas o industriales.

- En segundo lugar, si bien la sociedad de la información no se refiere exclusivamente a Internet en particular sino a las TIC en general, debe destacarse que éste ha desempeñado un papel muy importante como medio que facilita el acceso e intercambio de información y datos. En este orden de ideas, Internet ha revolucionado en la difusión del conocimiento; gracias a la red, millones de personas tienen fácil e inmediato acceso a una cantidad extensa y diversa de información.

- Por último, resta aclarar que en una sociedad informatizada, la propiedad de las nuevas tecnologías se erige como un nuevo factor de estratificación social, dando lugar a la llamada "brecha digital", que separa a aquellos sujetos, ya sean estados o personas, que utilizan las TIC como una parte rutinaria de su vida y aquellos que no tienen acceso a las mismas (brecha digital tecnológica) y que aunque las tengan no saben cómo utilizarlas (brecha digital educacional)[12].

Como se ve, el concepto de Sociedad de la Información es el que más se ajusta a una descripción de la sociedad posmoderna altamente informatizada de nuestros tiempos, y ha sido esbozado no sólo por distintos autores[13], sino que también

[11] OLIVERA, Noemí L., "Reflexiones en torno al sistema jurídico de la Sociedad de la Información", publicado en: www.abeledoperrot.com, consultado: 09/09/2010.
[12] Cfr. OLIVERA, Noemí L., *ob. cit.*
[13] Según Olivera, el pionero fue el sociólogo japonés Yoneji Masuda, quien ya en 1984 anticipaba el concepto de Sociedad de la Información como una "*Sociedad que crece y se desarrolla alrededor de la información y aporta un florecimiento general de la creatividad intelectual humana, en lugar de un aumento del consumo material*".

tuvo recepción en distintos instrumentos internacionales resultantes de las dos ediciones de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), convocadas por la Organización de Naciones Unidas a través de la Unión Internacional de Telecomunicaciones en 2003 (Ginebra[14]) y 2005 (Túnez[15]). Respecto de él, la UIT, en su página web, nos da el siguiente panorama:

"El mundo moderno está experimentando una transformación fundamental a medida que la sociedad industrial que marcó el siglo XX deriva a gran velocidad hacia la Sociedad de la Información del siglo XXI. Este proceso dinámico anuncia un cambio fundamental en todos los aspectos de nuestras vidas, incluyendo la difusión de los conocimientos, el comportamiento social, las prácticas económicas y empresariales, el compromiso político, los medios de comunicación, la educación y la salud, el ocio y el entretenimiento. Nos encontramos sin duda en medio de una gran revolución, tal vez la mayor que la humanidad haya experimentado. Con el fin de poder beneficiar a toda la comunidad, el crecimiento exitoso y continuo de esta nueva dinámica requiere una discusión a nivel mundial"[16]

En esta tesitura se pronuncian los distintos objetivos de la primera edición de la CMSI, los cuales pueden sintetizarse en el primero de ellos:

"*Nosotros, los representantes de los pueblos del mundo, reunidos en Ginebra del 10 al 12 de diciembre de 2003 con motivo de la primera fase de la Cumbre Mundial sobre la Sociedad de la Información, declaramos nuestro deseo y compromiso comunes de construir una Sociedad de la Información centrada en la persona, integradora y*

Asimismo, otros autores como Peter Drucker o Robin Mansel prefieren utilizar el término "Sociedad del Conocimiento" (*Knowledge Society*).

[14] El objetivo de la primera fase era redactar y propiciar una clara declaración de voluntad política, y tomar medidas concretas para preparar los fundamentos de la Sociedad de la Información para todos, que tenga en cuenta los distintos intereses en juego.
A la Fase de Ginebra de la CMSI asistieron cerca de 50 jefes de Estado o Gobierno y Vicepresidentes, 82 Ministros y 26 Viceministros de 175 países, así como representantes de organizaciones internacionales, el sector privado y la sociedad civil, que proporcionaron apoyo político a la Declaración de Principios de Ginebra y el Plan de Acción de Ginebra, que se aprobaron el 12 de diciembre de 2003. Más de 11000 participantes de 175 países asistieron a la Cumbre y a los eventos conexos.

[15] El objetivo de la segunda fase fue poner en marcha el Plan de Acción de Ginebra y hallar soluciones y alcanzar acuerdos en los campos de gobierno de Internet, mecanismos de financiación y el seguimiento y la aplicación de los documentos de Ginebra y Túnez.
A la Fase de Túnez de la CMSI asistieron cerca de 50 jefes de Estado o Gobierno y Vicepresidentes y 197 Ministros, Viceministros y Subsecretarios de 174 países, así como representantes de organizaciones internacionales, el sector privado y la sociedad civil, que proporcionaron apoyo político al Compromiso de Túnez y al Programa de Acciones de Túnez para la Sociedad de la Información, que se aprobaron el 18 de noviembre de 2005. Más de 19000 participantes de 174 países asistieron a la Cumbre y a los eventos conexos.

[16] http://www.itu.int/wsis/basic/about-es.html, consultado: 09/09/2010.

orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento, para que las personas, las comunidades y los pueblos puedan emplear plenamente sus posibilidades en la promoción de su desarrollo sostenible y en la mejora de su calidad de vida, sobre la base de los propósitos y principios de la Carta de las Naciones Unidas y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos."

En lo que respecta a la Internet, la segunda edición de la CSMI, se refiere de la siguiente manera:

"Internet se ha convertido en un recurso global disponible para el público, y su gestión debe ser una de las cuestiones esenciales del programa de la Sociedad de la Información. La gestión internacional de Internet debe ser multilateral, transparente y democrática, y contar con la plena participación de los gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales. Esta gestión debería garantizar la distribución equitativa de recursos, facilitar el acceso a todos y garantizar un funcionamiento estable y seguro de Internet, teniendo en cuenta el plurilingüismo."

Asimismo, en Túnez también se propuso un "gobierno internacional de Internet" en el marco de un proceso abierto e integrador que garantice un mecanismo para la participación plena y activa de los gobiernos, el sector privado y la sociedad civil de los países desarrollados y en desarrollo, con inclusión de las organizaciones y foros intergubernamentales e internacionales relevantes, a fin de investigar y formular propuestas de acción. Esto último, finalmente terminaría de concretarse a través del Foro para la Gobernanza de Internet (FGI).

A la fecha, se han realizado cuatro reuniones del FGI[17], en las cuales se ha debatido arduamente respecto de cómo debería ser la infraestructura lógica que gobierne la Internet. Según Alfonso[18], de estas reuniones han surgido dos opiniones totalmente opuestas: por un lado, una postura "privatista", conformada por aquellos que insisten en que si hay algo que es necesario arreglar, esto puede hacerse

[17] La Primera reunión del IGF, se celebró del 30 de octubre al 2 de noviembre de 2006 en Atenas, Grecia. La Segunda del 12-15 de noviembre de 2007 en Río de Janeiro, Brasil. La Tercera del 3-6 de diciembre de 2008 en Hyderabad, India. Y finalmente, la Cuarta del 15-18 de noviembre de 2009 en Sharm El Sheikh, Egipto.

[18] Cfr. ALFONSO, Carlos A.; "Gobernanza de Internet. Un Análisis en el Contexto de la CMSI", publicado en: http://wsispapers.choike.org//papers/esp/carlos_gobernanza_internet.pdf, Julio de 2005, consultado: 09/09/2010.

dentro de la estructura actual de la Corporación de Internet para la Asignación de Nombres y Números (*Internet Corporation for Assigned Names and Numbers*; ICANN en inglés). En el extremo opuesto, hay representantes de algunos países (no necesariamente miembros del FGI) que son partidarios de que se transfieran todas las funciones de la ICANN a la Unión Internacional de Telecomunicaciones (UIT). Refuerza esta postura "publicista" el hecho de que la UIT patrocinó al FGI.

Sin embargo, la discusión no sólo se limitó a los aspectos técnicos, y, entre otros temas que hacen a la problemática de Internet, se han debatido los siguientes: costos de conexión entre países; ciberseguridad y ciberdelito (incluyendo *spam*, *phishing* y otros tipos de delitos o acciones socialmente perjudiciales vía Internet); libertad de expresión; patentes, derechos de autor y marcas comerciales (derechos de propiedad intelectual); protección de datos y privacidad; derechos de los usuarios; y muchos otros[19].

3.2. EL DERECHO EN LA SOCIEDAD DE LA INFORMACIÓN

Más allá de estos antecedentes, que por supuesto son importantes por valer como declaraciones de voluntad política de los distintos gobiernos de los Estados que conforman la UIT para regular la Internet, cabe preguntarse por las características del derecho en la Sociedad de la Información, y cuál es el rol que debe cumplir en la reglamentación de la red de redes.

En relación al primer interrogante, es posible hablar de un fenómeno de globalización jurídica[20], en virtud del cual el derecho se encuentra sujeto a permanentes cambios en la forma de crear e interpretar las normas. Esto ocurre, a su vez, como consecuencia de sustanciales modificaciones en materia social y económica – materias respecto de las cuales el derecho siempre se encuentra un paso atrás – y que se inscriben en el mismo proceso o conjunto de procesos a los que se agrupa bajo el nombre de "globalización".

[19] Para mayor profundidad, consultar el artículo citado de Carlos Alfonso.
[20] Según la terminología usada por Ernesto Grün en "Una visión sistémica y cibernética del derecho en el mundo globalizado del siglo XXI", Ed. Lexis Nexis, 2005, p. 83 y ss.

Asimismo, debe aclararse que este proceso de globalización del derecho, aún se encuentra en formación, y por ende muchas de las instituciones que se crean para dar respuesta a los permanentes cambios, no pueden ser categóricamente definidas en cuanto a su alcance. Ejemplo de esto último lo vemos en materia de registro de nombres de dominio, donde se crean normas técnicas de fuente supranacional no estatales (pues no son dictadas por legisladores o jueces sino por quienes entienden cómo funciona el ciberespacio: vgr. normas del ICANN), y de las cuales se duda respecto de su juridicidad, y con mayor razón de su aplicación por órganos jurisdiccionales.

En lo que respecta a las características del derecho del mundo globalizado, Grün[21] advierte la aparición de algunos nuevos y aún rudimentarios sistemas jurídicos, que se diferencian de los tradicionales sistemas nacionales e internacionales del siglo XX que habitualmente se conocen en las prácticas y teorías jurídicas. Según el autor, estos nuevos sistemas son los siguientes:

– Por un lado, la *lex mercatoria,* que incluye un conjunto de prácticas, usos y costumbres internacionales que resultan del incremento del comercio a nivel global, y que presenta propios y novedosos lineamientos, problemáticas y mecanismos.

– Por otro lado, el autor se refiere a un nuevo sistema jurídico que todavía se encuentra en el límite entre la realidad y la ciencia ficción: las normas aplicables a los "robots".

– Por último, se destaca la aparición del derecho de Internet, o también llamado *ius retis,* al cual se hará referencia a continuación, intentando resolver el segundo interrogante.

De esta manera, para contestar a la cuestión relativa al rol del derecho en la regulación de Internet, resulta indispensable considerar los límites del mismo. Es decir, debemos destacar que, el contexto actual de proliferación de actores multinacionales, ya sean compañías globales o entidades supranacionales conformadas por un bloque de países que ceden soberanía, y el consecuente debilitamiento de los Estados-Nación como unidades efectivas y monopólicas de poder, nos lleva a afirmar que el derecho estatal se encuentra en crisis, y con él, la ley interna como

[21] GRÜN, Ernesto, *Ob. cit.*, p.105 y ss.

única fuente admitida[22]. Es decir, si bien la ley nacional sigue siendo la principal fuente utilizada para la resolución de algunos de los problemas de Internet (vgr. amplitud de la libertad de expresión, delitos informáticos, etc.), el carácter internacional y descentralizado de la red la convierte en insuficiente.

Pero esta crisis de legalidad no necesariamente afecta al derecho en sí mismo, que tiene diversas fuentes, o sea otros mecanismos distintos a la ley para la regulación de la Internet, a saber: tratados internacionales en materia de derechos de autor, normas técnicas dictadas por los órganos que forman la infraestructura de la red en materia de registro de nombres de dominio, *lex mercatoria* en el ámbito del comercio electrónico, costumbres internacionales, entre otras soluciones.

4. NATURALEZA JURÍDICA

Se discute acerca de la naturaleza jurídica de Internet:

A) Internet no es un medio de comunicación: esta postura es sostenida por Wolton y por Barber, quienes llegan a la misma conclusión pero con distintos argumentos.

Según Wolton, citado por Crovi Druetta[23], *"Internet no es un medio de comunicación, debido a que no es un medio generalista sino un medio temático. Un medio de comunicación descansa en tres dimensiones: tecnológica, profesional y comercial. En pocas palabras, el medio de comunicación nace de una oferta construida por profesionales, que utiliza un sistema tecnológico para encontrar un público. Internet, sistema de información automatizado interactivo, obtiene su fuerza del hecho de no ser un medio de comunicación: se trata de mensajes en todos los sentidos, enviados por cualquiera, captados por cualquiera y organizados por nadie".*

De estas palabras, se concluye que Wolton no pone en tela de juicio las dimensiones tecnológica y comercial de Internet, pero en cambio, duda de la profe-

[22] Cfr. VIBES, Federico; "¿Qué ley gobierna Internet?". Publicado en www.abeledoperrot.com.ar, consultado: 09/09/2010.
[23] Cfr. CROVI DRUETTA, Delia María; "¿Es Internet un medio de comunicación?". Revista Digital Universitaria [en línea]. 10 de junio 2006, Vol. 7, No. 6. Publicado en: http://www.revista.unam.mx/vol.7/num6/art46/int46.htm, consultado: 09/09/2010.

sional, razón por la cual falta un elemento tipificante del concepto de medio de comunicación.

En otro orden de ideas, Barber[24] opina que Internet no llega a ser un medio masivo de comunicación, sino que sólo es un medio de transporte de la información, en cuanto permite transmitir datos e información mediante un método de interconexión de redes de computadoras, que hace que todas ellas funcionen como una red única. En este sentido, se compara a la Internet, por su estructura y forma de funcionar, con la telefonía, pues el usuario, a través de su ordenador (emisor) se conecta con el proveedor de servicio de Internet (destinatario final del paquete de información, vale decir, el mensaje) de manera directa e interpersonal. De esta forma, Internet sería, por su arquitectura tecnológica, un medio horizontal (interpersonal) y no un medio vertical (dirigido a las masas). En este sentido, "*Internet es punto a punto como el teléfono; no nos engancha a un líder, editor, o emisión. Nos engancha unos a otros*"[25].

B) Internet es un medio de comunicación: según Crovi Druetta, la lectura que hace la postura anterior respecto de la naturaleza de Internet resulta parcial, debido a que "*no toma en cuenta que junto con este sistema que envía mensajes en todos los sentidos y que son captados por cualquiera, convive otro, perfectamente estructurado, que es el de los grandes medios en sus versiones digitales, así como sitios y portales que responden a una oferta construida por profesionales*"[26]. Vale decir, la mentada falta de profesionalismo en la elaboración del contenido de Internet es solamente parcial si se tiene en cuenta que en la red pueden encontrarse sitios altamente profesionalizados; inclusive igual o más que los medios tradicionales.

Así, la autora concluye que "*Internet es un medio de comunicación complejo y diferente a sus antecesores. Tiene la particularidad y capacidad de combinar dos funciones básicas: ser un canal de distribución para los medios tradicionales (generalista),*

[24] Cfr. BARBER, Benjamin R.; "¿Hasta qué punto son democráticas las nuevas tecnologías de telecomunicación?". En BARBER, Benjamín R. y otros, Internet, Derecho y Política, Editorial UOC, 2009, p. 17.
[25] BARBER, Benjamin R, *ob. cit.*, p. 23.
[26] CROVI DRUETTA, Delia María, *ob. cit.*

y proporcionar un espacio de expresión para emisores emergentes de diversa índole (temáticos o no)"[27].

A esto agregamos que la presencia de Internet en todo el mundo lo convierte en un medio masivo de comunicación, pues, más allá de que su estructura técnica y la dinámica interactiva que plantea muchos de sus servicios no se ajusten estrictamente a la definición tradicional de "*mass media*"[28], en esencia se da una relación entre un emisor único y un receptor heterogéneo, indeterminado y masivo a nivel global.

Siguiendo esta misma tesitura - que por cierto compartimos - Fernández Delpech afirma que *"Internet es un medio de acceso a la información que permite a los diversos actores interactuar con diversos fines"*[29]. Con ello, se alude a Internet como medio de transporte de información y medio de comunicación al mismo tiempo. Como medio de información, es el centro de documentación más grande y completo del mundo; a través de la red se accede sencilla y libremente a una cantidad extensa y diversa de información sin límites geográficos, fronteras, ni jurisdicción alguna que regule su contenido. Además, es un medio de comunicación porque los usuarios pueden usar la red como instrumento de realización del proceso comunicacional entre un emisor y un receptor, ya sea éste determinado (del mismo modo que la carta, el teléfono fijo o móvil, o el fax) o indeterminado (del mismo modo que la radio, el cine o la televisión).

La distinción no es meramente teórica y/o solamente útil a los fines académicos. Por el contrario, la doctrina a la que se adhiera tendrá repercusión en el régimen jurídico aplicable. Por ejemplo, en materia de aplicación de la ley de defensa del consumidor a los proveedores de contenido, en la mayor o menor intervención que el Estado pueda hacer a través de la regulación administrativa, la aplicabilidad de las normas constitucionales y/o legales que protegen la libertad de prensa y el derecho a la información, la posibilidad de aplicar un factor de atribución objetivo en caso de

[27] CROVI DRUETTA, Delia María, *ob. cit.*
[28] Entendemos que por medio masivo de comunicación debe entenderse a todos los medios de comunicación recibidos simultáneamente por una gran audiencia, equivalente al concepto sociológico de masa (por masa debemos entender a un grupo numeroso de personas que cumpla simultáneamente con tres condiciones: ser grande, ser heterogéneo y ser anónimo).
[29] FERNANDEZ DELPECH, Horacio, *ob. cit.*, p. 15.

noticias inexactas o agraviantes, la posibilidad de censurar previamente el contenido ilícito o nocivo, la posibilidad de otorgar derecho a réplica, etc.

En Argentina, la cuestión de la naturaleza jurídica de Internet, parecería estar resuelta con el decreto 1279/97[30]. En esta disposición del Poder Ejecutivo Nacional se declara que 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. Asimismo, entre los considerandos, se deja claro que "*el servicio de Internet es otro medio moderno que resulta plenamente apto para la difusión masiva de las ideas tanto para darlas a conocer como para recibirlas en beneficio del conocimiento del hombre*" y que "*dada la vastedad y heterogeneidad de los contenidos del servicio de Internet es posible inferir que el mismo se encuentra comprendido dentro del actual concepto de prensa escrita, el cual no se encuentra sujeto a restricción ni censura previa alguna*".

Sin dudas que este decreto reviste vital importancia, pues implica la extensión de la garantía constitucional que ampara la libertad de expresión de los medios de comunicación a la Internet. En este sentido, resultan de aplicación los arts. 14, 32 y 42 de la Constitución Nacional, así como el Pacto San José de Costa Rica, la jurisprudencia de la Corte Suprema de los EEUU, y la de nuestro Alto Tribunal.

5. POSTURAS RELATIVAS A LA CONVENIENCIA DE SU REGULACIÓN

En relación al tema de la regulación de Internet existen básicamente dos posturas, a saber: A) Internet no debe regularse; B) Internet debe regularse.

A) La "no regulación": desde una primera posición – que podría llamarse anarquista[31] – se sostiene que la inexistencia de límites geográficos en Internet impide todo tipo de regulación, pues nadie tiene soberanía para arrogarse tal potestad. En este sentido, se concluye que en Internet no hay posibilidad de regulación, puesto a que se trata de un espacio que excede a la jurisdicción de cualquier Estado[32].

[30] *B.O.*, 1/XII/1997.
[31] Según la terminología usada por Ernesto Grün, *Ob. cit.*, p. 111.
[32] Cfr. VIBES, Federico P., *ob. cit*, párrafo IV.

El gran exponente de esta postura es el norteamericano John Perry Barlow, autor de la famosa "Declaración de Independencia del Ciberespacio"[33], en la que, entre otras cosas, se dejó establecido lo siguiente:

"Gobiernos del mundo industrial, fatigado gigante de carne y acero, yo vengo del ciberespacio, el nuevo hogar de la mente. En nombre del futuro, les pido que nos dejen solos. Ustedes no son bienvenidos entre nosotros. Ustedes no ejercen soberanía alguna en el lugar por el cual transitamos.

No hemos elegido ningún gobierno, ni pretendemos tenerlo, así que me dirijo a ustedes sin más autoridad que aquella con la cual la libertad siempre habla [...]

[...] Sus conceptos legales sobre propiedad, expresión, identidad, movimiento y contexto no se aplican a nosotros. Ellos se basan en la materia. Aquí no hay materia. Nuestras identidades no tienen cuerpo, así que, a diferencia de ustedes, no podemos obtener orden por coacción física. Confiamos en que de la ética, del propio interés y del bien común, emergerá nuestro gobierno [...]"[34].

Esta lírica declaración de Barlow tiene el valor de constituir una reivindicación de las libertades en el ciberespacio, manifestándose abiertamente en contra de las interferencias de los poderes políticos que afectan al mundo de Internet.

Sin embargo, se pueden formular dos críticas al texto: por un lado, que Internet nunca careció absolutamente de regulación, pues la red, desde su misma génesis, siempre estuvo sujeta a diversas normas éticas y técnicas; por otro lado, al decir de Grün, *"evidentemente esta posición es ingenua, pues cualquier grupo humano integrado por un importante número de personas necesita algo más que normas éticas para regular sus relaciones"*[35].

B) La regulación de Internet: según Castro Bonilla[36], bajo esta segunda tesitura, se enrolan aquellos que piensan que Internet es un espacio social, y como tal debe necesariamente ser regulado por el derecho. Se sostiene como principal argumento el hecho de que no existe diferencia alguna entre las actividades que se

[33] Este documento fue publicado online el 8 de febrero de 1996 por John Perry Barlow, fundador de la *Electronic Frontier Foundation* (EFF), como respuesta a la sanción de la reforma a la Ley de Telecomunicaciones en EEUU en el año 1996.

[34] Puede consultarse el texto completo en su idioma de origen (inglés) en: http://www.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration, consultado: 09/09/2010.

[35] GRÜN, *Ob. cit.*, p. 112.

[36] Cfr. CASTRO BONILLA, Alejandra, "La regulación de Internet: un reto jurídico", publicado en http://www.uned.ac.cr/redti/documentos/regulacion.pdf, consultado: 09/09/2010.

llevan a cabo en la red y las que se desarrollan en el mundo real. En consecuencia – se concluye – el derecho del mundo real resulta completamente aplicable al mundo virtual, y por ende, no se requieren nuevas interpretaciones sobre nuevos derechos, sino simplemente concreciones en el ámbito informático con respecto a derechos ya existentes.

A su vez, dentro de esta postura, se discute respecto de quién debería ejercer el control de Internet, arrojando dos posiciones:

a) "Alguien" debe regular Internet: se concibe la idea de que sea "algún" sujeto el que dicte normas para regular la actividad en la red. Ese sujeto puede ser, o bien Estados que impongan decisiones en virtud de su soberanía, o bien bloques supranacionales conformados por Estados soberanos. Asimismo, también se plantea la posibilidad de crear un ente único compuesto por instancias públicas e internacionales, dotado de competencias universales.

b) "Autorregulación": Internet debe "autorregularse" por normas no jurídicas impuestas por sus propios partícipes. Está basada en la idea neoliberal de que la autorregulación de la red es equivalente a las reglas del mercado, por ende libre y basada en la competencia.

Es así que - se concluye - la regulación debe hacerse por organizaciones privadas conformadas por cualquier prestador o grupo de prestadores de servicios o bien usuarios de Internet. Entre los sujetos de naturaleza privada se destacan distintas organizaciones de tipo no gubernamental que, si bien no dictan normas jurídicas, están a cargo de distintos aspectos técnicos y de infraestructura de la red, a saber: ICANN[37], ISOC[38], IAB, IETF, IESG[39], IRTF[40], entre otras.

[37] La *Internet Corporation for Assigned Names and Numbers* es la organización responsable de asignar las direcciones del protocolo IP, de los identificadores de protocolo, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores. Reemplazó a la *Internet Assigned Numbers Authority* (IANA).

[38] La *Internet Society* es un órgano de coordinación que administra los recursos comunes y marca la dirección que ha de seguir la red para hacer frente a los retos impuestos por su crecimiento y la constante evolución tecnológica.

[39] La *Internet Architecture Board,* la *Internet Engineering Task Force* y el *Internet Engineering Steering Group* son órganos a través de los cuales la ISOC ejerce sus funciones, y se encargan de la supervisión y aprobación de normas, de la especificación de estándares, y de la coordinación en general respectivamente.

[40] *Internet Research Task Force* es un órgano cuya principal misión es promover la investigación de la importancia de la evolución de futuro de Internet, y sobre los asuntos relacionados con los protocolos, los usos, la arquitectura y la tecnología de Internet.

No dudamos en enrolarnos en esta segunda postura, pues entendemos que todo lo que es regulable fuera del mundo virtual lo es también a nivel del ciberespacio. Creemos que el espacio virtual que abre Internet es un espacio social, y como tal debe necesariamente ser regulado por el derecho. No es cierto que Internet sea "tierra de nadie", como sostiene la tesis anterior, ni que sería imposible regularlo, so pretexto de que las leyes alteran su esencia o impiden su progreso.

Lo que sí deben reconocerse son ciertas dificultades fácticas – relacionadas con la estructura técnica y global de Internet - que obstan a una regulación óptima. Es por ello que, hoy en día resulta excesivo exigir al derecho que dé soluciones totalmente satisfactorias. Lo que sí podrá exigírsele son mejores soluciones que las existentes, para lo cual sería necesario que los institutos jurídicos tradiciones se ajusten a esta nueva problemática, y que otros nuevos se implementen a fin de brindar soluciones a una realidad tan cambiante.

Finalmente, respecto de quién debería regular el ciberespacio, entendemos que ambas posiciones son plenamente compatibles, pues creemos que todas aquellas cuestiones relacionadas con materias extrajurídicas efectivamente debieran ser reguladas por organizaciones privadas – vgr. ICANN – y que aquellas cuestiones estrictamente jurídicas deben ser de competencia de los Estados, ya sea a través de normas internas, convencionales o comunitarias. Inclusive, para un futuro sería interesante proponer la creación de un organismo de regulación de Internet con competencias universales para aquellas cuestiones que sean de difícil o imposible regulación a nivel territorial estatal.

CAPÍTULO II

INTERNET Y EL DERECHO A LA LIBERTAD DE EXPRESIÓN

Antes de comenzar a analizar en profundidad el tema de la intimidad, preciso es referirnos, aunque sea en pocas líneas, a una problemática estrechamente relacionada: el derecho a la libertad de expresión en Internet.

En el presente capitulo se considerará especialmente cómo influye el fenómeno de Internet en el concepto y la esencia misma de la libertad de expresión.

Cabe advertir que, se pondrá atención en las libertades de contenido y de uso en Internet, la situación de la legislación y la jurisprudencia nacional en relación al tema, y, finalmente, la responsabilidad ulterior que surge del ejercicio abusivo de tales libertades, cuando se afectan otros derechos de igual o mayor jerarquía, entre los que se incluye al derecho a la intimidad.

1. LA LIBERTAD DE EXPRESIÓN

Se ha definido a la libertad de expresión como *"el derecho a hacer público, a transmitir, a difundir y a exteriorizar un conjunto de ideas, informaciones, opiniones, críticas y/o creencias, a través de cualquier medio: oralmente, mediante símbolos y gestos y/o en forma escrita"* [1].

A partir de este concepto, amplio y comprensivo de los distintos supuestos que admite este derecho, el objeto del mismo, y el medio o canal por el cual se exterioriza el objeto, se admiten diversas interpretaciones, dependiendo del momento histórico en que se hagan.

Si tenemos en cuenta el contexto en el cual tuvo su génesis, vale decir, fines del siglo XVII y principios del XIX, se advierte que la libertad de expresión como ins-

[1] BIDART CAMPOS, Germán J., "Manual de la Constitución Reformada", Editorial Ediar, Buenos Aires, 1996, Tomo II, pág. 12.

trumento indispensable para la configuración de la sociedad liberal se circunscribía a la prensa escrita, una prensa verdaderamente independiente del Estado y de las presiones económicas, basada en opiniones individuales más que en la divulgación de noticias e informaciones. No había llegado aún el tiempo en que el conocimiento de los hechos sea relevante para la sociedad, pues ésta última tenía escasa o nula participación en la prensa, la cual se hallaba restringida a una reducida clase intelectual y política dominante[2].

Ahora bien, si tal interpretación es hecha durante las primeras décadas del siglo XX, advertimos una profunda transformación en el concepto y en la función de los medios de comunicación, y en el alcance del derecho a la libertad de expresión. Desde ese entonces, se comienza a vislumbrar un proceso de cambio de un sistema de prensa de opinión a un sistema de prensa comercial.

Este último, se identifica principalmente por el reemplazo de un periodismo no profesional por grandes empresas periodísticas con un enorme poderío económico, menor espacio para la opinión y mayor espacio para la información, el monopolio u oligopolio en el manejo de la misma, la necesidad de la inmediatez en la noticia, la despersonalización de la información, la paradoja de un aumento de interés por la cosa pública y al mismo tiempo un menor acceso a los medios para opinar de ella, la rentabilidad a obtener de la publicidad como disparador de una prensa sensacionalista y alejada de la verdadera función periodística, entre otras características relevantes[3].

En base a lo descripto, se puede concluir que la garantía de libertad de expresión es más amplia durante esta segunda etapa, e incluye no solamente la libre opinión sin censura previa, sino también el derecho a la información, el cual, a su vez, comprende una faz activa, reservada al emisor, y una faz pasiva, que consiste en el derecho de los destinatarios/consumidores a estar informados. Asimismo, comprende otros derechos íntimamente relacionados como el de réplica, el de libertad de contenido en los mensajes publicitarios, el de libertad de empresa perio-

[2] Cfr. PIZARRO, Ramón Daniel, "Responsabilidad civil de los medios masivos de comunicación. Daños por noticias inexactas o agraviantes.", Editorial Hammurabi, Buenos Aires, 1999, pág. 41 a 43.
[3] Para un análisis profundo del sistema de prensa comercial, consultar: PIZARRO, Ramón Daniel, *ob. cit.*, p. 53 a 69.

dística, el del periodista profesional a no revelar las fuentes, los derechos del protagonista de informaciones inexactas, entre otros.

Finalmente, nuestro análisis no estaría completo si no se propusiera una interpretación de la garantía de libertad de expresión en los tiempos actuales. A continuación, se intentará efectuar una relectura de dicho concepto desde el advenimiento de Internet, y cómo se manifiesta en la red de redes.

1.1. PERSPECTIVA ACTUAL DESDE EL FENÓMENO DE INTERNET

Hoy en día, no sólo la libertad de expresión, sino las libertades públicas en general adquieren una dimensión totalmente novedosa, imposible de imaginar al momento de su concepción. En la hora actual, a causa de los avances en las TICs, y especialmente desde la aparición del fenómeno de Internet, parecerían haberse eliminado algunas barreras que las limitaban[4] (por ejemplo el derecho a la educación encuentra una nueva herramienta para llegar a millones de personas a las que antes no llegaba; y la libertad de reunión, encuentra una nueva forma: la reunión "virtual", sin ningún tipo de condición en cuanto al tiempo y al espacio).

Sin embargo, esas limitaciones siguen existiendo en el ejercicio de las libertades, y en especial en la de expresión. Los medios de comunicación, así, resultan soportes muy restrictivos para la libertad de expresión desde su faz "universal", entendiendo por ello a la efectiva participación de los ciudadanos en el proceso comunicacional-informativo, ya que siempre estuvo reservada a una pequeña elite con suficiente capacidad económica para poner en funcionamiento una empresa periodística[5].

El advenimiento de Internet, y la consecuente facilidad de los usuarios para confeccionar una página web con un contenido "sin filtro", sin embargo, parecerían haber influido en la cuestión, permitiendo que las opiniones de quienes no tenían lugar en los medios tradicionales sean escuchadas o leídas. De esta forma, no sólo

[4] Cfr. SANCHEZ FERRIZ, Remedio, "Las libertades públicas y su ejercicio en Internet". En COTINO HUESO, Lorenzo (coord.) y otros, "Libertad en Internet. La red y las libertades de expresión e información", Editorial Tirant Lo Blanch, Valencia, 2007, págs. 76 y 77.
[5] Cfr. SANCHEZ FERRIZ, Remedio, *ob. cit.* En COTINO HUESO, Lorenzo (coord.) y otros, *ob. cit*., págs. 78 a 82.

aumenta la cantidad de información u opiniones, sino la calidad de las mismas, al poder el usuario obtener material más especializado, evitando la simplificación propia de los medios audiovisuales, que tienden a no reflejar la complejidad de la realidad, pues es parte del negocio llegar a un público más numeroso.

Asimismo, debe advertirse que la Internet, si bien amplió considerablemente el espectro de opiniones e informaciones, no deja de plantear los mismos riesgos de concentración en el manejo de la información que los medios audiovisuales[6], como así otros problemas, a saber: la internacionalidad de la red excede la posibilidad de regulación nacional; la veracidad de las informaciones se ve puesta más que nunca en tela de juicio; el régimen de responsabilidad se ve con la dificultad de determinar cuál es el emisor sobre quién debe recaer la misma, pues son varios los intervinientes en la difusión a través de la red; el régimen jurídico aplicable a quien no es periodista, pero cumple las funciones de tal en un sitio web; la constitucionalidad de la aplicación de filtros a los contenidos inadecuados por el Estado; la afectación de otros derechos con jerarquía constitucional, entre otros.

En síntesis, la libertad de expresión en la era de Internet adquiere un nuevo significado: es ahora un derecho verdaderamente "universal", en cuanto a que permite un espacio en el que se oyen más voces y se leen otros puntos de vista, democratizando la información y las opiniones. Pero también deben advertirse algunos problemas que también afectan a los medios anteriores a su irrupción, y otros tantos más que surgen por su estructura y particularidades, y no registran precedentes en la historia.

1.2. LIBERTAD DE CONTENIDO Y LIBERTAD DE USO

Al decir de Molina Quiroga, "*como toda tecnología, Internet es una creación cultural que refleja los principios y valores de sus inventores, que también fueron sus primeros usuarios y experimentadores. Los valores libertarios de quienes crearon y desarrollaron Internet determinaron una arquitectura abierta y de difícil control. Al*

[6] Es así que los sitios más visitados en materia de información y noticias por los usuarios argentinos son las ediciones digitales de los diarios El Clarín y La Nación. (http://www.alexa.com/topsites/countries/AR, consultado 09/09/10).

mismo tiempo, cuando la sociedad se dio cuenta de la extraordinaria capacidad que representa Internet en relación al ejercicio de la libertad de expresión, los principios inherentes a la red se difundieron ampliamente, sobre todo en las generaciones jóvenes y avezadas en materia informática, para quienes Internet y libertad son conceptos correlativos e inescindibles"[7].

Ahora bien, cabe preguntarse: ¿cómo se manifiesta la libertad de expresión en Internet? Para contestar este interrogante, debe hacerse una distinción a partir de una analogía: del mismo modo en que el derecho a la información, del cual nadie discute forma parte de la genérica "libertad de expresión", tiene una faz activa o de los medios a informar, y una faz pasiva o de los destinatarios a estar informados, pensamos que Internet, por sus particularidades, debería tener un principio análogo que comprenda una faz activa o de los proveedores de contenido a suministrar material de manera libre, como así también una faz pasiva o de los usuarios a acceder sin restricciones a esos contenidos. Es así que - concluimos - la libertad en la red adquiere dos formas de manifestarse: libertad de contenido y libertad de uso.

La primera de ellas, parece ser más sencilla de explicar, y sería aquella reservada a los proveedores de contenido, vale decir, a todo sujeto que suministra, administra y publica información en sitios o páginas web, con lo cual se incluye no sólo al titular registral del nombre de dominio, sino también a los administradores de foros de discusión y/o blogs[8]. En este sentido, se afirma que "*a través de Internet pueden transmitirse datos, documentos, imágenes y sonidos de diversa naturaleza o contenido, sean lícitos o ilícitos, morales o inmorales, permitidos o prohibidos, benignos o nocivos. Esta es una característica de la esencia de la red que, salvo excepciones muy reguladas y justificadas, no puede - y nunca debería - modificarse legalmente*"[9].

La libertad de uso, por otro lado, se refiere a los derechos de los usuarios a emplear todos servicios de Internet de manera libre, y sin restricciones a los conte-

[7] Cfr. MOLINA QUIROGA, Eduardo, "Internet y la libertad de expresión. A propósito de la ley 26032", JA 2005-III-865 - SJA 24/8/2005. Publicado en http://www.abeledoperrot.com.ar, consultado 09/09/10.

[8] Ambos son espacios dentro de un sitio web, propio o de un tercero, en los que se permite a los usuarios expresarse respecto de un tema propuesto por el administrador. En cuanto a las diferencias, los foros de discusión tienen por objeto permitir el debate de distintos temas, con el afán de buscar soluciones y tratar de llegar a una respuesta que resuelva el problema en cuestión; los blogs, por otro lado, se utilizan más para comunicar a una gran audiencia acontecimientos que van sucediendo cronológicamente, permitiendo a los usuarios introducir comentarios.

[9] JIJENA LEIVA, Renato Javier, "Contenidos de Internet: Censura o Libertad de Expresión", publicado en: http://www.mass.co.cl/acui/leyes-jijena2.html, consultado 09/09/10.

nidos de la red. Esto incluye no sólo el derecho a ingresar a todas las páginas o sitios web sin censura previa, sino también otros derechos, como lo son el de crear y opinar en foros de discusión o blogs, participar de redes sociales[10], enviar y recibir correos electrónicos[11], compartir archivos en redes entre pares (P2P), etc.

Este conjunto de libertades, a su vez presupone el derecho de acceso igualitario y universal a Internet, que se erige como un derecho distinto al de libertad de expresión, pues es un derecho difuso que debe considerarse como parte del derecho a la educación, del de acceso a la cultura, o en su caso del de igualdad de oportunidades en el acceso a las nuevas tecnologías[12]. Es así que, a pesar de existir una íntima vinculación entre ambos conceptos, no deben confundirse, pues el derecho de acceso a Internet es esencialmente distinto al derecho a la libertad de uso, al ser aquél una condición de existencia de éste.

Por último, otro de los presupuestos respecto de la libertad de uso es el derecho al anonimato en Internet, entendiendo por ello a "*la posibilidad de acceder a la red, y de usar sus servicios, sin necesidad de identificarse, ni ser controlado por ello, y sin que sea posible localizar o rastrear las actividades en línea*"[13]. Debe advertirse que, dado que la navegación en Internet no es inocua, sino que deja rastros que permiten la identificación del usuario, se explica que este "nuevo" derecho forme parte del derecho a la intimidad, del secreto de las comunicaciones, y también de la libertad de expresión, razón por la cual debe inferirse que se trata de un derecho con amparo constitucional[14].

[10] La red social por excelencia, Facebook, permite al usuario crear su propio perfil público, basado en ideas, opiniones y comentarios, e incluso "unirse" a grupos de usuarios en base a sus preferencias ideológicas, políticas, religiosas, etc. Si bien todo ello forma parte del derecho a la intimidad del sujeto, cuando éste decide hacerlo público, pasa a ser parte de la libertad de expresión.

[11] El correo electrónico, si bien constituye un espacio privado y reservado a la intimidad de la persona, también puede ser considerado un espacio público, en aquellos casos donde resulta un vehículo para transmitir documentos públicos (por ejemplo en muchos países se acepta la notificación procesal por esta vía), y porque además es un instrumento idóneo para el intercambio de informaciones y opiniones (en este último caso, puede adquirir importancia si por ejemplo se utiliza para copiar el contenido de una página censurada, y permitir la difusión de las informaciones que se pretenden prohibir, en los países en que se aplica la censura).

[12] Cfr. CORREDOIRA Y ALFONSO, Loreto, "Lectura de la Declaración Universal de Derechos Humanos de 1948 en el paradigma de la nueva Soceidad de la Información. Estudio específico del artículo 19". En COTINO HUESO, Lorenzo (coord.), *ob. cit.*, p. 68 a 71.

[13] ROIG BATALLA, Antoni, "El anonimato y los límites a la libertad en Internet". En COTINO HUESO, Lorenzo (coord.), *ob. cit* , p. 321.

[14] Cfr. ROIG BATALLA, Antoni, *ob. cit.* En COTINO HUESO, Lorenzo (coord.), *ob. cit* , p. 323.

2. LA SITUACIÓN EN LA LEGISLACIÓN ARGENTINA

La libertad de expresión ha sido receptada por casi la totalidad de las Constituciones de los estados democráticos, y reafirmada en los principales acuerdos y declaraciones internacionales. A continuación, conoceremos las normas de fuente internacional y nacional que rigen en el derecho argentino:

A) Tratados internacionales: deben destacarse dos documentos, a saber: el Pacto Internacional de Derechos Civiles y Políticos, y la Convención Americana sobre Derechos Humanos.

Por un lado, el Pacto Internacional de Derechos Civiles y Políticos, aprobado por ley 23.313[15], y ratificado el 8 de agosto de 1996, establece en su artículo 19:

"1. Nadie podrá ser molestado a causa de sus opiniones.

2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones 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.

3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a) Asegurar el respeto a los derechos o a la reputación de los demás;

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

Por su parte, la Convención Americana sobre Derechos Humanos, más conocida como Pacto de San José de Costa Rica, aprobada por ley 23.054[16] y ratificada el 5 de septiembre de 1984, en su artículo 13 dispone lo siguiente:

"1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de

[15] *B.O.* 13-V-1986.
[16] *B.O.* 27-III-1984.

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.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura, sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la Ley y ser necesarias para asegurar:

a) El respeto a los derechos o a la reputación de los demás, o

b) La protección de la seguridad nacional, el orden público o a la salud o la moral pública".

B) Constitución Nacional: las disposiciones que entran en juego son las que se citan a continuación:

a) Artículo 14: "*Todos los habitantes de la Nación gozan de los siguientes derechos [...] de publicar sus ideas por la prensa sin censura previa.*".

Esta disposición debe interpretarse de manera amplia y flexible, tal cual se hizo al comienzo del capítulo al esbozar un concepto, pues va más allá de la simple protección de la libertad de prensa, ya sea en lo relativo al objeto (abarca la publicación de ideas, opiniones, hechos, noticias e informaciones), al medio (prensa escrita, radio, televisión, cable, Internet), y al sujeto titular del derecho (desde una faz activa el derecho lo tiene el propietario del medio de comunicación, y desde una faz pasiva, toda persona tiene derecho a "recibir" sin censura previa todo tipo de información y por distintos medios[17]). El alcance de la prohibición de censura previa, será analizado con mayor profundidad en el próximo punto.

b) Artículo 32: "*El Congreso Federal no dictará leyes que restrinjan la libertad de imprenta o establezcan sobre ella la jurisdicción federal*".

Aquí, es preciso distinguir la atribución legislativa de la jurisdiccional. Respecto de la primera, si bien el artículo en un principio fue interpretado de manera estricta por la Corte Suprema de Justicia de la Nación, con ciertos vaivenes en cuanto a la rigurosidad literal (ver fallos "Argerich"[18] y "Ministerio Fiscal de Santa Fe"[19]), en la

[17] Cfr. PIZARRO, Ramón Daniel, *ob. cit.*, p. 113 a 115.
[18] CSJN, 12/4/1864, *Fallos*, 1:130.

hora actual predomina la interpretación de que el Congreso Nacional tiene exclusiva competencia para legislar dentro del Código Penal (Art. 75 inc. 12 CN) los delitos comunes, independientemente de que sea cometido por medio de la prensa (en autos *"Ramos, Raúl Alberto"*[20]). Respecto de la jurisdicción, la evolución ha sido idéntica, prevaleciendo la idea de que los delitos comunes cometidos por la prensa deben ser juzgados por tribunales federales o tribunales provinciales, según las personas, las cosas o los lugares caigan en una jurisdicción o en otra.

c) Artículo 42: "*Los consumidores y usuarios de bienes y servicios tienen derecho, en la relación de consumo, [...] a una información adecuada y veraz; a la libertad de elección, y a condiciones de trato equitativo y digno."*

La relación informativa, vale decir, aquella que se establece entre el medio de comunicación y el destinatario de la información, es una relación de consumo, y por tanto, debe ser encuadrada dentro de éste artículo y dentro de las previsiones normativas de la ley de Defensa del Consumidor 24.240[21]. Al respecto, sostiene Pizarro que *"la realidad muestra día a día un profundo menosprecio de algunos medios por los derechos de los consumidores* (de información periodística), *que se traduce en la emisión intencional de noticias o difusiones inexactas [...]. Ello genera un grave atentado contra el derecho que todos tenemos a estar verazmente informados [...]"*[22]. Asimismo, este derecho es de vital importancia, pues los consumidores toman decisiones y/o actúan en base al conocimiento de la información de hechos u opiniones ajenas que reciben de los medios.

En lo que respecta a Internet, el vínculo anterior se da efectivamente entre el proveedor de contenidos y el usuario, pero también se da otra relación de consumo, independiente de aquélla, entre el proveedor de servicio de acceso a la red y el usuario, que por supuesto también se inscribe dentro de la esfera tuitiva del *ius consommatoris*.

d) Artículo 75 inc. 22: "*Corresponde al Congreso: [...] 22. Aprobar o desechar tratados concluidos con las demás naciones y con las organizaciones internacionales y*

[19] CSJN, 23/12/1932, *Fallos*, 167:121.
[20] CSJN, 21/10/1970, *Fallos*, 278:73.
[21] *B.O.* 15-X-1993.
[22] PIZARRO, Ramón Daniel, *ob. cit.*, p. 92.

los concordatos con la Santa Sede. Los tratados y concordatos tienen jerarquía superior a las leyes.

[...] la Declaración Universal de Derechos Humanos; la Convención Americana sobre Derechos Humanos; el Pacto Internacional de Derechos Civiles y Políticos y su Protocolo Facultativo [...] en las condiciones de su vigencia, tienen jerarquía constitucional, no derogan artículo alguno de la primera parte de esta Constitución y deben entenderse complementarios de los derechos y garantías por ella reconocidos."

Este artículo debe interpretarse conjuntamente con el 31, pues ambos establecen la jerarquía de las normas en nuestro país. De esta manera, se incorporan los tratados de derechos humanos mencionados *ut supra* a la parte dogmática de nuestra Carta Magna, complementándola y ampliándola.

B) Leyes y decretos: luego de haber analizado el conjunto de preceptos que conforman el bloque constitucional aplicable al tema, debe hacerse referencia a las normas que en su consecuencia se dictaron:

a) Ley 26.032[23]: incorpora al derecho positivo argentino el reconocimiento de la libertad de expresión en Internet. En este sentido, establece que: "L*a 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 Molina Quiroga, entre los fundamentos del proyecto se destacó "*la importancia que en las sociedades modernas tiene el servicio de Internet, pues resulta 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*." [24]

b) decreto 1279/1997[25]: como antecedente inmediato a la ley 26.032 podría citarse a este decreto. El mismo declaró que "*el servicio de Internet se considera com-*

[23] *B.O.* 17-VI-2005.
[24] MOLINA QUIROGA, Eduardo, *ob. cit.*
[25] *B.O.*, 1-XII-1997.

prendido 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". El Poder Ejecutivo, en sus considerandos, se refirió a "*la necesidad de remover los obstáculos que frenan el crecimiento de Internet, pero sin interferir en la producción, creación y/o difusión del material*", y justificó la norma resaltando que "*una de las características esenciales del servicio Internet es su interconectividad, por la cual los usuarios tienen la libertad de elegir la información de su propio interés, resultando por ello que cualquier pretensión de manipular, regular o de censurar los contenidos del servicio, se encuentra absolutamente vedada por la normativa vigente*". Asimismo, destacó que, resultan de aplicación los arts. 14, 32 y 42 de la Constitución Nacional, el Pacto San José de Costa Rica, y la jurisprudencia de nuestro Alto Tribunal, como así también la de la Corte Suprema de los EE.UU.

c) decreto 554/1997[26]: declara "*de interés nacional el acceso de los habitantes de la República Argentina a la red mundial Internet, en condiciones sociales y geográficas equitativas, con tarifas razonables y con parámetros de calidad acordes a las modernas aplicaciones de la multimedia*".

d) otras normas que regulan la prestación del servicio de Internet: la Ley Nacional de Telecomunicaciones N° 19.798[27], el decreto N° 764/2000[28], la Ley de Lealtad Comercial N° 22.802[29], la Ley de Defensa al Consumidor N° 24.240, y la Ley de Defensa de la Competencia N° 25.156[30].

[26] *B.O.*, 23-VI-1997.
[27] *B.O.*, 22-VIII-1972.
[28] *B.O.*, 3-IX-2000.
[29] *B.O.*, 5-V-1983.
[30] *B.O.*, 20-IX-1999.

3. LA SITUACIÓN EN LA JURISPRUDENCIA ARGENTINA

Existe un extendido consenso sobre la equiparación de Internet a un medio de comunicación, con las características novedosas y particulares que esta tecnología implica. En el ámbito judicial nacional, es de rigor destacar algunos precedentes de trascendencia, a saber:

En el caso Vita[31], los imputados habían utilizado el espacio de Internet para difundir sus ideas acerca de la problemática del consumo de estupefacientes y su prohibición legal (contenida en el artículo 12 de la ley 23.737[32]). El tribunal entendió que habían utilizado "*un medio de prensa para criticar, dar y recibir información sobre el tema antes apuntado*", y que de ello no se derivaba ninguna conducta ilícita, pues "*el derecho de los ciudadanos a expresarse en dirección contraria a la política criminal del Estado debe prevalecer* (por sobre la prohibición aludida)".

El fallo, entre sus importantes consideraciones, se refirió expresamente a la naturaleza jurídica de Internet, diciendo que "*las publicaciones en páginas de Internet se encuentran alcanzadas por las garantías que protegen tanto la libertad de expresión como la libertad de prensa. En efecto, más allá de las discusiones doctrinarias sobre el alcance de la libertad de prensa, es claro que nos encontramos ante un nuevo medio de comunicación, "Internet", en el que conviven y mediante el cual se expresan - entre otras - actividades científicas, comerciales, periodísticas y personales. Por ello, corresponde, a la luz de los hechos del caso, y al amparo de la Ley Fundamental, considerar a la "red de redes" como otro medio comunicacional público y masivo, en el que se vierten diversas formas de expresión, lo cual incluye a la prensa".*

Otra asimilación de Internet a los medios de prensa tuvo lugar en un tribunal laboral en el caso "Hojman"[33], al analizarse cuál era la naturaleza de las tareas cumplidas por el responsable de contenidos de un portal en Internet. Como el sitio de

[31] Vita Leonardo G. y González Eggers, Matías s/procesamiento, Sala I de la Cámara de Apelaciones en lo Criminal y Correccional de la Capital Federal, 13/03/2002. Publicado en: http://www.hfernandezdelpech.com.ar/JurisprudenciaArgLiberExpreFalloCamaraFed.htm, consultado 09/09/10.

[32] Art. 12: *"Será reprimido con prisión de dos a seis años y multa de doscientos veinticinco mil a cuatro millones quinientos mil australes: a) El que preconizare o difundiere públicamente el uso de estupefacientes, o indujere a otro a consumirlos; b) El que usare estupefacientes con ostentación y trascendencia al público.".*

[33] Hojman, Eduardo A. y otro c/ XSALIR.COM S.A. y otro s/despido, Sala 6ª de la Cámara Nacional de Apelaciones del Trabajo, 17/3/2003. Publicado en: http://www.abogadosrosarinos.com, consultado 09/09/2010.

las demandadas proporcionaba una guía de salidas para la ciudad incluyendo notas y reportajes periodísticos, se concluyó que dicho portal era *"similar a un suplemento de espectáculos de un diario, con la única diferencia que, en lugar de publicarse, se difundía en la red"*. El tribunal estableció que: "l*as nuevas tecnologías, entre ellas la de Internet, rebasan el contenido tradicional y real del periodismo escrito, oral o televisivo, para abrirse al aspecto virtual del mismo, entre el cual la existencia de un portal es uno de los más interesantes, aclarando que se entiende por "portal" un sitio en Internet que acumula informaciones, noticias, datos, tanto de interés general como particular*". La consecuencia fue la aplicación del estatuto del periodista profesional al responsable del citado sitio web.

4. RESTRICCIONES A LA LIBERTAD DE CONTENIDO EN INTERNET

En el sistema constitucional argentino, no hay derechos absolutos y todos están subordinados a las leyes que reglamenten su ejercicio (arts. 14 y 28 CN). La libertad de expresión, como derecho reconocido en la Carta Magna (art. 14 y 75 inc. 22), entonces es siempre relativa y sujeta a restricciones impuestas por los poderes públicos en cuanto tiendan a la protección de la seguridad, la moralidad, la salubridad, y el ámbito económico y social en procura del bienestar general.

Debe advertirse, sin embargo, que las limitaciones impuestas a este derecho resultan particulares por el hecho de que su ejercicio sólo se hace efectivo una vez que se opinó o informó y no antes, razón por la cual no puede ser objeto de control preventivo pero si puede ser fundamento de responsabilidad posterior. Lo anteriormente manifestado, se puede resumir en el siguiente principio: *"el ejercicio del derecho a la libertad de expresión no está sujeto a censura previa sino sólo a responsabilidades ulteriores expresamente establecidas por ley y destinadas exclusivamente a garantizar el respeto de los derechos, la reputación de las personas y la protección de la seguridad, la moral y el orden público"*[34].

De esta forma, debe concluirse que existen dos tipos de restricciones en el caso en que exista un abuso en el ejercicio de la libertad de expresión: la que surgen

[34] Fórmula consagrada en el Pacto San José de Costa Rica (art.13 inc. 2) e incluso en algunas constituciones provinciales como por ejemplo la de Córdoba (art. 51).

con posterioridad a su ejercicio (responsabilidad ulterior), y las que se imponen con anterioridad (censura previa). Asimismo, también debe concluirse que así como la responsabilidad ulterior es excepcional (pues está condicionada a estar consagrada expresamente por ley y ser necesaria para asegurar el respeto de los derechos, la reputación de las personas y la protección de la seguridad, la moral y el orden público), la censura previa es excepcionalísima (pues se admite en un sólo caso: el del art. 13 inc 4° del PSJCR[35]).

En base a ello, entonces, es posible afirmar que en materia de restricciones al ejercicio de la libertad de expresión, la regla es la imposición de responsabilidades ulteriores, y la excepción es la censura previa.

Por supuesto que todas estas consideraciones son aplicables a la Internet, y, siguiendo el mismo razonamiento, puede sostenerse que hay dos formas de restringir el derecho a la libertad de contenido en la red: censurando previamente un material que se considera ilícito o inadecuado (se evita que se consume un abuso con su publicación en un sitio web), o bien, imponiendo la obligación de resarcir los daños causados (para disuadirlos a que no se vuelvan a cometer otros abusos) más la remoción del material que afectan los derechos de terceros.

5. EL DERECHO A LA INTIMIDAD COMO LÍMITE A LA LIBERTAD DE CONTENIDO

Queda claro que el principio general adoptado para los contenidos en Internet es el de absoluta libertad, y que en ningún caso puede haber censura previa, salvo la única excepción prevista por el artículo 13 inciso 4 del Pacto San José de Costa Rica relativa a la pornografía infantil. En todo caso, el remedio para los excesos en el ejercicio de la libertad de expresión será la responsabilidad ulterior a la que deben atenerse los autores de dichos abusos. De esta forma, serán responsables aquellos que "suban" a la red contenidos que puedan afectar legítimos intereses, como ser derechos de autor, derechos de propiedad sobre una marca o nombre

[35] *"Artículo 13.- Libertad de pensamiento y de expresión. […] 4) Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2".*

comercial, o bien contenidos que sean calumniosos o injuriosos o puedan implicar una incitación a cometer delitos o actos discriminatorios, o finalmente contenidos que afecten a la intimidad o privacidad de las personas.

Este último, resulta un caso paradigmático, y sobre él hará hincapié nuestra tesis. Nos referimos al caso en el que la intimidad o privacidad del ser humano, su honor o su imagen se ven vulnerados por otros particulares y concretamente por el exceso en el ejercicio de la libertad de expresión o del derecho a la información.

En lo que aquí interesa, sólo diremos que el bien jurídico "intimidad", expresamente protegido por nuestra Constitución Nacional y por los tratados internacionales con jerarquía constitucional, al entrar en conflicto con la libertad de expresión, originan una espinosa cuestión jurídica, generadora de un arduo debate respecto de qué valor debe prevalecer.

En nuestro país, no existe norma constitucional o legal alguna que reglamente el derecho a la información y el derecho al honor, a la intimidad y a la imagen propia, delimitando bien las fronteras entre unos y otros, y estableciendo los medios para salvaguardarlos y para restituir a los afectados cuando estos hubieren sido vulnerados[36].

Sin embargo, una vez más, la Corte Suprema ha resuelto el tema en autos "Campillay"[37] (ratificado en "Costa"[38]), donde se refirió a la responsabilidad de la prensa por noticias agraviantes o inexactas. Entendemos que, la doctrina que se desprende del caso es aplicable a Internet, pues coincidimos con Galdós en que "*podría aludirse a información inexacta y agraviante como sinónimo de* (contenido) *nocivo [...] el material nocivo, inexacto, agraviante es esencialmente dañino; afecta el honor, la honra, reputación de terceros lesionando sus convicciones, creencias, opiniones, fama, etc.*"[39]

---

[36] Cfr. PIACENZA, Diego Fabio, "El derecho a la intimidad y los medios de comunicación", agosto de 2009, publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=16099, consultado: 24/09/2010.

[37] "Campillay, Julio C. c/ La Razón y otros", CSJN (Fallos 308:789), 15/05/1986. Para un extenso análisis del fallo y de la doctrina que se sienta en base al mismo, ver: PIZARRO, Ramón Daniel, "Responsabilidad civil de los medios masivos de comunicación. Daños por noticias inexactas o agraviantes.", Editorial Hammurabi, Buenos Aires, 1999, p. 298 a 317.

[38] "Costa, Héctor R. c/ Municipalidad de la Ciudad de Buenos Aires y otros", CSJN, 12/03/1987.

[39] GALDÓS, Jorge Mario, "Responsabilidad civil e Internet: Algunas aproximaciones", JA 2001-III-819, publicado en: http://www.abeledoperrot.com.ar, consultado 09/09/2010.
Sostiene Galdós que, en pocas palabras, la Corte Federal a partir del precedente "Campillay" sentó esta interpretación sobre la responsabilidad de la prensa:

Creemos que excedería con creces el objeto del presente trabajo el análisis de la responsabilidad de los medios de comunicación en general. Por ello, para un tratamiento más especializado en relación a la responsabilidad de los ISP por contenidos ilícitos o nocivos, remitimos al capítulo VI.

-"el honor puede afectarse no sólo a través del delito de calumnias e injurias, sino también de un acto meramente culpable o aun del ejercicio abusivo del derecho de informar;
-para excusar su responsabilidad el órgano de prensa debió haber indicado la fuente, y utilizado un tiempo de verbo potencial, o haber guardado reserva sobre la identidad de las personas;
-si se trata de funcionarios públicos, éstos deben probar que la información fue efectuada a sabiendas de su falsedad o con total despreocupación acerca de tal circunstancia; en cambio, basta la negligencia precipitada o simple culpa en la propagación de una noticia de carácter difamatorio de un particular -o de un empleado público de ínfima categoría".

CAPÍTULO III

EL DERECHO A LA INTIMIDAD

En la actualidad, en pleno auge de Internet como nuevo medio de comunicación e información, el derecho a la intimidad puede verse seriamente afectado por la utilización indebida de los datos o las imágenes que de una persona pueden obtenerse por los hábitos de navegación de los usuarios.

En el presente capítulo se analizará el concepto del derecho a la intimidad desde el punto de vista del derecho constitucional y legal argentino, pero sin dejar de tener en cuenta la perspectiva que se tiene otros sistemas jurídicos más sofisticados, como lo son la normativa europea y estadounidense.

1. CONCEPTO

Puede definirse al derecho a la intimidad como "*el derecho personalísimo que garantiza a su titular el desenvolvimiento de su vida y de sus acciones dentro de un ámbito de privacidad, sin injerencias que puedan provenir de autoridad o de terceros, y en tanto dicha conducta no ofenda a la moral, a las buenas costumbres y al orden público, ni perjudique los bienes o la persona de terceros*"[1].

En el mismo sentido, debemos destacar una definición propuesta por nuestra Corte Suprema en el *leading case* "Ponzetti de Balbín"[2], al establecer que "*el derecho a la privacidad e intimidad, con fundamento en el artículo 19 de la Constitución*

[1] PANDIELLA, Juan Carlos, "El bien jurídico tutelado por el habeas data", publicado en: http://www.foroabogadossanjuan.org.ar/Doctrina_Provincial/pandiella.htm, consultado: 09/08/2010.

[2] Ponzetti de Balbín, Indalia c. Editorial Atlántida S.A, CSJN, 11/12/1984 (Fallos, 306:1892).
El fallo, entre sus ricos considerandos, amplía el concepto de la siguiente manera: "*En rigor, el derecho a la privacidad comprende no sólo a la esfera doméstica, el círculo familiar y de amistad, sino otros aspectos de la personalidad espiritual o 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 otros, la defensa de la sociedad, las buenas costumbres o la persecución del crimen*".

Nacional, en relación directa con la libertad individual, protege jurídicamente un ámbito de autonomía individual constituido por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o datos que, teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significan un peligro real o potencial a la intimidad".

Debemos hacer algunas consideraciones a los fines de precisar el alcance de esta noción:

- En primer lugar, entendemos que el derecho a la intimidad suele comprender una amplia gama de garantías: la protección del secreto o reserva de actos de la vida privada de toda persona (datos sobre su salud, sus prácticas religiosas, su sexualidad, su ideología política, etc.), el secreto de la correspondencia epistolar, electrónica y de otros papeles privados, la inviolabilidad del domicilio, el derecho a la imagen, el derecho al buen nombre y honor, y el derecho al secreto profesional.

- Asimismo, debe aclararse que al ser un derecho personalísimo, y como tal inherente a la personalidad de un ser humano, de un hombre "de carne y hueso", al decir de Unamuno, es exclusivo de las personas de existencia física y no de las de existencia ideal o jurídicas. En todo caso, estas últimas estarán amparadas por un derecho a la reputación, al nombre comercial y a la inviolabilidad de su sede social, pero no forman parte del concepto de derecho a la intimidad.

- Por último, si bien suelen utilizarse los términos "intimidad" y "privacidad" como sinónimos, debe advertirse que no son nociones idénticas, pues la intimidad se refiere a la esfera personal que no se exterioriza a terceros, mientras que la privacidad comprende las acciones y conductas que se exteriorizan, y son conocidas por terceros, en tanto no afecten sus derechos[3]. En el presente trabajo, sin embargo, se utilizaran ambos términos de manera indistinta, y en el sentido amplio apuntado *ut supra.*

[3] Cfr. PANDIELLA, Juan Carlos, *ob. cit.*

2. ANTECEDENTES HISTÓRICOS. CONTEXTO ACTUAL

Según Piacenza[4], la primera formulación moderna del derecho a la intimidad podemos encontrarla en la Constitución de los Estados Unidos de 1787, en particular en la IV Enmienda, que dispone: *"el derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen seguros de inquisiciones y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto órdenes que no se apoyen en una causa probable, estén sostenidas mediante juramento o protesta y describan particularmente el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas"*[5].

Según el autor, tal consagración responde a "*la idea de esbozar un derecho a gozar de la vida, el llamado a estar solo, frente a los frecuentes ataques de la prensa amarilla norteamericana, que suponía un peligro para el pensamiento puritano de la Nueva Inglaterra, entre el que, se encontraba la privacidad*" [6].

Estas consideraciones respecto de la experiencia estadounidense, a su vez, son plenamente aplicables a lo que acontecía contemporáneamente en Europa, y que daría lugar a un proceso de constitucionalización de los derechos fundamentales. En este contexto, podemos afirmar que el concepto de intimidad nace a partir de la noción de libertad individual, pues se consideraba que el desarrollo de la personalidad del hombre sólo puede alcanzarse si se garantiza su privacidad frente a injerencias arbitrarias del Estado. Recordemos que en aquél tiempo se alzaba como bandera la defensa de las libertades individuales - y un consecuente Estado liberal como garante de ellas - como respuesta al absolutismo de los regímenes imperantes.

Avanzando en el tiempo, ya en la segunda mitad del siglo XX, con el advenimiento de las innovaciones tecnológicas en materia de información y comunicación, y del consumo masivo de los nuevos medios, el ámbito de la inviolabilidad de la persona y la necesidad de tutelar la intimidad adquiere un nuevo significado.

---

[4] Cfr. PIACENZA, Diego Fabio, "El derecho a la intimidad y los medios de comunicación", agosto de 2009, publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=16099, consultado: 24/09/2010.

[5] Fourth Amendment: *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized"*.

[6] PIACENZA, Diego Fabio, *ob. cit.*

En este sentido, el derecho a la intimidad ya no es solamente un presupuesto de la libertad del individuo o una mera garantía para evitar injerencias arbitrarias del Estado; por el contrario, adquiere una notable trascendencia como derecho humano fundamental frente a las injerencias de los particulares, que en su mayoría son empresas periodísticas titulares de los modernos medios de comunicación.

Asimismo, resulta característico de esta etapa que las nuevas amenazas para la libertad y dignidad del ser humano se perfeccionan con el poder que ofrece la tecnología. Al decir de Piacenza, *"no alcanza la inviolabilidad del habeas corpus, pues hoy no es necesario constreñir o coartar la libertad y los derechos políticos por medio de controles físicos o corpóreos sobre el ciudadano"* [7].

El derecho, ante esta realidad, reacciona a través de la consagración de nuevos institutos jurídicos, cuyo paradigma es el *habeas data*, el cual se erige como el gran remedio ante el avance de las técnicas informáticas de tratamiento y manipulación de los datos personales. Las primeras leyes que trataron este problema fueron: la ley de Hesse en Alemania (1970), la *Datalag* sueca (1973), la *Privacy Act* estadounidense (1974), la Constitución Portuguesa de 1976 y la Española de 1978, la Ley de Protección de datos francesa (1978), la *Data Protection Act* inglesa (1984), entre otras[8]. Recordemos que, a partir de la reforma del año 1994, en nuestro país el *habeas data* goza de jerarquía constitucional (art. 43 CN, párrafo 3°), y que ha sido reglamentado recién en el año 2000 con el dictado de la ley 25.326[9].

Finalmente, en la actualidad, este problema llega a un grado máximo de tensión. A partir de la cuasi-masificación del uso de Internet, los riesgos de afectación se multiplican, dada la mayor cantidad de información que circula por la red, y la mayor complejidad de los sistemas informáticos que se utilizan para su recolección. Paralelamente, surgen nuevas formas de intromisión: violación del correo electrónico, "spoofing", "cookies", "spam", redes sociales, entre otras.

En suma, todo esto deja en evidencia que la intimidad en la era de Internet, lejos está de su concepto originario, y que, ni siquiera algunas "nuevas" institucio-

[7] PIACENZA, Diego Fabio, *ob. cit*.
[8] Cfr BRENNA, Ramón Gerónimo, "Internet y Privacidad. Reflexiones sobre la Sociedad de la Información y la Recolección de Datos *On Line*". En ALTMARK, Daniel R. (dir.), BIELSA, Rafael A. (coord.) y otros, "Informática y Derecho", Editorial Lexis Nexis, Buenos Aires, 2002, Volumen 8: Internet, pág. 2.
[99] *B.O.*, 02-XI-2000.

nes – como el *habeas data* – llegan a ser del todo efectivas. Por ello, es preciso que las teorías y prácticas jurídicas propongan y dispongan soluciones globales – pues globales son los problemas que plantea el ciberespacio - en la forma de proteger este derecho fundamental.

3. EN LA CONSTITUCIÓN NACIONAL

Nuestra Carta Magna consagra el derecho a la intimidad en varios artículos:

A) "*Art. 18.- […] El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados; y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación. […]*"

Nuestro artículo 18 recepta la garantía que Bidart Campos denomina "libertad de intimidad"[10], la cual se proyecta a la inviolabilidad del domicilio y de la correspondencia epistolar y demás papeles privados, en las condiciones que las leyes que reglamentan su ejercicio estipulen.

En cuanto a la protección constitucional del domicilio, éste debe entenderse en un sentido más amplio que el concepto que nos da el Código Civil; debe entenderse por domicilio a "*toda morada destinada a la habitación y desenvolvimiento de la libertad personal en lo concerniente a la vida privada, ya sea cerrada o abierta parcialmente, móvil o inmóvil, de uso permanente o transitorio*"[11]. La garantía de inviolabilidad se extiende en dos sentidos: por un lado, frente al Estado, impide a sus funcionarios el allanamiento sin una orden judicial; por otro lado, frente a los particulares, implica el derecho a impedir el acceso y la permanencia contra la voluntad del titular.

En cuanto a la correspondencia epistolar y los papeles privados, la garantía de inviolabilidad se extiende a las cartas misivas, legajos, fichas e historias clínicas de clientes o enfermos que reservan los profesionales, libros de comercio, etc.

[10] BIDART CAMPOS, Germán J., "Manual de la Constitución Reformada", Editorial Ediar, Buenos Aires, 1996, Tomo I, pág. 522.
[11] BIDART CAMPOS, Germán J., *ob. cit*., pág. 523.

Asimismo, la libertad de intimidad se amplía hacia otros ámbitos: comunicaciones que por cualquier medio no están destinadas a terceros, sea por teléfono, por fax, y, por supuesto, las comunicaciones personales que pueden establecerse por medio de los distintos servicios de Internet. Este último aspecto, a su vez, afecta simultáneamente a la libertad de expresión, pues la expresión que se transmite en uso de la libertad de intimidad no puede ser interferida o capturada arbitrariamente.

B) *"Art. 19.- Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas 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."*

Este artículo se refiere a las acciones que de ninguna manera se exteriorizan al público, es decir, aquellas que permanecen en el esfera íntima del hombre. Bidart Campos alude a ellas como "conductas autorreferentes", es decir, *"las que sólo se refieren y atañen al propio sujeto autor, sin proyección o incidencias dañinas de modo directo para terceros"* [12].

Asimismo, se advierte que este tipo de conductas tienen estrecha vinculación con otras libertades individuales. Así, por ejemplo, cuando la libertad de intimidad se relaciona con ciertos aspectos de la libertad religiosa que hacen al fuero íntimo del hombre, da lugar a la llamada libertad de conciencia, o cuando se la relaciona con la libertad de expresión, en su sentido negativo, da lugar al llamado derecho "al silencio" y "al secreto", que implica la facultad de reservarse ideas, sentimientos, conocimientos y acciones que el sujeto no desea voluntariamente revelar a terceros.[13]

C) "Art. 43. - [...] Toda persona podrá interponer esta acción (en referencia al amparo) *para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso*

[12] BIDART CAMPOS, Germán J., *ob. cit*., pág. 523. El autor cita a título enunciativo los siguientes ejemplos de conductas autorreferenciales: a) La elección del plan personal de vida autorreferente, y su realización; b) la objeción de conciencia por razones morales o religiosas, cuando es inofensiva para terceros; c) la preservación de la propia imagen frente a terceros; d) el control y la disposición de los datos personales, incluso para impedir su difusión innecesaria; e) el derecho a la identidad personal; f) el derecho a ser "diferente".

[13] Cfr. BIDART CAMPOS, Germán J., *ob. cit*., págs. 524 y 525.

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. […]"

Debe dejarse en claro que el artículo 43 fue incorporado con la reforma de 1994, dentro del Capítulo II de la Primera Parte de la Constitución, denominado "Nuevos derechos y garantías", y que hasta ese momento las únicas normas relativas al derecho a la intimidad eran los artículos 18 y 19.

La citada norma incorpora expresamente en el primer párrafo, la acción de amparo, en el segundo, el amparo colectivo, y, finalmente, en su tercer párrafo, la acción de *habeas data*[14]. Ésta última ha sido definida como *"una acción de protección de los datos personales específicamente ordenada a la defensa de la intimidad de los datos, al derecho a la autodeterminación informativa y a la propia imagen, aun cuando no estén dadas las condiciones de arbitrariedad e ilegalidad del acto cuestionado"*[15]. A partir de esta definición, debe destacarse que, más allá de la discusión respecto de si es una acción de amparo o una acción independiente, la arbitrariedad o ilegalidad manifiesta no son requisitos para su procedencia.

Esta parte del art. 43, debe interpretarse en concordancia con la ley 25.326, que se dictó en el año 2000, y que, además de reglamentar la acción de habeas data, incluye una serie de disposiciones relativas a la protección integral de la privacidad de los datos personales frente a los abusos informáticos. Volveremos sobre el tema al tratar los datos personales en Internet (capítulo IV).

4. EN LOS PACTOS INTERNACIONALES

Los pactos internacionales firmados por nuestro país contienen disposiciones expresas relacionadas con el derecho a la intimidad:

[14] El art. 43 no utiliza ni menciona la expresión "*habeas data*" (que significa que una persona "tiene sus datos" o "eres dueño de tus datos"). La omisión se debe a que la declaración de la necesidad de reforma constitucional no hizo referencia al *habeas data*, y solamente habilitó enmiendas para incorporar el *habeas corpus* y el amparo. De ahí que se introdujo esta garantía a través de la acción de amparo.

[15] BASTERRA, Marcela I. "El *Habeas Data*". En MANILI, Pablo Luis y otros, "Derecho Procesal Constitucional", Editorial Universidad, Buenos Aires, 2005, p. 144.

A) En la Declaración Universal de Derechos Humanos: *"Artículo 12. 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."*

B) En el Pacto Internacional de Derechos Civiles y Políticos: *"Artículo 17.*

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

C) En el Pacto San José de Costa Rica: *"Artículo 11.- Protección de la honra y de la dignidad.*

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. 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.

3. Toda persona tiene derecho a la protección de la Ley contra esas injerencias o esos ataques".

Del juego de los arts. 31 y 75 inc. 22, surge con evidencia que este conjunto de normas revisten de jerarquía supralegal, y complementan la protección constitucional que del derecho a la intimidad se hace en la primera parte de la Constitución.

Si bien en los tratados no existe una norma expresa que consagre el *habeas data,* coincidimos con Bidart Campos en cuanto *"cada vez que en alguna norma de los mismos se hace referencia a derechos y bienes jurídicos que guardan relación o se identifican con los que el habeas data protege, es muy claro comprender que se les debe dispensar el "recurso sencillo y rápido" que, innominadamente, aparece en el Pacto de San José de Costa Rica y en el Pacto Internacional de Derechos Civiles y Políticos"*[16].

Por otro lado, también debe resaltarse que, por la naturaleza del derecho que se encuentra en boga, se trata de normas plenamente operativas, y por tal mo-

[16] BIDART CAMPOS, Germán J., *ob. cit.*, Tomo 2, pág. 393.

tivo, no requieren para su goce efectivo de una ley específica que reglamente su ejercicio.

5. EN EL DERECHO COMPARADO

A continuación, pasaremos revista de las principales cláusulas constitucionales de otros países, que reafirman la protección de la intimidad:

A) En los Estados Unidos de América, la Constitución Federal ha consagrado el derecho a la intimidad – si bien no de manera expresa – en la ya citada IV enmienda. La interpretación de esta garantía constitucional ha sido definida por la *Supreme Court* a través de dos etapas muy marcadas.

En una primera etapa, se destaca el caso *"Olmstead v. United States"*[17], particularmente el voto del juez Brandeis (quien casualmente hace casi 40 años atrás había publicado - junto a Warren - un artículo intitulado "R*ight to Privacy",* el cual, en su momento, fue el primero en tratar el tema de la intimidad desde la óptica jurídica), ya que por primera vez se interpreta que el interés de la IV enmienda no es el de proteger la propiedad sino el "derecho a ser dejado solo" (*right to be let alone*), que, al decir de Piacenza, se refiere a "*un derecho a la privacidad consistente en no estar obligado a participar en la vida colectiva, y por tanto, el poder permanecer aislado de la comunidad sin establecer relaciones y que implica también el permanecer en el anonimato, el ser dejado en paz sin ser molestado y el no sufrir intromisiones en la soledad física que la persona reserva sólo para sí misma*"[18].

Ahora bien, dentro de lo que podríamos llamar una segunda etapa, este concepto de "*right to privacy*" ha sido ampliado por la jurisprudencia norteamericana, a punto tal de haber constituido una noción tan vaga que, parecería comprender un conjunto de elementos que - de acuerdo a nuestras tradiciones jurídicas - poca relación tendrían con nuestro derecho a la intimidad. Así lo advierte Puente de la Mora cuando afirma que "*a diferencia de las tendencias europeas que se observa respecto a*

[17] Olmstead v. United States (277 U.S. 438, 1928). El caso es citado por PUENTE DE LA MORA, Ximena, "Privacidad de la Información Personal y su Protección Legal en Estados Unidos", Alfa-Redi: Revista de Derecho Informático, No. 097, Junio del 2006, publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=6956, consultado: 27/09/2010.
[18] PIACENZA, Diego Fabio, *ob. cit.*

la intimidad informática o protección de datos personales, en Estados Unidos se ha seguido un camino diferente a través del desarrollo del concepto de "privacy" en cual se aplica a varias vertientes del derecho: privacidad genética, privacidad en las conversaciones de un psicoterapeuta y su paciente, privacidad en la información médica, privacidad en las asociaciones, privacidad en el hogar, en la escuela, en el trabajo, etc. siendo la protección de datos personales un concepto que se protege a través de la privacidad aplicada a los registros y bases de datos electrónicas"[19].

B) La regulación legal en México de la vida privada se desprende del artículo 16 de la Constitución Federal. Dicha norma dispone una fórmula similar a la IV enmienda de la Constitución de los EE.UU.: *"Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones sino en virtud de mandamiento escrito de autoridad competente que funde y motive la causa legal del procedimiento"*[20]. Además, en su extensa redacción, el artículo incluye principios destinados a regular el hábeas data, como así también la inviolabilidad del domicilio y de las comunicaciones privadas.

C) En Europa, a nivel comunitario, son los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea[21] los que protegen el derecho a la intimidad. Éstos disponen:

"Artículo 7.- Respeto de la vida privada y familiar:

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Artículo 8.- Protección de datos de carácter personal:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

[19] PUENTE DE LA MORA, Ximena, *ob.cit.* En relación al tema, advierte la autora que en el caso "Whalen v. Roe" (433 U. S. 425, 1977), la Corte entendió que la protección constitucional de la privacidad abarca el "interés individual de evitar la divulgación de los asuntos personales"; asimismo, señala que esta vertiente del derecho a la privacidad se ha vuelto conocida como el "derecho constitucional a la privacidad informática".

[20] Puede consultarse el texto de la Constitución Mexicana en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1.pdf, consultado: 29/09/2010.

[21] Este tratado fue aprobado el 18 de junio de 2004 y firmado por los jefes de gobierno de los países que forman la Unión Europea, el 29 de octubre de 2004, en Roma. Puede consultarse su texto en español en: http://www.europarl.europa.eu/charter/pdf/text_es.pdf, consultado: 29/07/2010.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente."

A nivel de derecho constitucional nacional, se destacan: el art. 10 de la Constitución Alemana, el artículo 8 de la Constitución de Finlandia, los artículos 14 y 15 de la Constitución Italiana, los artículos 34 y 35 de la Constitución de la República Portuguesa, entre otros[22]. Por último, especial consideración merece el artículo 18 de la Constitución Española[23]. Éste dispone:

"Artículo 18: Derecho a la intimidad. Inviolabilidad del domicilio.

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

2 El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. 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."

Creemos que este último inciso constituye un verdadero ejemplo a nivel de defensa del derecho a la intimidad en los tiempos actuales, ya que es la única norma constitucional que establece expresamente la protección de la correspondencia electrónica.

6. EN EL DERECHO ARGENTINO

Se han dictado en nuestro país diversas normas tuitivas del derecho a la intimidad. Entre ellas deben destacarse por su importancia:

[22] Cfr. HOCSMAN, Heriberto Simón, "Negocios en Internet", Editorial Astrea, Buenos Aires, 2005, págs. 147 y 148.

[23] Puede consultarse el texto completo de la Constitución Española de 1978 en: http://www.boe.es/aeboe/consultas/enlaces/documentos/ConstitucionCASTELLANO.pdf, consultado: 29/07/2010.

A) En el Código Civil: la norma de protección más importante de la intimidad se volcó al Código Civil, específicamente a su artículo 1071 bis (agregado por la ley 21.173[24]), de la siguiente forma: *"El que arbitrariamente se entrometiere en la vida ajena publicando retratos, difundiendo correspondencia, mortificando a otro 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".*

A los fines de reflejar el alcance de la norma, se ha dicho que: *"el artículo 1071 bis del Código Civil contempla, más allá de la revelación de secretos o de intromisiones en lo reservado e íntimo, los ataques u ofensas que mortificando a otros en sus costumbres o sentimientos perturban de cualquier modo su intimidad. Es decir si superada la mera revelación de lo privado se acentúa la lesión por la molestia que produce, prevalece este segundo aspecto y la cuestión roza y hasta se confunde con la estima propia"*[25]. Así, vemos que el 1071 bis contiene una enumeración meramente ejemplificativa, pues no sólo la perturbación a la intimidad puede concretarse "de cualquier modo" (entre los que se incluye a los servicios de Internet), sino que, además, el bien jurídico a tutelar va más allá de la correspondencia y la privacidad, y llega a incluir el honor, la reputación y el buen nombre de la víctima. Creemos que este artículo prevé una herramienta subsidiaria fundamental[26] para cuando la afectación a la intimidad de una persona no sea susceptible de encaminarse por la vía del habeas data, o en su caso, cuando el hecho no llegue a configurar un delito penal (vgr. calumnias e injurias).

De la redacción del artículo, a su vez, se infiere que esta acción no sólo tiende a la reparación de daños y perjuicios, sino también a evitar - en tanto aun sea facti-

[24] *B.O.*, 22-X-1975.
[25] CNCiv., sala C, 276-89 citado por PANDIELLA, Juan Carlos, *ob. cit.*
[26] Procesalmente, el art. 1071 bis podrá encaminarse por la vía del amparo, en el caso en el que se solicite el cese de la acción u omisión arbitraria lesiva de la intimidad (en tanto se cumplan con los requisitos del art. 43, primer párrafo, de la Constitución, y del decreto-ley 16.986), o bien, directamente por medio de una acción por daños y perjuicios.

ble - que el daño siga produciéndose, con lo cual se evidencia la vocación preventiva de la norma.

Por último, se incorpora la posibilidad de una reparación "*in natura*", previéndose la publicación de la sentencia favorable a la víctima "en un diario o periódico del lugar", si es que de tal forma puede atenuarse el daño sufrido. Creemos que este tipo de reparación es plenamente aplicable a los daños cometidos a través de Internet, y que, haciendo una interpretación analógica, la sentencia podría incluirse en el mismo sitio web donde se cometió alguno de los supuestos descriptos en el artículo.

B) En el Código Penal: la garantía se extiende a: a) la violación del domicilio (arts. 150 a 152), b) calumnias e injurias (arts. 109 a 117 bis), y, c) violación de secretos (arts. 153 a 157 bis).

a) Respecto de la violación de domicilio, si bien forma parte de la intimidad, no tiene relación alguna con Internet, pues el domicilio (que en el ámbito penal debe entenderse de bajo el concepto señalado *ut supra*, cuando se hizo alusión a la protección constitucional del mismo), se refiere a un ámbito físico - y no virtual - de la persona.

b) En relación a las calumnias e injurias, que son delitos contra el honor de la persona, debe advertirse que "*si bien estas figuras no fueron pensadas para la era informática, igualmente la doctrina considera que serían aplicables, en casos como la reproducción o la publicación a través de una página web o vía e-mail*"[27].

Vale decir, resulta aplicable el artículo 113 del C.P.[28], que se refiere particularmente a la publicación o reproducción de calumnias e injurias inferidas por otro.

[27] PIACENZA, Diego Fabio, "Delitos Informáticos", Alfa-Redi: Revista de Derecho Informático, No. 127, Febrero del 2009, publicado en: http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/piacenza_2.pdf, consultado: 27/09/2010.

[28] *"Art. 113. El que publicare o reprodujere, por cualquier medio, injurias o calumnias inferidas por otro, será reprimido como autor de las injurias o calumnias de que se trate, siempre que su contenido no fuera atribuido en forma sustancialmente fiel a la fuente pertinente. En ningún caso configurarán delito de calumnia las expresiones referidas a asuntos de interés público o las que no sean asertivas"*. (Texto conforme Ley 26.551).

El que hubiere incurrido en cualquiera de estas dos acciones típicas, será reprimido como autor de ellas, siempre que su contenido no fuera atribuido en forma sustancialmente fiel a la fuente pertinente.

Tal conclusión, a su vez, es sostenida por la asimilación que, tanto el decreto del P.E.N 1279/1997 como la ley 26.032, hacen respecto de la naturaleza de Internet como medio de comunicación. El tipo penal es amplio en este sentido, pues permite la publicación o reproducción de las calumnias e injurias "por cualquier medio". Creemos que, la responsabilidad penal en este caso deberá recaer sobre el proveedor de contenidos, y en cuanto las calumnias e injurias se encontraren publicadas o reproducidas en páginas propias.

c) Por último, respecto de los distintos tipos penales que se agrupan bajo la "violación de secretos", debe aclararse que, con la sanción de la ley 26.388[29] de delitos informáticos, se incorpora al derecho positivo lo que se venía sosteniendo jurisprudencialmente a partir del *leading case* "Lanata"[30] respecto de la equiparación de la correspondencia electrónica a la correspondencia epistolar. Más adelante se analizará con profundidad el fallo, al tratar el tema del correo electrónico (capítulo V).

Por lo que aquí interesa, debe destacarse que la nueva ley no conforma un cuerpo legal autónomo, sino que incorpora un conjunto de modificaciones al Código Penal. En ese sentido, no crea nuevos delitos sino que agrega nuevos conceptos a categorías ya existentes, ampliando el tipo penal, y, de esta forma, evitando forzadas interpretaciones analógicas.

A continuación, analizaremos brevemente las disposiciones del Código Penal, reformadas por la ley de delitos informáticos, y relacionadas con el derecho a la intimidad:

- *"Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el 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*

Con el agregado de esta ley, se recoge lo que se sostuvo en autos "Campillay, Julio C. c/ La Razón y otros", CSJN (Fallos 308:789), 15/05/1986.

[29] *B.O.* 25-VI-2008.

[30] Martolio, Edgardo H. c. Lanata, Jorge E., Sala IV de la Cámara Nacional de Casación Penal, 12/05/2000.

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.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica. Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena."

Este artículo contiene dos acciones típicas que deben diferenciarse: por un lado, en el primer párrafo, se prevé el delito de violación, apoderamiento y desvío de comunicación electrónica, mientras que, en el segundo párrafo, se describe la figura de intercepción o captación indebida de comunicaciones electrónicas o telecomunicaciones.

Al decir de San Juan, *"el hecho que se explicite que el acceso sea "indebido", refiere a que no se cuente con una expresa autorización para ello. Con esta modificación, de aquí en adelante, ha de prestarse atención, y asegurarse de contar con las debidas autorizaciones (por escrito) siempre que se deba intermediar en la correspondencia electrónica de terceros"*[31].

A ello, agrega el autor que, "indebidamente" también se refiere a que se trata de un delito doloso, es decir, aquel que se comete con pleno conocimiento de los hechos y con ánimo de lesionar un bien jurídico determinado. De ese modo, quien no tenía la finalidad de interceptar o captar un e-mail, sino simplemente filtrar *spam* - por ejemplo -, o que lo ha hecho por descuido o error, no habría actuado dolosamente[32].

- "Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en

[31] SAN JUAN, Andrés, "Comentarios sobre la Ley de Delitos Informáticos", Alfa-Redi: Revista de Derecho Informático, No. 119, Junio del 2008, publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=10653, consultado: 27/09/2010.
[32] Cfr. SAN JUAN, Andrés, *ob. cit.*

perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros."

Se ha optado por incorporar esta figura genérica (conocida como "*hacking*") en la que por "acceso" debe entenderse todo ingreso no consentido, ilegítimo y a sabiendas, a un sistema o dato informático. Decimos que es una figura genérica porque su aplicación se restringe a aquellos supuestos en que no media intención fraudulenta ni voluntad de dañar, limitándose la acción a acceder a un sistema o dato informático que se sabe privado o público de acceso restringido, y del cual no se posee autorización, o bien, si se tiene, resulta insuficiente.

La escala penal se duplica cuando se "*hackean*" sistemas o datos informáticos de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

- "Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el 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."

Se recepta el delito de publicación indebida de una comunicación electrónica.

A los fines de la tipicidad, basta con que el hecho pueda causar perjuicios a terceros, vale decir, es un delito de peligro abstracto. Asimismo, resulta intrascendente, a los fines de la calificación, si el hecho hubiere causado efectivamente un daño; no así a la hora de evaluar la pena en concreto, pues será un parámetro objetivo fundamental para la graduación del monto de la multa.

Por último, se prevé como causa de eximición el hecho de alegar y probar que se actuó con el fin de custodiar un interés público.

- "Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley;

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años."

Este artículo contiene tres acciones típicas que deben diferenciarse: por un lado, en el primer inciso, se prevé el delito de acceso a un banco de datos personales, en el segundo, el delito de revelación de información registrada en un banco de datos personales, y, finalmente, en el tercer inciso, se describe la figura de inserción de datos falsos en un archivo de datos personales (anteriormente regulado en el artículo 117 bis, inc. 1°, incorporado por la Ley de Hábeas Data).

No se producen grandes cambios en estos tipos penales, pues sólo se modifican dos cuestiones: por un lado, en el segundo inciso, se agrega como acción típica el hecho de "proporcionar" ilegítimamente a otro información registrada en un banco de datos personales protegido por ley; y por otro, se traslada el tipo previsto en el 117 bis, inciso 1° como tercer inciso del presente artículo, con la única diferencia que no se requiere que el dato sea falso (se omite tal palabra en la nueva redacción).

C) Ley 11.723[33]: en sus arts. 31 a 35 se protege el derecho a la imagen. El más importante es el primero de ellos: *"Art. 31. - El retrato fotográfico de una persona no puede ser puesto en el comercio sin el consentimiento expreso de la persona misma, y muerta ésta, de su cónyuge e hijos o descendientes directos de éstos, o en su defecto del padre o de la madre. Faltando el cónyuge, los hijos, el padre o la madre, o los descendientes directos de los hijos, la publicación es libre. La persona que haya dado su consentimiento puede revocarlo resarciendo daños y perjuicios. Es libre la publicación del retrato cuando se relacione con fines científicos, didácticos y en general culturales, o con hechos o acontecimientos de interés público o que se hubieren desarrollado en público."*

A pesar de lo señalado con anterioridad respecto de la inclusión de la imagen dentro de la garantía de la intimidad, la jurisprudencia fue todavía más allá, al am-

[33] *B.O.*, 28-IX-1933.

pliar su ámbito de protección y considerarlo un derecho autónomo. Así se dijo que: *"El derecho a la imagen no se identifica con otros derechos personalísimos, tales como el honor o la intimidad, ya que aquél puede verse lesionado sin que sean afectados estos últimos; vale decir que, aunque no cause ningún gravamen a la privacidad, honor o reputación del afectado, la simple exhibición no consentida de la imagen - en el caso, la fotografía de dos menores que se encontraban en la vía pública, en el ámbito de una nota periodística referida a los problemas sociales relacionados con los adolescentes - afecta el derecho que se intenta proteger por medio del art. 31 de la ley 11.723, y genera, por sí sola, un daño moral representado por el disgusto de ver avasallada la propia personalidad"*[34].

Asimismo, en relación al tema de la protección de la imagen y el honor en Internet, resulta de ineludible cita el caso "Da Cunha, Virginia c/ Yahoo de Argentina S.R.L. y Google Inc."[35], relativo a la responsabilidad de los famosos buscadores por la utilización indebida de la imagen de la famosa modelo y cantante. En la sentencia de primera instancia, se condena a los demandados al cese definitivo del uso antijurídico y no autorizado de la imagen de la actora, como así también la eliminación de su imagen y nombre de los sitios de contenido sexual, erótico y pornográfico denunciados y/o a eliminar las vinculaciones de su nombre, imagen y fotografías con esos sitios y actividades, todo ello más una indemnización por daño moral (no así por daño material, pues si bien se invocó correctamente el art. 31 de la ley 11.723, se demandó - incorrectamente - a los buscadores y no a los titulares de las páginas web, que son quienes en realidad utilizan comercialmente la imagen).

D) Ley 23.592[36]: más conocida como ley antidiscriminación, resulta también de aplicación en cuanto las acciones u omisiones discriminatorias menoscaban la dignidad y el honor de la persona. Su artículo 3° establece el siguiente tipo penal: *"Serán reprimidos con prisión de 1 (un) mes a 3 (tres) años los que participaren en una organización o realizaren propaganda basados en ideas o teorías de superioridad de una raza o de un*

[34] S., D. A. y otros c. Editorial Atlántida S.A., Cámara Nacional de Apelaciones en lo Civil, sala E, 25/03/2004.
[35] Da Cunha, Virginia c/ Yahoo de Argentina S.R.L. Y Google Inc. s/ Daños y Perjuicios; Juzgado Nacional de Primera Instancia en lo Civil N° 75, 29/07/2009. Publicado en: http://www.iprofesional.com/notas/85292-Da-Cunha-Virginia-c-Yahoo-de-Argentina-sDanos-y-perjuicios.html, consultado 09/09/2010.
[36] *B.O.*, 05-IX-1988.

grupo de personas de determinada religión, origen étnico o color, que tengan por objeto la justificación o promoción de la discriminación racial o religiosa en cualquier forma. En igual pena incurrirán quienes por cualquier medio alentaren o incitaren a la persecución o el odio contra una persona o grupos de personas a causa de su raza, religión, nacionalidad o ideas políticas".

Indudablemente, vemos que de la amplitud del propio texto legal ("por cualquier medio"), surge con evidencia que las conductas allí descriptas pueden perfectamente llevarse adelante a través de Internet. La red, así, resulta un medio idóneo para la comisión de conductas discriminatorias, pues el anonimato, la falta de un control sobre el contenido de los sitios web, la relativa facilidad para subir comentarios, ideas u opiniones en cualquier página que lo permita, sumado a una vasta audiencia global (entre los que encontramos otras personas que, escudados en la generosa libertad del ciberespacio, "adhieren" a la intolerancia y a la segregación) contribuyen a alentar la persecución o el odio contra una persona o grupos de personas, por motivos raciales, religiosos, étnicos, ideológicos, etc.

E) Ley 25.326: el tema de la Ley de Protección de Datos Personales, y su aplicación a Internet, será tratado en el capítulo IV, al cual remitimos.

F) Otras leyes aplicables: La Ley Nacional de Telecomunicaciones 19.798[37] establece en su artículo 18 que *"la correspondencia de telecomunicaciones es inviolable. Su interceptación solo procederá a requerimiento de juez competente"*, mientras que en el art. 19 explica el significado de dicha inviolabilidad expresando que *"importa la prohibición de abrir, sustraer, interceptar, interferir, cambiar su texto, desviar su curso, publicar, usar, tratar de conocer o facilitar que otra persona que no sea su destinatario conozca la existencia o el contenido de cualquier comunicación confiada a los prestadores del servicio y la de dar ocasión de cometer tales actos*".

Por otro lado, la ley 25.520[38] de Inteligencia Nacional en su artículo 5° establece también este derecho: *"las comunicaciones telefónicas, postales, de telégrafo o facsímil, o cualquier otro sistema de envió de objetos o transmisión de imágenes, voces*

[37] *B.O.*, 23-VIII-1972.
[38] *B.O.*, 06-XII-2001.

o paquetes de datos, así como cualquier tipo de información, archivos, registros y/o documentos privados o de entrada o lectura no autorizada o no accesible al público, son inviolables en todo el ámbito de la República Argentina, excepto cuando mediare orden o dispensa judicial en sentido contrario".

En síntesis, se evidencia una gran cantidad de normas de orden infraconstitucional que tienden a establecer el alcance de las cláusulas constitucionales relativas al derecho a la intimidad. Ahora bien, dada la amplitud en la redacción tanto de las normas constitucionales como infraconstitucionales respecto de las formas de afectación al derecho a la intimidad, debe concluirse que todas las consideraciones anteriormente expuestas resultan plenamente aplicables a Internet como nuevo medio para la intromisión en la vida privada.

CAPÍTULO IV

PRIVACIDAD DE LOS DATOS PERSONALES EN INTERNET

El tema de la privacidad de los datos personales en Internet merece una especial consideración dentro del amplio conjunto de problemas que plantea la red en relación al derecho a la intimidad.

El presente capítulo tiene por objeto analizar las distintas formas de afectación a la privacidad de los datos personales de los usuarios, como así también exponer las principales herramientas jurídicas con las que se cuenta para contrarrestar este problema.

Nos referiremos particularmente a la aplicación de la ley 25.326 a las bases de datos publicadas u obtenidas a partir de la recolección de datos personales en Internet, a la captación y derivación de las comunicaciones en Internet, a las redes sociales como nueva modalidad de poner en riesgo la privacidad, y, por último, trataremos el tema de las "*cookies*" como herramienta de los navegadores de Internet para la recolección de datos personales.

1. LEY 25.326 DE PROTECCIÓN DE DATOS PERSONALES

En esta parte de la obra, estudiaremos lo atinente a la protección de los datos personales efectuada por la ley 25.326[1] (en adelante LPDP). Si bien no se hará un análisis exhaustivo de todas sus normas, pues ello excedería el objeto del presente trabajo, sí se harán breves consideraciones para introducir sus principios generales, las reglas que consideramos específicamente aplicables a Internet, y, por último, trataremos un caso especial, cual es la naturaleza de la dirección IP en el derecho argentino, y sus efectos jurídicos.

[1] *B.O.*, 2-XI-2000.

1.1. PRINCIPIOS GENERALES

Como punto de partida, podemos afirmar que hoy en día el derecho a mantener nuestra vida ajena a la intromisión de terceros se ve atacado de una manera muy distinta a lo que sucedía al momento en que se acuñó el concepto de derecho a la intimidad. En la hora actual, con la irrupción de la informática, no resulta suficiente estar solos para garantizar la intimidad personal, pues ésta puede ser dañada por actos que se realizan a distancia y frecuentemente sin que la persona se entere del mismo, e Internet resulta un medio ideal para la comisión de estas conductas antijurídicas.

Como consecuencia de ello, el concepto y el contenido del derecho a la intimidad han sufrido una evolución significativa, y ha dado lugar al surgimiento de un nuevo derecho fundamental denominado "autodeterminación informativa", que se encuentra estrechamente vinculado con el de la intimidad[2]. Se lo ha definido como "*la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente los almacenados en los medios informáticos*"[3].

Nuestra ley se refiere expresamente a cuál es su objeto de protección: *"Art. 1: La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas."*

Coincidimos con Basterra cuando afirma que "*la ley tutela el derecho a la intimidad, pero no en forma genérica, sino una especie de intimidad: "la intimidad in-*

[2] Cfr. PANDIELLA, Juan Carlos, "El bien jurídico tutelado por el *habeas data*", publicado en: http://www.foroabogadossanjuan.org.ar/Doctrina_Provincial/pandiella.htm, consultado: 30/09/10.
[3] FERNANDEZ DELPECH, Horacio, "Internet: Su problemática jurídica", Editorial Abeledo Perrot, Buenos Aires, p. 280.

formática", lo que implica la autodeterminación informática y, a través de ella, el derecho a la imagen o el propio perfil"[4].

De ello se infiere que el objeto de esta autodeterminación informativa (o también llamada libertad informática, por su mayor vinculación con la libertad individual que con la intimidad) son los datos personales, es decir, *"el conjunto de representaciones de las características identificatorias que tienen las personas o que se les pueden imputar"*[5]. Nuestra ley se refiere a ellos como *"la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"* (art.2). Asimismo, los clasifica en datos públicos (nombre, D.N.I., identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio) y datos privados o íntimos (art. 5 inc. c), y entre estos últimos distingue entre datos sensibles (según el art. 2 son aquellos que *"revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual"*) y datos no sensibles. Los datos sensibles son los que especialmente se protegen, pues se prohíbe su recolección, salvo ciertas excepciones taxativamente previstas en el art. 7[6].

En cuanto a su recolección, los datos deben ser ciertos, adecuados, pertinentes, exactos, actualizados, no excesivos en relación a la finalidad para los que se hubieren obtenido, fácilmente accesibles para su titular (art. 4), y obtenidos mediante su consentimiento libre, expreso e informado, salvo las excepciones previstas en el art. 5[7].

---

[4] BASTERRA, Marcela I. "El *Habeas Data*". En MANILI, Pablo Luis y otros, "Derecho Procesal Constitucional", Editorial Universidad, Buenos Aires, 2005, p. 171.

[5] VANINETTI, Hugo A., "Derecho a la intimidad e Internet", SJA 12/1/2005, Publicado en: http://www.abeledoperrot.com.ar, consultado: 09/09/2010.

[6] *"ARTICULO 7° — (Categoría de datos).*
1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.
3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas."

[7] "*ARTICULO 5° — (Consentimiento).*
1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su con-sentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.

En tanto se cumplan estas condiciones, los datos puede ser recogidos y acumulados, dando lugar a las llamadas "bases o bancos de datos". La ley alcanza a *"todos los archivos, registros, bases de datos u otros medio técnicos de tratamiento de datos, sean estos públicos o privados, destinados a dar informes".* Vale decir, sólo excluye a aquellos que sean de uso personal (art. 1 D.R. 1558/2001[8]).

Asimismo, las bases de datos se clasifican en públicas y privadas (según la naturaleza de la personalidad jurídica del titular), y en lícitas e ilícitas (según esté o no registrada ante la Dirección Nacional de Protección de Datos Personales).

En lo relativo a los derechos del titular de los datos, éste pueden solicitar - gratuitamente (art. 19) - información al organismo de control sobre la existencia de los archivos o registros con sus datos, identidad de los responsables y finalidad (art. 13), pueden acceder a modo de consulta a cada una de las bases de datos (art. 14), y por último, tienen la facultad de rectificar, actualizar, y cuando corresponda, suprimir o someter a confidencialidad sus datos personales (art. 16), salvo en los casos excepcionales previstos por el artículo 17[9]. Cabe aclarar que, para ejercer los dere-

El referido consentimiento prestado con otras declaraciones, deberá figurar en forma ex-presa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.

2. No será necesario el consentimiento cuando:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526."

[8] *B.O.* 3-XII-2001.

"ARTICULO 1°.- A los efectos de esta reglamentación, quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito".

[9] "*ARTICULO 17. — (Excepciones).*

1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa".

chos otorgados por los artículos 14 y 16, se prevé una instancia extrajudicial obligatoria[10] a la interposición de la acción de protección de datos personales o *habeas data*.

Como contrapartida a los derechos de los titulares de los datos, los responsables de las bases de datos tienen la obligación de suministrar la información solicitada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen; asimismo, esa información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales; y, finalmente, la información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin (art. 15).

El incumplimiento de ésta y otras obligaciones de los titulares de bases de datos (las exigidas en materia de consentimiento de los arts. 4, 5 y 6; y las que surgen de los arts. 8, 9 y 10 referidas a medidas técnicas y organizativas tendientes a garantizar la seguridad y confidencialidad de los datos personales) acarrean sanciones administrativas (art. 31) y penales (art. 32).

Por último, en relación al trámite de la acción de *habeas data,* ya se dijo que, el artículo 43 de la Constitución Nacional introduce este instituto como una subespecie de amparo. Incluso la propia LPDP sostiene que la acción tramitará según el procedimiento que corresponde a la acción de amparo común, y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo (art. 37).

Sin embargo, la ley contiene una serie de disposiciones que intentan reglamentar el trámite y otros aspectos procesales de manera particular (art. 38 a 43). Entre los aspectos más importantes, debe destacarse que tanto el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado, como así también los representantes legales o apoderados de las personas de existencia ideal

[10] Esta instancia se cuestiona de inconstitucionalidad porque el legislador no puede ampliar los recaudos exigidos por el constituyente, o en su caso, si se acepta la constitucionalidad, se critican por excesivos los plazos para interponer la acción, que son de 10 y 5 días desde que se agota la instancia previa.

(art. 34) podrán interponer la acción en contra de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes (art. 35) en los casos previstos en el art. 33, en concordancia con lo dispuesto por el artículo 43 C.N., reconociéndose así los distintos tipos de *habeas data*, a saber:

"a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos (Habeas data informativo*);*

b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación (Habeas data rectificador*), supresión (Habeas data* cancelatorio*), confidencialidad (Habeas data* reservador*), o actualización (Habeas data* aditivo*)."*

1.2. REGLAS ESPECÍFICAS PARA INTERNET

Deben hacerse algunas aclaraciones respecto de ciertas exigencias o expresiones previstas en la ley 25.326, que pueden ser útiles como lineamientos rectores en la aplicación de la misma a Internet:

- Los principios de la LPDP son aplicables a los archivos, registros o bancos de datos publicados u obtenidos a partir de la recolección de datos personales en Internet, ya que la norma se refiere a los *"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).

- Como principio general, en Internet debe preferirse el mantenimiento del anonimato, salvo que exista una causa legítima para la solicitud de datos personales[11].

- En materia de consentimiento, se considerará cumplido este requisito previo cuando el titular del dato acepte la política de privacidad publicada en el sitio de

[11] Es lo que Brenna (*ob. cit.*, p.23) llama "principio de minimización de los datos".

Internet a través del cual se recolecten sus datos (suelen conocerse bajo el nombre de "Términos de uso" o "Política de privacidad")[12].

- Deberá informarse si la página web utiliza *"cookies"* para la recolección de datos; de ser así, deberá también informarse qué datos van a ser almacenados, con qué objeto, y, en todo caso, deberá informarse la identidad del titular de la base de datos (en el punto 3.2 se analizará el tema en profundidad).

- Se entiende que la expresión "fuentes de acceso público irrestricto" (art. 5 inc. 2), incluye las publicaciones efectuadas a través de Internet sólo en páginas web públicas y oficiales[13] (caso en el cual se exceptúa de la necesidad del consentimiento).

- Si la recolección de datos se realiza mediante cuestionarios, formularios, encuestas o similares impresos o incluidos en un sitio de Internet, éstos deberían contener, en un lugar visible y de modo claro, la información exigida por el art. 6[14].

- En materia de jurisdicción y competencia, se ha dicho: *"El art. 36 inc. b) de la ley establece que procederá la competencia federal cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales. Por su parte, el art. 44, último párrafo de la referida norma, reserva la jurisdicción federal respecto a los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional. Por ende, si la información que se pretende suprimir fue proporcionada por Internet, que constituye una red*

[12] Esta fórmula está consagrada en el art. 5 de la Ley 1.845 de protección de datos personales de la Ciudad de Buenos Aires (*B.O.* C.B.A. Nº 2494 del 03-08-2006). *De lege ferenda*, creemos que la normativa nacional debería incluir expresamente una norma similar en su reglamentación; o bien podría incluirse a través de alguna resolución del órgano de contralor (vgr. Dirección Nacional de Protección de Datos Personales).

[13] Así lo dispone el art. 3 del anexo del decreto 725/07 (*B.O.* (C.B.A.) Nº 2691 del 24/05/07.), que reglamenta la Ley 1.845 citada recientemente. Puede consultarse el texto de ambas normas en: http://www.protecciondedatos.com.ar/legislacion.htm, consultado: 17/10/2010.

[14] "*Art. 6.- Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:*
a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;
b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;
c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;
d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos."

interconectada a la que se refiere el art. 44 citado, es claro que deben intervenir en la controversia los jueces federales con competencia Civil y Comercial"[15].

- La gran mayoría del correo electrónico no deseado (*spam*) proviene de bases de datos (de correos electrónicos) ilegales, pues no sólo no cumplen con el requisito del consentimiento previo (art. 5), sino que tampoco se encuentran registrados ante el órgano de contralor (art. 3). Por esto último, tampoco cumplen los *spammers* con su obligación de identificarse, ni con la de precisar la finalidad para la cual se requieren las direcciones de e-mail (art. 13). Más adelante volveremos sobre el tema (ver cap. V).

- Se acepta pacíficamente que la dirección de correo electrónico es un dato personal, más específicamente un dato personal privado no sensible (de acuerdo a la clasificación que se infiere de la LPDP), mientras que se encuentra ampliamente discutido si la dirección IP es un dato personal o no. A continuación trataremos esta cuestión.

1.3. ¿ES LA DIRECCIÓN IP UN DATO PERSONAL?

Un párrafo aparte entre las consideraciones que recientemente enunciamos merece la discusión acerca de la naturaleza jurídica de la dirección IP[16]. Al respecto, entendemos que hay dos posiciones: por un lado, se afirma que no es un dato de carácter personal, y, por otro lado, se sostiene que es un dato personal privado, y paradójicamente público en algunos casos.

[15] Svatzky, Betina L. c/ Datos Virtuales S.A. s/ Habeas Data. C.N.Civil, Sala G, 28/04/04. El mismo criterio ha sido ratificado por la Corte Suprema, el 30/12/04, en los mismos autos de referencia. Puede consultarse el texto del fallo en: http://www.jus.gov.ar/scripts/dnpdp-jurisprudencia/im_verpag.asp?ID=161, consultado: 04/10/2010.

[16] Según Fernández Delpech (*ob. cit.*, págs. 20 y 21), las direcciones IP son números de identificación único e irrepetible que se le asigna a un ordenador que se conecta a la red Internet, a los fines de permitir su reconocimiento por las demás computadoras. Las direcciones IP constan de números y letras separadas por puntos, y son asignadas por la ICANN (Corporación de Internet para la Asignación de Nombres y Números de Dominios), a través de distintos registros regionales (LACNIC es el registro que asigna direcciones IP para Latinoamérica y el Caribe).

La primera postura, sostenida por el gigante Google[17], y por algunas decisiones de tribunales franceses[18], entiende que las IP en ningún caso constituyen datos personales, pues en realidad no identifican usuarios sino ordenadores.

Esto, a su vez, trae dos consecuencias en el plano jurídico: por un lado, la no aplicación para ningún caso de la tutela de las leyes de datos personales; por otro, implica la irresponsabilidad de quienes a través de la red cometen conductas antijurídicas. Se argumenta esta conclusión a partir del siguiente razonamiento: si la IP es fija, no resulta suficiente para imputar responsabilidad a una determinada persona, pues la computadora pudo haber sido utilizada por distintos usuarios; en caso de ser variable o dinámica, la mentada imputación de responsabilidad resulta aún más absurda, pues esa IP ha sido y es permanentemente asignada a distintos ordenadores, y por ende a distintos usuarios.

La segunda tesitura, sostenida principalmente por la Unión Europea (a través del Grupo sobre Protección de Datos del Artículo 29[19]) y la Agencia Española de Protección de Datos (AEPD[20]), entiende que las direcciones IP son datos personales

[17] Un interesante artículo del diario "El País" refleja la posición del buscador en relación al tema: http://www.elpais.com/articulo/internet/Google/contrario/considerar/direcciones/IP/dato/personal/elpeputec/20080529elpepunet_3/Tes, consultado: 03/10/2010.
Asimismo, desde el propio seno de Google, y a través de un blog oficial del famoso buscador, se ha dicho que: *"La dirección IP de un usuario no puede ser considerada como un dato personal porque los sitios web que los almacenan (entre ellos Google) no pueden identificar a la persona que hay detrás de los cuatro números de ese dato.*
En algunos contextos quizá sí. Si eres un proveedor de Internet, y asignas una dirección IP a un determinado cliente, y sabes su nombre y su dirección postal, entonces sí que podría ser considerado como un dato personal, incluso cuando sabes que varias personas pueden compartir esa dirección IP. En la mayoría de los casos (excepto los sitios web de los proveedores de Internet), los sitios web no pueden considerar ese dato como información personal si no tienen más variables que lo puedan identificar".
El artículo completo está publicado en inglés en: http://googlepublicpolicy.blogspot.com/2008/02/are-ip-addresses-personal.html, consultado: 03/10/2010.
[18] Los dos casos que se pronuncian en igual sentido son: "Anthony G. c/ Société Civile des Producteurs Phonographiques", Tribunal de Apelación de París, Sala 13, Sección B Sentencia de 27 de abril 2007; y, "Henri S. c/ Société Civile des Producteurs Phonographiques", Tribunal de Apelación de París, Sala 13, Sección A, Sentencia del 15 de mayo 2007. Ambas sentencias publicadas en francés en: http://www.legalis.net/jurisprudence-decision.php3?id_article=1954, y http://www.legalis.net/jurisprudence-decision.php3?id_article=1955, respectivamente, consultadas: 03/10/2010.
[19] Este Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE (de protección de las personas frente al tratamiento de sus datos personales y de la libre circulación de estos datos). Es un órgano consultivo europeo independiente que se ocupa de la protección de datos y la intimidad. En su Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda, emitido el 4 de abril de 2008, deja bien en claro la posición adoptada por la UE: *"el proveedor de servicios de Internet* (el dictamen se refiere a los buscadores) *tendrá que tratar toda información IP como datos personales, a menos que sepa con absoluta certeza que los datos corresponden a usuarios que no pueden ser identificados"*.
[20] La AEPD a través de su informe 327/2003entiende que *"aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, desde esta Agencia de*

privados, pues si bien identifican computadoras, permiten, a través de técnicas de rastreo informático, la identificación del usuario con un alto grado de certeza. Si bien se reconoce que, aún en caso de direcciones IP dinámicas resulte difícil la identificación del usuario, ello no es técnicamente imposible; por ello, la sola posibilidad - aunque sea mínima - de identificar a una persona, lo convierte en un dato personal.

Ello tiene dos consecuencias en el plano jurídico: por un lado, implicaría la aplicación de las leyes de datos personales, con todos los derechos y garantías que le corresponda al usuario; por otro lado, significaría la posibilidad de imputar responsabilidades legales, siempre y cuando el dato (IP) se hubiere obtenido legalmente.

En el mismo sentido se ha pronunciado la Corte Suprema Federal Suiza, cuando al referirse sobre la legalidad o ilegalidad de la actividad de una empresa (*Logistep*), que consistía en la recolección de direcciones IP para un posterior rastreo privado de presuntos infractores a las leyes de derecho de autor, consideró que la obtención de la identidad del titular de una dirección IP sólo podía hacerse legítimamente en el marco de una investigación penal, y no de manera privada[21]. De ello, se infiere que, para la Corte Suiza, la IP es claramente un dato personal, y que el derecho a la intimidad está incluso por encima de los derechos de autor (por más que el fin de la empresa sea el rastreo informático de infractores, el medio (la recolección de IPs sin orden judicial), resulta insuficiente para justificar tal fin)[22].

Sin embargo, Prenafeta advierte que el principio no es absoluto, y que admite una importante excepción en el supuesto de las redes P2P. Es decir, en los casos en que se utilizan programas para el intercambio de archivos de persona a persona (como *Ares, KaZaA, E-Mule o BitTorrent*), las direcciones IP son datos públicos, pues el acceso a esta información está a la vista del resto de los usuarios (quien al usar el

Protección de Datos se parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos". Puede consultarse en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf, consultado: 03/10/2010.

[21] Puede consultarse en el diario "El País", en: http://www.elpais.com/articulo/tecnologia/Suiza/declara/ilegal/actividad/empresa/dedicada/cazar/descargas/P2P/elpeputec/20100908elpeputec_6/Tes, consultado: 03/10/2010.

[22] Un resumen del fallo en inglés, también puede verse en: http://www.edoeb.admin.ch/aktuell/01688.index.html?lang=en, consultado: 03/10/2010.

programa manifiesta su voluntad de exhibir su IP), y por ende puede ser consultada por cualquiera que esté conectado a esa red[23]. En este sentido se ha pronunciado el Tribunal Supremo Español en su sentencia 236/2008[24], cuando al referirse sobre la nulidad de una investigación policial sobre un delito de facilitación de material de pornografía infantil que se basó en un rastreo informático a partir de la dirección IP de la acusada (obtenida sin autorización judicial), sostuvo que *"quien utiliza un programa P2P [...] asume que muchos de los datos se convierten en públicos para los usuarios de Internet, circunstancia que conocen o deben conocer los internautas, y tales datos conocidos por la policía, datos públicos en Internet, no se hallaban protegidos por el art. 18-1º ni por el 18-3 C.E.* (el artículo 18 protege los datos personales en la Constitución Española)."

En este singular caso - el de las redes P2P -, la consecuencia resulta de trascendencia jurídica, pues implica que las IP estarían excluidas de la tutela de las leyes sobre datos personales.

En nuestro país, este debate aún no se ha planteado a nivel jurisprudencial ni doctrinario como si efectivamente ha sido discutido, con más vacilaciones que certezas, en la Unión Europea y en EE.UU. Sin embargo, consideramos de fundamental importancia que tenga lugar en el derecho argentino, y que se tengan en cuenta los lineamientos expuestos en la segunda postura. Pensamos que los argumentos seguidos por la Agencia Española de Protección de Datos y la Unión Europea son correctos, pues son los que más se ajustan a los principios de la ley 25.236, que define a los datos personales de manera casi idéntica a la ley española y a la Directiva 95/46/CE[25], ambos antecedentes claves a la hora de adoptar un modelo para nuestra legislación.

---

[23] Cfr. PRENAFETA, Javier, "Protección de datos y secreto de las comunicaciones en las redes P2P", publicado en: http://www.jprenafeta.com/2008/06/06/proteccion-de-datos-y-secreto-de-las-comunicaciones-en-las-redes-p2p, consultado: 09/09/2010.

[24] Tribunal Supremo Sala II de lo Penal. Sentencia 236/2008, del 9 de mayo. Puede encontrarse el fallo completo en: http://sentencias.juridicas.com/docs/00286723.html, consultado el 03/10/2010.

[25] Nuestra ley define a los datos personales en su artículo 2 como *"Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"*, la Ley Orgánica de Protección de Datos de Carácter Personal de España los define en su artículo 3 como *"cualquier información concerniente a personas físicas identificadas o identificables*"; por último, la Directiva 95/46/CE, en su art. 2 inc. a) los define como "*toda información sobre una persona física idientificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social*".

2. CAPTACIÓN Y DERIVACIÓN DE LAS COMUNICACIONES EN INTERNET

Un tema íntimamente vinculado con el derecho a la intimidad es el de la captación y derivación de las telecomunicaciones. A continuación, se analizará la cuestión desde la perspectiva del derecho nacional, pero sin perder de vista la legislación comunitaria europea y la legislación federal de los EE.UU., las cuales han sido pioneras en el ámbito internacional.

2.1. LA SITUACIÓN EN EL DERECHO COMPARADO

No es redundante afirmar que el mundo ha cambiado a partir de los atentados del 11 de septiembre de 2001. En materia de privacidad, se ha destacado un profundo cambio en las políticas destinadas a la protección de las telecomunicaciones, motivado por la necesidad de combatir un nuevo "enemigo": el terrorismo global.

En este marco, en los Estados Unidos, y a un mes de los atentados, se ha dictado la *USA Patriot Act*[26], que dispone un conjunto de medidas tendientes a investigar, prevenir y eliminar las actividades terroristas. Al decir de Grün, esta ley *"contiene numerosas previsiones y enmiendas a leyes y disposiciones vigentes que según expertos en derecho y representantes de organizaciones de derechos civiles norteamericanas son anticonstitucionales y constituyen un grave obstáculo para el desarrollo de las actividades asociativas y un ataque contra las libertades civiles dentro y fuera de los Estados Unidos, bajo el pretexto de garantizar la seguridad nacional"*[27].

Entre los puntos oscuros de la ley, se cuestionan las facultades otorgadas a los organismos de investigación e inteligencia del gobierno federal (vgr. FBI y CIA) a interferir comunicaciones electrónicas siempre que se trate de motivos de seguridad nacional, pues para tal intervención basta sólo con alegar que dichos datos son relevantes para una investigación en curso. Asimismo, impone a los proveedores de

[26] Promulgada el 26 de Octubre de 2001 y promulgada el 2 de marzo de 2006, el nombre completo de la ley es *"Uniting and Strenghtening America by Providing Appropiate Tools Required to Intercept and Obstruct Terrorism"*. De sus iniciales se forma "USA PATRIOT".

[27] GRÜN, "Una visión sistémica y cibernética del derecho en el mundo globalizado del siglo XXI", Ed. Lexis Nexis, 2005, págs. 183 y 184.

telecomunicaciones (en nuestro caso a los proveedores de servicio de Internet o ISP) a guardar datos de tráfico y de contenido de sus usuarios[28].

No dudamos en sostener que coincidimos con los objetivos de resguardar la seguridad y la lucha contra el terrorismo, pero también creemos que tal fin no debe alcanzarse a cualquier precio, y mucho menos a expensas del derecho a la intimidad, a la protección de los datos personales y al secreto de las comunicaciones.

Una situación similar a la apuntada, también se vivió en Europa. Luego de los atentados de Madrid y Londres en 2004 y 2005 respectivamente, se dictó la directiva 06/24/CE "Sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones"[29]. Debemos recordar que esta directiva modifica el régimen de protección de la privacidad de las telecomunicaciones establecido en la directiva 02/58/CE[30] (en sus arts. 5, 6 y 9), el cual, a su vez, se basa en la directiva 95/46/CE[31], que establece un régimen general de protección de datos personales, y que las disposiciones y principios de ambas resultan plenamente aplicables.

Su artículo 1°, inc. 1 aclara que su objeto es *"armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro."*

Como surge de su objeto, al igual que la *Patriot Act* norteamericana, no sólo se enrola dentro de la lucha contra el terrorismo, sino que además comete el mismo error en cuanto, al imponer a los proveedores de servicio la obligación de conservar los datos de tráfico y localización de los usuarios, se están - cuanto menos- poniendo en riesgo los principios de confidencialidad de las comunicaciones, el de elimina-

[28] Cfr. UICICH, Rodolfo D., "El derecho a la intimidad en Internet y en las comunicaciones electrónicas", Editorial Ad Hoc, Buenos Aires, 2009, p. 117.
[29] Publicada en el Boletín Oficial de la Unión Europea el 13/04/2006.
[30] Directiva "relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas". Publicada en el Boletín Oficial de la Unión Europea el 31/07/2002.
[31] Directiva "relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos". Publicada en el Boletín Oficial de la Unión Europea el 23/11/1995.

ción de los datos de tráfico, y el de anonimato de los datos de localización (consagrados en los arts. 5, 6 y 9 respectivamente de la Directiva 02/58/CE)[32].

Finalmente, para completar este breve panorama en el derecho comparado, cabe simplemente destacar que muchos países europeos han dictado normas que se compadecen con el espíritu de esta directiva (Ley 25/2007 de España, Decreto Legislativo 109/2008 de Italia, Decreto 2006-358 de Francia, la *Data Retention (EC Directive) Regulations* 2009 del Reino Unido, entre otras leyes), y otros que aún no han legislado el tema (Irlanda, Grecia, Austria y Suecia)[33].

2.2. LA SITUACIÓN EN LA LEGISLACIÓN ARGENTINA: LEY 25.873

Nuestro país no se ha mantenido al margen de esta tendencia de intentar regular la captación y derivación de las telecomunicaciones. Es por ello que se ha dictado la polémica ley 25.873[34] (reglamentada por el decreto 1563/2004[35]), modificatoria de la ley de telecomunicaciones 19.798. En ella, básicamente, se regularon tres aspectos diferentes: a) la obligación de toda empresa de telecomunicaciones de colaborar con una investigación en la justicia y en concreto con los pedidos de informes; b) la obligación de retener ciertos datos de tráfico en materia de comunicaciones por el plazo de 10 años; y c) la responsabilidad del Estado por los daños que esta actividad pueda ocasionar.

A continuación, procederemos al análisis de los tres artículos de la ley, enfocándonos en su aplicación a los proveedores de servicio de Internet:

Art. 1º — Incorpórase el artículo 45 bis a la Ley 19.798 con el siguiente texto:

"Todo prestador de servicios de telecomunicaciones deberá disponer de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que

[32] Cfr. UICICH, Rodolfo D., *ob. cit.*, p. 126.
[33] Para el listado completo de medidas nacionales de ejecución de la directiva 2006/24/CE, ver: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72006L0024:ES:NOT#FIELD_UK, consultado: 03/10/2010.
[34] *B.O.* 09-II-2004.
[35] *B.O.* 09-XI-2004. Debe resaltarse que, si bien a través del dictado del decreto 357/2005 se suspendió la aplicación del dec. 1563/2004 a los fines de "permitir un nuevo análisis del tema y de las consecuencias que el mismo implica", tal cual reza uno de sus considerandos, en rigor, la ley sigue vigente, pues no se ha dictado una ley que derogue o que, respetando las garantías constitucionales afectadas, la reemplace.

transmiten, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente.

Los prestadores de servicios de telecomunicaciones deberán soportar los costos derivados de dicha obligación y dar inmediato cumplimiento a la misma a toda hora y todos los días del año.

El Poder Ejecutivo nacional reglamentará las condiciones técnicas y de seguridad que deberán cumplir los prestadores de servicios de telecomunicaciones con relación a la captación y derivación de las comunicaciones para su observación remota por parte del Poder Judicial o el Ministerio Público."

Es importante destacar que las obligaciones que impone este primer artículo no sólo están restringidas a los prestadores de telefonía o servicios de voz, ya sea telefonía fija o móvil (si bien esta normativa fue dictada teniendo en cuenta específicamente a estos sujetos, y de hecho se conoce como "ley de escuchas"), sino que están referidas a los prestadores de telecomunicaciones en general. A tal fin, es menester recordar que ley 19.798 define como telecomunicación a "*toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos*" (art. 2). El decreto 1563/04 (reglamentario de la ley 25.873), se pronuncia en el mismo sentido (art. 1).

De tal definición, se infiere que la obligación en cuestión es de plena aplicación a los proveedores de servicio de Internet. Así lo entiende Fernández Delpech, quien llega a tal conclusión a partir de los siguientes argumentos: "*a) que la ley 19.798 a que se refiere es la Ley Nacional de Telecomunicaciones, b) que el Dec. 764/2000 que aprobó el Reglamento de Licencias para Servicios de Telecomunicaciones estableció la existencia de una licencia única para la prestación de los servicios de telecomunicaciones. Destacando que en los considerandos del decreto se expresa: "Que el anterior régimen establecía divisiones de servicios que no se correspondían con la evolución real de su prestación en el mundo, observándose, por ejemplo, que se establecían distingos entre el servicio telefónico, los servicios de telecomunicaciones- excepto telefonía- y los servicios de valor agregado. Que dichas distinciones no responden a tendencias cada vez más actuales toda vez que poco a poco Internet podría transfor-*

marse en servicio básico y configurar la red básica, absorbiendo en su prestación a los demás servicios de datos y de telefonía en un periodo relativamente corto" c) Que la Guía orientativa para la solicitud de licencias de la Comisión Nacional de Comunicaciones contempla el otorgamiento de una licencia única que habilita al prestador a brindar al público todo servicio de telecomunicaciones. En su Capítulo III y dentro de la Guía de contenidos de planes técnicos, contempla expresamente el acceso a Internet y los servicios de valor agregado"[36].

En cuanto al segundo párrafo, entendemos que la obligación de cargar con los costos de los recursos humanos y tecnológicos de un sistema de captación y derivación de las comunicaciones afecta el derecho de propiedad e igualdad de los prestadores de telecomunicaciones. Resulta injusto y contrario a las garantías constitucionales de los arts. 16 y 17 de la C.N. que el Estado haga recaer los costos de una política pública tendiente al bienestar general (la lucha contra la delincuencia) sobre un sector en particular (los prestadores de servicios de telecomunicaciones)[37].

Finalmente, el párrafo tercero se limita a establecer que será tarea del Poder Ejecutivo reglamentar las condiciones técnicas y de seguridad que deberán cumplir los prestadores de servicios de telecomunicaciones con relación a la captación y derivación de las comunicaciones para su observación remota por parte del Poder Judicial o el Ministerio Publico; cuestión que fue resuelta en el decreto 1563/2004, art. 2 Incisos B), E), I) y J).

Art. 2° — Incorpórase el artículo 45 ter a la Ley 19.798 con el siguiente texto:

"Los prestadores de servicios de telecomunicaciones deberán registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente. La información referida en el presente deberá ser conservada por los prestadores de servicios de telecomunicaciones por el plazo de diez años."

[36] FERNANDEZ DELPECH, Horacio, *ob. cit.*, p. 215 y 216.
[37] Cfr. VIEGENER, Federico, "El derecho a la Intimidad y los límites a la injerencia estatal", Alfa-Redi: Revista de Derecho Informático No. 116, Marzo del 2008, publicado en: http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/viegener.pdf, consultado: 04/10/2010.

El hecho de que este artículo disponga la obligación de almacenar datos referentes a las telecomunicaciones puede generar polémica y hasta cierto temor por parte de los usuarios, quienes ven su intimidad seriamente amenazada. Sin embargo, para poder llegar a un real entendimiento de la cuestión, resulta necesario referirnos a dos aspectos: A) qué datos serán objeto de almacenamiento por los prestadores, y B) el plazo de guarda de los mismos.

A) Respecto de la información que debe ser almacenada, se incluye a los datos filiatorios y domiciliarios de los usuarios y clientes, como así también a los datos de tráfico de las comunicaciones cursadas[38].

En cuanto a los datos filiatorios y domiciliarios, y particularmente con respecto a las comunicaciones cursadas por Internet, es factible señalar dos factores que pueden perjudicar la medida de retención: por un lado, la gran cantidad de *cybers* que brindan acceso al público en general a Internet, y por otro lado, la tecnología de Internet inalámbrico o *Wi-Fi*[39].

La información que debe ser conservada es uno de los puntos más oscuros de la ley, ya que se presta a confusiones si el alcance de dicha obligación se refiere a datos de tráfico o bien de contenido[40]. Igualmente, la distinción entre ambos conceptos resulta prácticamente inútil en el caso de Internet, ya que los datos de tráfico permiten conocer cada uno de los sitios que el usuario visita, el tiempo de cada visita, su dirección IP, el contenido y el interlocutor con el que el usuario establece una comunicación por chat, por correo electrónico o por las redes sociales, etc.[41]

En relación a los datos de tráfico, la ley no define qué debe entenderse por tales. Tampoco lo hace el decreto 1563/2004; por el contrario, la reglamentación amplía el objeto de aplicación de la ley a "la ubicación geográfica del abonado" y a

[38] Creemos que por "comunicaciones cursadas por los usuarios", debe entenderse toda comunicación que se transmite a través de Internet, entre las que se incluyen no sólo las del servicio de correo electrónico sino también las del servicio de mensajería instantánea, los chats, los mensajes que se envían por las redes sociales, las comunicaciones por telefonía IP, el intercambio de archivos con otros usuarios, los sitios Web visitados, etc.

[39] Mediante la misma, cualquier persona con una computadora portátil o celular, puede ingresar a Internet, sin identificarse, simplemente estando dentro de la zona de cobertura del servidor Wi-Fi (generalmente ubicado en universidades, bares, aeropuertos, shoppings, hoteles, etc.).

[40] Los datos de tráfico, son los referidos solamente a la fecha en que se produjo el envío o remisión del correo electrónico, duración de la conexión, el número e identificación de los equipos de origen y destino de las comunicaciones. Mientras que los datos de contenido serían la información específica objeto de la transmisión, como ejemplo de ello, los archivos adjuntos que se envían, el mensaje en sí, etc.

[41] Cfr. UICICH, *ob. cit.*, p. 134.

"la demás información asociada a las telecomunicaciones" (art. 3 inc. a y d). Creemos que es uno de los puntos de la ley que debiera aclararse cuanto antes, y para ello, debería tomarse como modelo el art. 5 de la directiva europea 2006/24/CE[42].

B) Por último, respecto del tiempo de conservación de los datos retenidos, la ley estipula un plazo de 10 años. Creemos que es excesivo, sobre todo si tenemos en cuenta que, por ejemplo quintuplica al plazo máximo establecido por la directiva 06/24/CE, que fija el plazo de conservación en un período entre 6 y 24 meses. A su vez, este extenso plazo incide directamente en el costo de tecnología que los ISP deben incurrir a los fines de la conservación de los mismos, y que no dudamos es inconstitucional.

Art. 3° — Incorpórase el artículo 45 quáter a la Ley 19.798 con el siguiente texto:

"El Estado nacional asume la responsabilidad por los eventuales daños y perjuicios que pudieran derivar para terceros, de la observación remota de las comunicaciones y de la utilización de la información de los datos filiatorios y domiciliarios y tráfico de comunicaciones de clientes y usuarios, provista por los prestadores de servicios de telecomunicaciones".

En la interpretación de este artículo, coincidimos con Viegener en que *"la deficiente redacción del precepto no puede derivar, en entender que se ha pretendido "socializar" - con cargo al Tesoro Público - las consecuencias patrimoniales que pudieran derivarse de los daños causados a terceros por el hecho propio de las empresas de telecomunicaciones, responsabilidad ésta respecto a la cual la ley nada innova y que, por lo tanto, sólo será enjuiciable por el Poder Judicial de la Nación bajo el prisma de las normas y principios que rigen la responsabilidad civil"*[43].

Es decir, lejos de introducir una solidaridad legal o un principio especial de responsabilidad, la norma termina siendo redundante, pues no hace más que repetir un principio harto conocido, cual es el de responsabilidad del Estado por el funcio-

[42] El artículo 5 se encarga de establecer en forma detallada las categorías de datos que deben conservarse, instituyéndose que serán los datos necesarios para: 1) rastrear e identificar el origen de una comunicación; 2) identificar el destino de una comunicación; 3) identificar la fecha, hora y duración de una comunicación; 4) identificar el tipo de comunicación; 5) identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación; 6) identificar la localización del equipo de comunicación móvil. Conjuntamente, dentro de cada de uno de los subgrupos de datos, se hace referencia precisa a su significado con respecto a la telefonía fija y móvil, acceso a Internet, Correo Electrónico y telefonía por Internet.

[43] VIEGENER, Federico, *ob. cit.* p.60.

namiento irregular o defectuoso de su función administrativa (resulta de aplicación subsidiaria el art. 1112 del Código Civil).

Por último, en relación al tema, no debe dejar de resaltarse que más allá de que se reconozca la responsabilidad del Estado, los daños en materia de intromisión en la privacidad adquieren el carácter de irreparables, por ser la producción del mismo irreversible y su reparación insuficiente[44].

2.3. LA LEY 25.873 EN LA JURISPRUDENCIA NACIONAL

La Corte Suprema ha analizado la constitucionalidad de la ley 25.873 y del decreto 1563/2004, en el caso "Halabi"[45], vale decir, si la obligación de conservar datos por parte de los ISP afecta o no el derecho a la intimidad. Para ello, ha considerado los siguientes aspectos, a saber:

- La normativa en crisis es violatoria de los arts. 18 y 19 CN, pues no determina en qué casos y con qué justificativos se autoriza la intervención de las comunicaciones.

- La ley y el decreto, asimismo, resultan contrarios a la Ley de Protección de Datos Personales, y consecuentemente al art. 43 C.N., en cuanto ignora los principios de seguridad y confidencialidad de los datos que están siendo registrados y/o derivados.

- No existió un debate legislativo suficiente previo al dictado de la ley, la cual carece de motivación y fundamentación apropiada. Asimismo, no se dan las causas suficientes en la realidad argentina para limitar de tal forma los derechos de los usuarios de Internet, como sí en otras naciones afectadas por el terrorismo global y que han dictado normas similares.

---

[44] Cfr. UICICH, Rodolfo D., *ob. cit.*, p. 135.

[45] Halabi, Ernesto c/ P.E.N. s/Amparo, CSJN, 24/02/2009. Puede consultarse el texto del fallo en: http://www.csjn.gov.ar/cfal/fallos/cfal3/ver_fallos.jsp, consultado 02/10/2010.
Cabe aclarar que, con anterioridad, ya la Sala I de la Cámara Nacional en lo Contencioso Administrativo Federal se había pronunciado respecto de la inconstitucionalidad del decreto reglamentario en autos "Cámara Argentina de Bases de Datos y Servicios en Línea c. Estado Nacional s/Amparo", en un fallo del 11/07/2006.

- No se han tomado las mismas precauciones que sí han sido tenidas en cuenta en el derecho comparado a los fines de evitar violaciones al derecho a la intimidad.

- Las normas exhiben gran vaguedad pues de sus previsiones no queda claro en qué medida pueden los proveedores captar el contenido de las comunicaciones sin autorización judicial. En relación a Internet, la CSJN ha sostenido que las previsiones de la norma *"no distinguen ni precisan de modo suficiente las oportunidades ni las situaciones en las que operarán las interceptaciones, toda vez que no especifican el tratamiento del tráfico de información de Internet en cuyo contexto es indiscutible que los datos de navegación anudan a los contenidos"* (considerando 26 del voto mayoritario).

- Las normas están redactadas de tal manera que crean el riesgo de que los datos captados sean utilizados para fines distintos de los que ella prevé.

- El Poder Ejecutivo se extralimita en su facultad de reglamentación, pues el decreto 1563/2004 amplía aún más las potestades de intervención, al extender los sujetos a quienes se le aplica la ley (art. 2 inc. f), y la información objeto de la misma (art. 3), entre la que se encuentra por ejemplo la ubicación geográfica, datos contractuales, y demás datos de los usuarios.

- No se respeta el principio de razonabilidad, vale decir, el medio utilizado (restricción a la privacidad) es desproporcionado respecto del objeto que se pretende tutelar (no se sabe bien por carecer de exposición de motivos, pero aparentemente sería la seguridad interna, la defensa nacional, o la investigación penal. En "Halabi", se hace referencia al objetivo general de "combatir el flagelo de la delincuencia").

- La ley en crisis causa una lesión a una pluralidad relevante de derechos individuales (se afecta a la privacidad e intimidad en su faz de derecho de incidencia colectiva referente a un interés individual homogéneo). La CSJN entendió que la pretensión del actor *"no se circunscribe a procurar una tutela para sus propios intereses sino que, por la índole de los derechos en juego, es representativa de los intereses de todos los usuarios de los servicios de telecomunicaciones"* (considerando 14 del voto mayoritario).

En conclusión, la normativa en cuestión ha sufrido los embates de la doctrina, la jurisprudencia, y hasta el propio Poder Ejecutivo ha reconocido su error en la reglamentación. De esta forma, no cabe otra conclusión que sostener su inconstitucionalidad por ser contraria a expresas garantías de orden constitucional contenidas en los arts. 18, 19 y 43 de nuestra Carta Magna.

3. OTRAS FORMAS DE AFECTACIÓN AL DERECHO A LA INTIMIDAD

En este punto nos referiremos a dos formas de afectación a la intimidad.

Por un lado, haremos un breve análisis de las redes sociales como uno de los servicios más novedosos y de moda en Internet, pero que pueden poner en riesgo no sólo los datos personales sino también la imagen, el honor y la dignidad, dando cuenta de las posibles soluciones legales y las escasas soluciones jurisprudenciales.

Además, haremos algunas consideraciones de las llamadas "*cookies*" como herramienta tecnológica que permite la recolección de datos personales por parte de los navegadores de Internet.

3.1. EL PROBLEMA DE LAS "REDES SOCIALES"

Puede definirse a una red social como "*aquel servicio que presenta Internet, a través de distintos sitios de la World Wide Web, por medio del cual los usuarios comparten gustos, intereses, opiniones, fotografías, videos, etc. con otros usuarios conocidos o desconocidos, en un espacio virtual que recrea un espacio de interacción social, a partir de perfiles públicos por ellos confeccionados*"[46].

Dentro de este amplio concepto, se comprenden no sólo los distintos tipos de redes sociales[47], sino también las diversas funciones y/o aplicaciones que pueden

[46] TRONCOSO ÁLVAREZ, Elizabeth - RIESTRA HERRERA, Eduardo - GARCÍA DEL VALLE MÉNDEZ, Alejandro, "Web 2.0. Regulación legal: Acciones de marketing y redes sociales", 2009, publicado en: http://www.riestra-abogados.com, p.27 a 48, consultado: 09/09/2010.

[47] Según los citados autores, las redes sociales se pueden clasificar desde diversas perspectivas:
1. Redes sociales públicas: aquéllas en que los contenidos y ciertos datos de identificación del usuario están abiertos incluso a usuarios no registrados; redes sociales restringidas: aquéllas en que es necesario registrarse y ser aceptada su solicitud para poder acceder a los contenidos fundamentales.
2. Redes sociales accesorias: funcionan en paralelo a la prestación de servicios o a la compraventa de productos *online*; redes sociales principales: tienen singularidad y entidad propia.

utilizarse, destacándose la posibilidad de chatear, dejar mensajes para cuando el usuario se conecte, subir y comentar fotografías y videos propios, compartir enlaces o *links* favoritos, jugar en línea, visitar perfiles de otros usuarios, crear un evento o un grupo, etc. Entre las más conocidas por su gran popularidad deben destacarse *Facebook*[48]*, My Space*[49] y *Twitter*[50]*.*

Ahora bien, una vez introducido el concepto de red social, deben analizarse en esta parte varias cuestiones de importancia jurídica relacionadas con la intimidad:

A) Políticas de privacidad: Naturaleza jurídica. Cláusulas abusivas.

La naturaleza jurídica de la suscripción o registro del usuario al servicio de red social es la de un contrato *online* atípico de adhesión a cláusulas generales, vale decir, una convención por medio de la cual la parte contractual más fuerte (el sitio web) predispone las cláusulas del convenio de modo tal que la otra (el usuario de la red social) no puede modificarlas, sino que sólo tiene la facultad de aceptarlas o rechazarlas en bloque. Esta suscripción presupone la aceptación de dos documentos, a saber: los "Términos de uso" ("*Terms of Service*") y la "Política de privacidad" ("*Privacy Policy*"). Ambos son imprescindibles para dejar constancia de la mecánica de su funcionamiento, además de regular los derechos y las obligaciones de los usuarios y del prestador del servicio de red social. Asimismo, creemos que es imprescindible incluir en los textos las condiciones de protección de datos, de forma

3. Redes sociales verticales: obedecen a una temática central, construyéndose la comunidad alrededor de ese eje; redes sociales horizontales: dirigidas a todo tipo de usuario y sin una temática definida.
En función de su especialización, pueden subclasificarse a su vez en: Profesionales: están dirigidas a generar relaciones profesionales entre los usuarios; De Ocio: su objetivo es congregar a usuarios que desarrollan actividades de ocio, deporte, usuarios de videojuegos, fans, etc.; y Mixtas: ofrecen a usuarios y empresas un entorno específico para desarrollar actividades tanto profesionales como personales.

[48] Facebook se autodefine como una *"herramienta social que pone en contacto a personas con sus amigos y otras personas que trabajan, estudian y viven en su entorno. Se emplea para cargar un número ilimitado de fotos, compartir enlaces y videos, y saber más sobre las personas conocidas*". (http://www.facebook.com, consultado: 03/10/2010)

[49] MySpace es una red social en la que se puede *"encontrar amigos y compañeros, conocer gente nueva, escucha música gratis y construir listados de canciones, compartir fotos, mirar videos, escribir en un blog, leer noticias sobre celebridades, utilizar aplicaciones, enviar mensajes instantáneos gratis, y mucho más"*. (http://www.myspace.com, consultado: 03/10/2010)

[50] Twitter se autodefine como "*un servicio para amigos, familiares y compañeros de trabajo para comunicarse y estar conectados a través del intercambio de los frecuentes mensajes rápidos. La gente escribe actualizaciones a corto, a menudo llamados "tweets" de 140 caracteres o menos. Estos mensajes son enviados a tu perfil o tu blog, envía a su seguidores, y se pueden buscar en la búsqueda de Twitter*". (http://support.twitter.com/forums/10711/entries/13920, consultado: 03/10/2010)

tal que antes de formar parte de la red social, los nuevos usuarios puedan saber: a) si existe una base de datos en la que se van a incluir sus datos personales, b) quién es el responsable de la misma, c) cuál va a ser la finalidad, d) si se van a ceder o no y a quién, y e) cuáles son sus derechos (acceder a los datos que se tenga sobre él, modificarlos, etc.).

En este orden de ideas, una cuestión que suscita debate es la relativa al consentimiento libre, expreso e informado del usuario en el proceso de adhesión a la red social, ya que generalmente éste no suele leer atentamente (o en muchas ocasiones ni siquiera lee) los términos y condiciones del sitio web. En este caso, ello resulta particularmente grave pues el usuario está consintiendo la disposición de sus datos personales de manera automatizada y sin tomar plena conciencia de los efectos jurídicos de sus actos. Tal como lo afirma González Frea, *"no se trata de discriminar ni restarle validez al consentimiento del usuario expresado por medios electrónicos, el cual es perfectamente válido, sino de plantear la problemática típica de los contratos por adhesión llevada al ámbito de Internet en relación a la información necesaria que debe tener el usuario a fin de actuar con un debido consentimiento informado en la manifestación de su voluntad al hacer "click" en la casilla de aceptación"* [51].

En cuanto al consentimiento y a la aceptación de las políticas de privacidad, creemos que deben seguirse los siguientes lineamientos a los fines de regularlo: el usuario debe poder acceder fácilmente al texto legal, debiéndose mostrar completo al momento del registro y no a través de un enlace o *link*[52]; el sitio web debe requerir que el usuario indefectiblemente tenga que bajar la barra lateral del navegador hasta el final de la página, a fin de que recién en ese acto aparezca el botón o la casilla de "Acepto" o "Estoy de acuerdo" (que por cierto, no debe estar marcada por defecto) para recién luego quedar habilitado el siguiente paso en la registración; las cláusulas deben redactarse de forma clara, sencilla y en idioma nacional, y las mis-

[51] Cfr. GONZÁLEZ FREA, Leandro, "Un breve Análisis Jurídico de las Redes Sociales en Internet en la óptica de la normativa Argentina", publicado en: http://www.gonzalezfrea.com.ar/derecho-informatico/aspectos-legales-redes-sociales-legislacion-normativa-facebook-regulacion-legal-argentina/265, consultado: 09/09/2010.

[52] Es interesante el fallo "Despegar.com.ar S.A. S/ Infracción Ley 18.829" de la Sala "A" de la Excma. Cámara Nacional de Apelaciones en lo Penal Económico de la Capital Federal, del 22/10/2008, en cuanto se deja sentado que tratándose de una transacción realizada por Internet, no basta con un simple enlace o *link* en la página del vendedor para garantizar que el comprador se haya interiorizado de las condiciones de contratación.

mas deben ser aceptadas expresamente por el usuario antes de poder acceder al servicio[53].

Dentro de las aludidas políticas de privacidad, se estila una cláusula de prórroga de competencia a favor del lugar donde el responsable de la red social tiene su sede principal, y que generalmente se trata de países extranjeros (por ejemplo Facebook somete sus disputas a los tribunales estatales o federales del condado de Santa Clara, siendo de aplicación las leyes del estado de California). Desde ya, se advierte que tal convención es a todas luces "abusiva" desde la óptica del derecho del consumo (los arts. 37, 38 y 39 de la Ley 24.240 son aplicables pues entre el usuario y el responsable de la red social hay una "relación de consumo").

Por último, otras cláusulas que son manifiestamente ilícitas y contrarias al orden público por ser violatorias de expresas garantías constitucionales y legales tuitivas de la intimidad son aquellas que otorgan de manera "irrevocable", "perpetua" y con "licencia mundial", los derechos sobre el material textual, fotográfico o audiovisual del usuario al responsable de la red social, y aquellas que dan derecho a este último a almacenar los datos, una vez que el usuario se dio de baja, en copias de seguridad durante un "plazo de tiempo razonable"[54].

B) Los datos personales en las redes sociales

En lo que respecta a su utilización, el auge que experimentan los servicios de redes sociales en la actualidad, ha propiciado un nivel de divulgación de datos personales (muchos de ellos de carácter "sensible") propios de los usuarios o bien de terceros, que no registra precedentes, no sólo por la gran cantidad de datos que circulan sino por el hecho de ser accesibles de forma pública y global. Cabe resaltar

[53] Cfr. GONZÁLEZ FREA, Leandro, *ob. cit.*

[54] Estas cláusulas se incluyen en la política de privacidad de Facebook (http://www.facebook.com/terms.php, consultado: 09/09/2010), aclarando que el primer tipo de cláusula ha sido modificada a comienzos del año 2009 tras suscitarse una polémica con distintas organizaciones de defensa de la privacidad de los consumidores a nivel mundial. Ver: http://archivo.lavoz.com.ar/09/02/18/Facebook-dio-marcha-atras-licencia-perpetua-contenidos.html, consultado: 09/09/2010.
Algo similar ocurre con la política de privacidad de Tuenti, la red social española más importante. Según su política de privacidad, *"El Usuario cede en exclusiva a Tuenti y para todo el mundo los derechos de reproducción, distribución y comunicación pública sobre los contenidos que suministre a través del Sitio Web, así como el de modificación para adaptarlos a las necesidades editoriales de Tuenti, y garantiza además la legítima titularidad o facultad de disposición sobre dichos derechos".*

que, si bien el usuario puede configurar el grado de privacidad con el cual desea contar, esa configuración, por defecto permite "compartir" el perfil del usuario con otros usuarios registrados o no, dependiendo a la configuración de cada red social en particular.

Otra situación particularmente grave se da cuando a través de los buscadores más conocidos se puede llegar al perfil de una persona que ha autorizado la publicación de sus datos personales. Una persona, cuando adhiere a las políticas de privacidad, simplemente autoriza al administrador de la red social a mostrar sus datos en su página, no así en los buscadores. Además, esto último, agrega potencialidad dañosa al tratamiento y recolección de datos personales, pues permite que cualquiera pueda acceder a ellos.

Consideramos que resulta de aplicación plena los principios consagrados en el art. 43 C.N. tercer párrafo, en concordancia con la ley 25.326.

C) El honor y la imagen en las redes sociales

Las redes sociales constituyen un ámbito en donde se pueden cometer gran cantidad de infracciones sobre el derecho al honor y a la imagen, lo cual ocurre con frecuencia cuando una persona publica una fotografía, y ésta inmediatamente se empieza a distribuir por toda la red de usuarios, llegando a contactos o publicaciones no deseadas por el usuario, o simplemente cuando su imagen es publicada sin su autorización (es usual que además de la publicación se identifique a una persona por medio de una "etiqueta", sin requerir su consentimiento).

Asimismo, la posibilidad de hacer comentarios a las fotografías y videos puede dar lugar a delitos contra el honor, como ser calumnias e injurias (109 a 117 C.P) o los tipos de violación de secretos y privacidad en las comunicaciones electrónicas (151 a 157 bis C.P.). Además, puede ser un ámbito propicio no sólo para la comisión de los delitos informáticos contra la propiedad (fraude y daño o sabotaje informático, artículos 173, inciso 16 y 183 y 184 incisos 5° y 6° C.P.), o contra la integridad sexual (pornografía infantil por medio de Internet, art. 128 C.P.), sino también puede ser utilizado para cometer otros ilícitos (amenazas o apología del delito, 149 bis y ter y 213 C.P.) o simplemente preparar la comisión de un delito fuera del "mundo vir-

tual", pues resulta un medio de "espionaje" de los datos personales, familiares, de amigos, e incluso de las actividades que una persona realizó o realizará y comenta en su perfil o en el de otros.

D) Discriminación en las redes sociales

Una de las principales funciones de la red social más famosa, Facebook, consiste en la posibilidad crear "grupos", es decir, un perfil público al cual los usuarios pueden unirse, y que actúa como una suerte de comunidad virtual, donde quienes forman parte de ella pueden comentar y compartir material respecto de alguna cosa, pensamiento, persona o lugar que les gusta o al cual pertenecen.

A pesar de que esta herramienta sea neutral en sí, la misma puede prestarse a situaciones de abuso, pues en lugar de utilizarse con los fines enunciados *ut supra*, en algunos casos se utiliza como forma de discriminar a personas individuales, o bien para fomentar el racismo, la xenofobia, la segregación religiosa, política, por condición social, o por preferencias sexuales[55].

Resultan de aplicación las disposiciones de la ley 23.592, y en particular su art. 3, última parte, que dispone una pena para quienes por cualquier medio alentaren o incitaren a la persecución o el odio contra una persona o grupos de personas a causa de su raza, religión, nacionalidad o ideas políticas.

E) Instrumentos jurídicos contra contenidos dañosos en las redes sociales

La legislación nacional cuenta con herramientas idóneas para solucionar estos problemas: son aplicables a todos estos casos los arts. 18, 19, 43 y 75 inc. 22 de la Constitución Nacional, la Ley de Protección de Datos Personales, el 1071 bis del Código Civil, el Código Penal, el art. 31 de la ley de derechos de autor, y el art. 3 de la ley antidiscriminación.

[55] Grupos como los siguientes pueden encontrarse en Facebook: "Nacional Socialismo Argentino", "Negros villeros al paredón", "Haga Patria, mate un *flogger*", "Unite si pensas que todos los chilenos tiene que morirse, por traidores!" (incluye fotos de la bandera de Chile quemada, y varios comentarios promoviendo la xenofobia), "Para que deporten a los bolivianos de argentina", **"**Yo Odio La Iglesia Católica!!!**",** etc. Lejos de ser una minoría, algunos de los grupos mencionados supera las 4000 personas que "adhieren" a esas ideas.

Una de las posibilidades que tiene el usuario de Internet, titular del derecho a la intimidad, honor y autodeterminación informativa afectado, es solicitar la baja de contenidos dañosos en la red social.

Podrá hacerlo de dos formas. Por un lado, el usuario puede recurrir a los distintos mecanismos que prevén las distintas redes sociales a los fines de reportar ya sea el tratamiento indebido o ilegal de los datos personales, suplantación de identidad, racismo, dar de baja grupos que fomentan el odio, publicación no consentida de imágenes o videos, entre otros abusos. En caso de que no se obtenga una solución por esta vía, podrá demandar (directamente, sin necesidad de recurrir al mecanismo anterior) a quién ha "subido" tal contenido, ya sea en sede penal (si el contenido da lugar a una acción típica descripta por el Código Penal) y/o civil, pudiendo en este último caso interponer una medida cautelar y luego el sucesivo juicio por daños, a los efectos de lograr una indemnización por el daño material, moral, psíquico, lucro cesante o lo que correspondiese según el caso.

Si bien estas herramientas están dirigidas hacia el autor del contenido dañoso, no resultan útiles a los fines de imputar responsabilidad al administrador de la red social. Así, se ha dicho que "*no existe una jurisprudencia uniforme a nivel nacional e internacional sobre esta materia. Sobre lo que sí existe unanimidad es en la imputación de responsabilidad al sitio web, ante la omisión de dar de baja contenidos dañosos una vez notificado fehacientemente por parte del usuario dañado. En el resto de los casos, se deberán analizar las circunstancias de hecho relevantes de cada caso en particular (el tipo de contenido con el cual se agravió, si se ha respetado la política de privacidad, si el sitio web omitió controlar los contenidos, etc.)*"[56].

Finalmente, es de destacar que existen instancias extrajudiciales ante los órganos de aplicación de la ley de protección de datos personales (Dirección Nacional de Protección de Datos Personales[57]) y de la ley antidiscriminación (Instituto Nacio-

[56] SANTOS, Estefanía, "¿Que Herramientas Legales Existen contra Contenidos Dañosos en Redes Sociales?", mayo de 2010, publicado en: http://www.estefaniasantos.com.ar, consultado: 03/10/2010.

[57] *"La Dirección Nacional de Protección de Datos Personales -DNPDP- es el órgano de control creado en el ámbito Nacional, dentro del Ministerio de Justicia, Seguridad y Derechos Humanos, para la efectiva protección de los datos personales. Tiene a su cargo el Registro de las Bases de Datos, instrumento organizado a fin de conocer y controlar las bases de datos. Asesora y asiste a los titulares de datos personales recibiendo las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos".*

nal contra la Discriminación, la Xenofobia y el Racismo o INADI[58]) que también resultan útiles. Ante la DNPDP, se pueden tramitar denuncias administrativas para intimar a la red social a que cumplan con su deber de permitir el acceso, supresión, bloqueo o rectificación de los datos personales[59]. El INADI, por su parte, también recibe las presentaciones que realizan particulares, grupos o instituciones sobre situaciones o actos discriminatorios que afecten a personas o grupos de personas, y procura dar una solución a través de audiencias de conciliación y dictámenes de su área legal y técnica[60].

F) La jurisprudencia nacional sobre las redes sociales

La jurisprudencia argentina ha tenido oportunidad de referirse a la red social más popular, en autos "Bartomioli, Jorge Alberto c/ Facebook Inc. S/ Medida Autosatisfactiva, Expte N° 1385/09"[61] como un *"espacio que funciona como una red social que permite a cualquier persona registrarse gratuitamente y ser usuario de dicha página y publicar fotos que puedan ser vistas por quienes quiera el usuario y crear grupos de manera sencilla, en pocos minutos, a los que puede sumarse cualquier persona, mencionando que los usuarios de dicha red en septiembre de 2009 superaron los 300 millones de personas"*. Si bien no se condenó al titular del sitio web a un resarcimiento económico, dada la naturaleza de la acción, la resolución se limitó a ordenar a la empresa Facebook Inc. a la inmediata eliminación de los sitios en los que se injurie, ofenda, agreda, vulnere, menoscabe o afecte de cualquier manera, el nombre, el honor, la imagen, la intimidad y/o la integridad del demandante, debiendo asimismo

Fuente: http://www.jus.gov.ar/datos-personales.aspx, consultado: 17/11/2010.

[58] *"El Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo (INADI) es un organismo descentralizado que fue creado mediante la Ley Nº 24.515 en el año 1995 y comenzó sus tareas en el año 1997. Desde el mes de marzo de 2005, por Decreto Presidencial Nº 184, se ubicó en la órbita del Ministerio de Justicia, Seguridad y Derechos Humanos de la Nación.*
Las acciones del INADI están dirigidas a todas aquellas personas cuyos derechos se ven afectados al ser discriminadas por su origen étnico o su nacionalidad, por sus opiniones políticas o sus creencias religiosas, por su género o identidad sexual, por tener alguna discapacidad o enfermedad, por su edad o por su aspecto físico. Sus funciones se orientan a garantizar para esas personas los mismos derechos y garantías de los que goza el conjunto de la sociedad, es decir, un trato igualitario."
Fuente: http://inadi.gob.ar/institucional/, consultado 17/11/10.

[59] El trámite se describe en la página web de la DNDP: http://www.jus.gov.ar/datos-personales.aspx, consultado 02/10/2010.

[60] El trámite se describe en la página web del INADI: http://inadi.gob.ar/, consultado 02/10/2010.

[61] El texto completo se encuentra publicado en: http://www.hfernandezdelpech.com.ar/JurisprudenciaMedidaAutosatisfactivaFacebock.html, consultado: 09/09/2010.

la empresa demandada abstenerse en el futuro de habilitar el uso de enlaces, blogs, foros, grupos, sitios de fans, o cualquier otro espacio web donde se lleven adelante esas acciones.

Asimismo, la justicia mendocina, en autos "Protectora c/ Facebook Inc. s/ medida cautelar"[62], se ha pronunciado en una polémica resolución de una medida cautelar accesoria a una acción colectiva de amparo donde se debate sobre la responsabilidad de los administradores de la red social Facebook, por haberse creado en su sitio web "grupos" con el objeto de promover la ausencia escolar, y de esta forma haberse afectado el derecho a la integridad de los menores ante el peligro que una nueva convocatoria implicaría para los mismos.

Por lo pronto no hay un fallo sobre el fondo de la cuestión, pero sí ya es un precedente de trascendencia el hecho de que se haya dado trámite a la acción a través de la vía del amparo colectivo, que se haya admitido la legitimación activa de la actora (se trata de una asociación con fines de defensa de los derechos del consumidor), y que se haya fijado la jurisdicción local a pesar de la cláusula de prórroga de jurisdicción a favor de Facebook Inc.

A modo de colofón, luego de haber expuesto someramente algunas nociones que hacen la problemática jurídica que presentan las redes sociales en torno a la privacidad de las personas, se puede concluir que, en la actualidad, si bien el derecho argentino adolece de disposiciones legales específicas que regulen el tema, igualmente presenta un plexo normativo que puede dar buenas soluciones a las distintas situaciones apuntadas. Será labor de los autores y de los jueces *aggiornar* "viejas" soluciones a "nuevos" problemas.

---

[62] "Protectora Asociación Defensa del Consumidor c/ Facebook Inc. s/medida cautelar", 2º Juzgado Civil y Comercial de la 1ª Circunscripción de Mendoza, 11/05/2010. En la parte resolutiva del fallo se dispuso: "*HACER LUGAR parcialmente a la medida precautoria solicitada, ordenar a FACEBOOK INC: el cese inmediato de los grupos creados o a crearse por menores de edad, respecto de los contenidos que sean vistos en la Provincia de Mendoza o recibidos y/o dirigidos a menores que se encuentran en ésta, con el objeto de promover la falta al ciclo escolar, sin el debido consentimiento de sus padres o la autoridad escolar, para juntarse en un sitio específico para poder festejar dicho incumplimiento; como también hacer extensivo a posibles otros objetos donde los menores de edad promuevan objetivos que puedan causarse daño ellos o a terceros con su accionar; y haga efectivo el control de los contenidos de los grupos de menores de edad y su seguridad, conforme lo manifestado en las condiciones publicadas en http://www.facebook.com/policy.php, hasta que exista en el presente expediente resolución definitiva"*. Publicado en: http://www.protectora.org.ar/notas/protectora-inicia-acciones-legales-contra-de-facebook/1811, consultado: 09/09/20 10.

3.2. LAS "COOKIES"

Podemos definir a las *cookies*[63] como *"archivos de texto que muchos servidores instalan en el disco duro del usuario y que registran los diferentes sitios a los que este usuario va ingresando, creando así una imagen de éste sobre sus preferencias de navegación y sitios que visita habitualmente"*[64].

Estos archivos de texto[65] se generan a partir de las instrucciones que los servidores web envían a los navegadores (*browsers*[66]), a fin de que se recuerden las preferencias del usuario en su navegación habitual por la red, lo cual facilita una conexión más rápida, permite una configuración personalizada, y que se reconozca al usuario cada vez que ingresa a un sitio web[67].

Si bien éste es el verdadero sentido con el cual las *cookies* deberían ser utilizadas, esta aparente inofensiva finalidad, se desvirtúa en la práctica, pues existe el riesgo concreto de que con la información recabada se creen perfiles de los usuarios en relación a sus gustos personales, afectando manifiestamente su derecho a la intimidad en cuanto a la navegación por Internet[68].

Es así que las *cookies* constituyen *"un poderoso instrumento de marketing para las empresas, pues se pueden conocer los hábitos de consumo del usuario, saber sus preferencias en la web – y por lo tanto en su vida particular -, el tiempo que le dedica a*

---

[63] *"Cookies"* en inglés significa "galletitas", en el sentido de huellas que se van dejando en el camino. En este caso, las *cookies* son huellas electrónicas que el usuario va dejando mientras navega por los distintos sitios o páginas web. La Unión Europea, en la ya citada directiva 2002/58/CE, les da el nombre de "chivatos", y que debe entenderse como algo que delata o da información de manera secreta.

[64] FERNÁNDEZ DELPECH, Horacio, *ob. cit.*, p. 334. El autor, aclara que las *cookies* poseen las siguientes características técnicas, a saber: se almacenan en el disco rígido de la PC del usuario (hasta 300 cookies, cada una de no más de 4 KB de tamaño), pero no se tiene acceso al mismo; poseen fecha de caducidad; el único que puede "leer" una *cookie* es el servidor que lo envió, y no otro/s; el usuario que desee, puede inhabilitar en su navegador la opción de recibir cookies, desactivándolo, o hacer que sea avisado cuando va a recibirlos.

[65] Las cookies no son un virus, y por ello deben diferenciarse de los *spywares*. El software espía o s*pyware*, registra todo lo que el usuario hace con el propósito de conocer sus preferencias y enviarle publicidad relacionada con su perfil (no son archivos de texto como las *cookies*, sino archivos ejecutables, ya sean .exe o .html).

[66] Se denomina así al software que interpreta el código HTML (es el lenguaje informático en el que se confeccionan las páginas web) y lo presenta en pantalla permitiendo al usuario interactuar con su contenido y navegar hacia otros lugares de la red mediante enlaces o hipervínculos. Los navegadores más conocidos son: Internet Explorer, Google Chrome, Firefox, Safari y Opera.

[67] Cfr. VANINETTI, *ob. cit*.

[68] Cfr. FERNANDEZ DELPECH, *ob. cit*., p. 334.

cada preferencia, las publicidades que ha visto, los productos o servicios contratados en la web, y mucha otra información"[69].

A esta modalidad de marketing directo, se suma el riesgo de que la información recopilada contenga datos personales íntimos, e inclusive datos que puedan llegar a ser considerados "sensibles". Esto último, es particularmente grave, pues al decir de Uicich, *"pueden afectarse indirectamente otros derechos como el de trabajar, a la salud, o a no ser discriminado, al formarse bases de datos con información recolectada de manera no consentida por el usuario*[70].

Como si ello fuera poco, debe agregarse que, por lo general, los usuarios desconocen qué son las *cookies*, cómo funcionan, qué tipo de información recopilan, cuál es su objeto y cómo pueden desactivarlas. Esta situación de ignorancia va acompañada de una escasa sino nula información por parte de los sitios web o de los servidores que almacenan estos archivos.

Ahora bien, en base a estas características, surge la duda respecto de su legalidad o ilegalidad. Frente a esta disyuntiva, en el derecho comparado se han esbozado dos soluciones, a saber: sistema *"opt in"* y sistema *"opt out"*. De acuerdo al primero, se presume que el usuario no acepta las *cookies,* a menos que se pronuncie expresamente a su favor (vale decir, se presume su ilegalidad, salvo que el usuario las acepte). Por otro lado, el sistema *"opt out"* presume lo contrario, es decir, que los usuarios aceptan el almacenamiento de *cookies* en su disco duro, salvo que se manifiesten expresamente en contra, para que las mismas no funcionen recolectando sus datos personales (se presume que son legales, a menos que el usuario no haya consentido su aceptación)[71].

Al respecto, coincidimos con Sobrino en que *"el sistema de "Opt-Out", es decir, el hecho que se nos diga que podemos quitar las "cookies" (que la gran mayoría de los usuarios de Internet, no sabe siquiera de qué se trata) y que nos expliquen cómo se*

[69] UICICH, *ob. cit.*, p. 82.
[70] UICICH, *ob. cit.*, p. 80 y 81. El autor advierte la peligrosidad de esto por ejemplo en el caso en el que se hayan obtenido datos de un usuario que realiza una consulta *online* sobre el HIV, o sobre medicamentos que puede ser utilizado para combatir esa enfermedad, y que visita páginas de contenido homosexual, pues los mismos serán utilizados para hacer un perfil sobre él, y que en un futuro le impedirá una cobertura de un seguro de vida, de cobertura médica, o en todo caso ser discriminado por un empleador que contrata en base a condiciones personales como la sexualidad o la salud.
[71] Cfr. SOBRINO, Waldo Augusto Roberto, "Las cookies y el Spam (y la violación de la Privacidad y la Intimidad)", Alfa-Redi: Revista de Derecho Informático, No. 035, Junio del 2001, publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=710, consultado: 07/10/10.

deben quitar (hecho técnico éste, que para la mayoría de los usuarios, es una 'misión imposible'), es absolutamente ilegal, dado que en la práctica, es de casi imposible compresión y realización", mientras que "*el sistema de "Opt-In", es más transparente y respetuoso de la intimidad y la privacidad, dado que significa que si queremos que las "cookies" funcionen (y recolecten nuestros datos), debemos incorporarnos de manera expresa y voluntaria*"[72].

En la Argentina, no existe normativa alguna que trate específicamente este tema. Sin embargo, entendemos que resulta de aplicación analógica la ley 25.326, en particular cuando se dispone que la recolección de datos "no puede hacerse por medios desleales", ni de manera "fraudulenta" (arts. 4 inc. 2°), y que el tratamiento de datos personales es ilícito, cuando el titular "no hubiera prestado su consentimiento libre, expreso e informado" (art. 5).

Por su parte, Fernández Delpech[73], quien entiende que la función principal de las *cookies* es ser una herramienta de marketing, sostiene que el art. 27 de la LPDP da una solución a la cuestión en su primer inciso, al establecer que *"en la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrá tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares y obtenidos con su expreso consentimiento"*.

De esta disposición surge que la recolección de datos con fines de hacer perfiles acerca de los hábitos de consumo está plenamente aceptada en nuestro derecho, pero se aclara - nuevamente - que los datos deben haber sido obtenidos con el consentimiento de su titular.

En conclusión, pese a la inexistencia de normas particulares, del juego de los arts. 4, 5 y 27, surge con evidencia que nuestra ley recepta el sistema "*opt in*". Es decir, se reconoce que la recolección de datos a partir de *cookies* es ilegal, salvo que tal recolección se haga bajo el consentimiento libre e informado de los usuarios y que se especifique claramente que la finalidad de las *cookies* es de marketing o publicidad.

[72] SOBRINO, Waldo Augusto Roberto, *ob. cit.*
[73] Cfr. FERNANDEZ DELPECH, *ob. cit.*, p. 336.

CAPÍTULO V
PROBLEMAS JURÍDICOS DERIVADOS DEL CORREO ELECTRÓNICO

La creciente difusión de Internet en general y la masiva utilización del correo electrónico como uno de los servicios más importantes que ofrece la red, son los fenómenos más trascendentes de los últimos tiempos en lo que a nuevas tecnologías de comunicación se refiere. Esta realidad, nos lleva a estudiar las implicancias y conflictos jurídicos que el correo electrónico puede ocasionar y cuál debería ser la legislación aplicable a las distintas situaciones que esta nueva herramienta genera. Cabe aclarar que entre los múltiples problemas se plantean, sólo nos referiremos a aquellos vinculados al derecho a la intimidad.

Es así que en esta parte de la obra se expondrán principalmente tres cuestiones, a saber: la violación del e-mail como manifestación actual de la privacidad de la correspondencia, el correo electrónico no solicitado o *"spam",* y las facultades del empleador de controlar el e-mail laboral de sus dependientes.

Respecto de cada una de estas cuestiones, abordaremos las distintas soluciones que desde la legislación y la jurisprudencia argentina resulten aplicables y/o se hubieren propuesto, todo ello, sin perder de vista las respuestas que se esbocen en el derecho comparado.

1. PRIVACIDAD Y VIOLACIÓN DEL CORREO ELECTRÓNICO

A continuación, intentaremos dar un concepto de correo electrónico y repasar sus aspectos más relevantes en relación con la inveterada correspondencia epistolar. Asimismo, nos referiremos a la protección constitucional y legal del e-mail como manifestación de la privacidad e intimidad de las personas, para finalmente hacer unas breves consideraciones del *leading case* "Lanata".

1.1. ASPECTOS GENERALES: CONCEPTO Y NATURALEZA JURÍDICA

A los fines de lograr una mejor comprensión del concepto de correo electrónico, resulta preciso definirlo desde el punto de vista técnico y jurídico.

Desde lo técnico, podemos afirmar que el correo electrónico es el servicio de Internet que, utilizando el protocolo SMTP y POP3 o HTTP, permite el envío y recepción de textos, imágenes y archivos de manera casi instantánea.

De esta definición, creemos preciso realizar las siguientes aclaraciones:

- El correo electrónico constituye el instrumento de comunicación por excelencia en la actualidad, sobre todo por su gran eficiencia, conveniencia y bajo costo.

- El correo electrónico es uno de los servicios más importantes que ofrece Internet, en conjunto con la *World Wide Web,* pues agrupa un gran número de usuarios. Según una estadística de *The Radicati Group Inc*, una empresa americana de investigaciones del mercado tecnológico, se estima que al año 2009, la cantidad de usuarios de correo electrónico superó los 1400 millones, proyectándose que para el año 2013 esa cifra rondará los 1900 millones de usuarios[1].

- A través del e-mail se desarrolla y completa el proceso comunicacional entre emisor/receptor, al permitirse el intercambio de un mensaje por medio de un canal determinado (vgr. red Internet). En este caso en particular, dicho intercambio, resulta peculiar, pues los mensajes son llevados por los proveedores de servicio de Internet, quienes actúan de mediadores (de la misma forma que lo hace el servicio de correo tradicional) en su envío y recepción[2].

- Para que la transferencia de mensajes se concrete, tanto el remitente como el destinatario, necesitan de una dirección de e-mail (los proveedores de acceso generalmente otorgan una), la cual se reconoce por el famoso signo de arroba @ en la mitad. Por ejemplo: nombre@servicio.com, donde la primer parte identifica el nombre o alias del usuario, y la segunda identifica el dominio o servidor en el que está esa persona.

[1] Para mayor información: http://www.radicati.com/?p=3237, consultado 10/10/10.
[2] Cfr. VANINETTI, Hugo A., "Derecho a la intimidad e Internet", SJA 12/1/2005, Publicado en: http://www.abeledoperrot.com.ar, consultado: 09/09/2010.

- Cuando se alude a los protocolos[3] SMTP y POP o HTTP, la definición sugiere que existen dos formas de operar cuentas de correo electrónico: a través de programas de "Cliente de Correo" (*Outlook Express* y *Eudora* son los programas más conocidos; para establecer la comunicación entre el remitente y el destinatario utilizan el protocolo SMTP para el envío de mensajes y el protocolo POP para recibirlos), o bien a través de una página web (los servidores de *webmail* más famosos son *Hotmail*, *Yahoo!* y AOL, y utilizan el protocolo HTTP). Debe aclararse que, más allá de estas diferencias técnicas, cualquiera sea la forma elegida para acceder a una cuenta de e-mail, el servicio es exactamente el mismo, y no trasciende al plano jurídico[4].

Ahora bien, desde el punto de vista jurídico, Farinella sostiene que el correo electrónico es *"toda correspondencia, mensaje, archivo, dato u otra información electrónica que se transmite a una o más personas por medio de una red de interconexión entre computadoras"*[5].

De esta definición, se infiere que el correo electrónico resulta más versátil que la tradicional carta, pues no sólo permite expresar ideas, pensamientos y sentimientos, sino también transferir imágenes, videos, sonidos, y demás documentos digitales que puede producir una computadora. Además, al decir de Uicich, *"se diferencia por la ausencia del papel, la velocidad de transmisión casi instantánea, el amplio espacio para enviar documentos de gran tamaño (medidos en bits), y la carencia de fronteras físicas o ideológicas"*[6].

De estas diferencias, sólo resta concluir que las mismas no resultan suficientes para otorgar al correo electrónico una naturaleza jurídica distinta respecto de la correspondencia epistolar. No vacilamos en pronunciarnos en esta corriente, coin-

[3] Desde el punto de vista informático, un protocolo es un conjunto de normas que permite el intercambio de información entre ordenadores conectados entre sí.
[4] Cfr. HOCSMAN, Heriberto Simón, "Negocios en Internet", Editorial Astrea, Buenos Aires, 2005, pág. 144.
[5] FARINELLA, Favio, "El correo electrónico y el spam, sometidos a una consulta sobre su regulación", Alfa-Redi: Revista de Derecho Informático, No. 041, Diciembre del 2001, publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=1005, consultado: 09/10/10. La definición es la que propone el "Anteproyecto de Ley de Protección Jurídica del Correo Electrónico" elaborado por la Secretaría de Comunicaciones, a través de la resolución 333/2001, del .10/9/2001. Su art. 2 aclara que: *"A los efectos legales, el correo electrónico se equipara a la correspondencia epistolar. La protección del correo electrónico abarca su creación, transmisión y almacenamiento"*.
[6] Cfr. UICICH, Rodolfo D., "El derecho a la intimidad en Internet y en las comunicaciones electrónicas", Editorial Ad Hoc, Buenos Aires, 2009, pág. 46.

cidiendo con Moeremans y Casas en que *"se trata de un documento particular que se encuentra asentado en un soporte inmaterial, en bites. Por tanto, es asimilable a la naturaleza de las cartas, no igual, debido a que estas últimas se asientan en soporte papel, no sería el caso del correo electrónico que al carecer de la armadura del sobre, deja abierta la posibilidad de que el proveedor de Internet vea el contenido de los e-mails"*[7].

1.2. PROTECCIÓN EN LA LEGISLACIÓN ARGENTINA

Tal como dijimos en líneas anteriores, nuestra Constitución garantiza la inviolabilidad de la correspondencia epistolar y los papeles privados, y que una ley determinará en qué casos y bajo qué circunstancias se permitirá su allanamiento (art. 18 C.N.). Cabe preguntarse si el correo electrónico se encuentra amparado por esta garantía.

Para responder esta cuestión, debemos tener en cuenta que el artículo 18 de nuestra Carta Magna se ha mantenido sin reforma alguna desde la histórica redacción de 1853/1860, razón por la cual se incluye expresamente a la correspondencia epistolar y no al correo electrónico. Resulta cuanto menos imposible que el constituyente pudiera haber previsto en aquélla época la aparición de este nuevo medio.

Es por ello que, resulta necesario hacer una interpretación flexible y dinámica del texto constitucional a los fines de dar cabida a nuevas realidades. No basta en este caso con hacer una interpretación literal y restrictiva, pues de este modo se excluye de tutela a todo aquello que no está expresamente previsto.

Coincidimos con Bidart Campos cuando afirma que *"la Constitución lleva en sí una pretensión de futuro y de continuidad. Lanzada hacia el porvenir, es menester interpretarla e integrarla históricamente, de modo progresivo. Interpretar la voluntad del autor como inmutable y detenida en la época originaria de la Constitución es atentar contra la propia voluntad de futuro y de perduración con que el autor la ha plasmado. Quiere decir que mientras no incurramos en contradicción con la Constitución,*

[7] MOEREMANS, Daniel E. - CASAS, Manuel Gonzalo, "Protección del e-mail como extensión del derecho a la intimidad", LA LEY 2007-E, 740, publicado en: http://www.laleyonline.com.ar, consultado: 09/09/2010.

ella misma habilita y asume su propia interpretación e integración dinámica, histórica, progresiva y flexible"[8].

De este modo, si seguimos este criterio teleológico progresista, nos permitimos afirmar que el texto del artículo 18 puede adaptarse a las nuevas formas de comunicación, e incluir al correo electrónico dentro del ámbito de tutela constitucional[9].

Ahora bien, más allá de esta interpretación, hay una realidad incontrastable en el derecho nacional, y es que no sólo no existe una norma de orden constitucional que consagre la garantía de inviolabilidad de las comunicaciones electrónicas -como si ocurre por ejemplo en España, tal cual lo vimos en el capítulo III -, sino que tampoco existe norma alguna de orden infraconstitucional que consagre directamente la privacidad del correo electrónico.

La única norma que se ha dictado en el derecho argentino, y que se refiere a él, es un decreto que declara la importancia de su utilización masiva y sin exclusiones de este servicio, a través del proyecto "Una dirección de correo electrónico para cada argentino", destinado a proveer una cuenta de correo electrónico gratuita con una dirección electrónica segura y reconocida a cada habitante de la República Argentina que posea Documento Nacional de Identidad y a cada persona jurídica que posea Clave Única de Identificación Tributaria (art. 1 dec. nac. 1335/1999[10]).

Lo que sí es destacable, por el contrario, es que recientemente, con la sanción de la ley 26.388 de delitos informáticos, modificatoria - en lo que aquí interesa - de los distintos tipos que se agrupan bajo la "violación de secretos" (153 y ss. del Código Penal), se introduce una norma de protección de la privacidad del correo electrónico. La inclusión de la "comunicación electrónica" dentro de los tipos aludidos, otorga un ámbito de tutela importante, pero sólo desde el punto de vista penal.

Si bien consideramos que esta reforma constituye un avance en materia de protección del e-mail, asimismo, entendemos que es insuficiente, pues, como se

[8] BIDART CAMPOS, Germán J., "Manual de la Constitución Reformada", Editorial Ediar, Buenos Aires, 1996, Tomo I, p. 318.
[9] En el mismo sentido: MOEREMANS – CASAS, *ob. cit.*, VANINETTI, *ob. cit.*, y HOCSMAN, *ob. cit.*, p. 145 a 147.
[10] *B.O.*, 19-XI-1999

verá en líneas subsiguientes, los numerosos problemas que plantea el correo electrónico - y de los cuales nos referiremos sólo a dos -, requieren de una ley especial, en la cual cada uno de ellos sean tratados de una manera integral y profunda.

A modo de conclusión, creemos que hasta tanto nuestro derecho no consagre una ley que regule exhaustivamente la problemática del correo electrónico, o por lo menos se limite a asimilarlo directamente a los papeles privados (del mismo modo que el decreto 1279/97 asimila Internet a los medios de comunicación, extendiéndole la garantía de libertad de expresión), las distintas formas de violación de la privacidad de los usuarios deberán regirse por el conjunto de normas tuitivas del derecho a la intimidad señaladas *ut supra (ver capítulo III)*, que si bien pueden dar soluciones utilizando la analogía para los casos no previstos, terminan careciendo de especificidad y precisión.

1.3. LA SITUACIÓN EN LA JURISPRUDENCIA NACIONAL

La pretendida igualación del correo electrónico con la correspondencia epistolar ha sido sostenida también desde la jurisprudencia nacional, destacándose el caso "Lanata" [11]. Más allá de los hechos y las pretensiones planteadas por ambas partes[12], viene al caso transcribir aquellas expresiones en donde se define la naturaleza jurídica del correo electrónico: *"El tan difundido e-mail de nuestros días es un medio idóneo, certero y veloz para enviar y recibir todo tipo de mensajes, misivas, fotografías, archivos completos, etc.; es decir, amplía la gama de posibilidades que brindaba el correo tradicional al usuario que tenga acceso al nuevo sistema. Es más, el correo electrónico posee características de protección de la privacidad más acentuadas que la inveterada vía postal a la que estábamos acostumbrados, ya que para su funcio-*

[11] Lanata, Jorge s/ desestimación, Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, causa 10.389/99, 02/12/1999.

[12] En pocas palabras, los hechos fueron los siguientes: En el año 1999, el señor Edgardo Héctor Martolio inició una querella penal contra el periodista Jorge Lanata por los delitos de violación de correspondencia y publicidad de correspondencia con fundamento en los arts.153 y 155 del Código Penal. Intervino el Juzgado Nacional en lo Correccional Nro. 6 de la Capital Federal, ante quién Lanata planteó un incidente de excepción de falta de acción por hecho atípico, el que fue rechazado con fecha 2/08/1999. Con fecha 2/121999, la Sala VI de la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, confirmó el auto del tribunal de instancia inferior. Contra ese pronunciamiento, el querellado interpuso recurso de casación que fue rechazado por la Sala interviniente. Planteado recurso de queja, la Sala IV de la Cámara Nacional de Casación Penal con fecha 12/05/2000, finalmente volvió a rechazar el mismo.

namiento se requiere un prestador del servicio, el nombre de usuario y un código de acceso que impide a terceros extraños la intromisión en los datos que a través del mismo puedan emitirse o archivarse. Sentadas estas bases preliminares, nada se opone para definir al medio de comunicación electrónico como un verdadero correo en versión actualizada".

La riqueza del fallo radica no sólo en la asimilación del correo electrónico al postal, y su correlativa extensión de los principios relacionados con la libertad de expresión, de circulación y la privacidad, sino que además este caso motivó una ulterior reforma a los tipos penales previstos en los arts. 153 (violación de correspondencia) y 155 (publicación indebida de correspondencia) que se invocaron por el demandante, y que tuvo lugar con la ya mencionada reciente ley 26.388 de delitos informáticos.

Además, debe destacarse un detalle no menor: paradójicamente el fallo fue dictado en sede penal, donde rige la prohibición de analogía. *A fortiori,* los mismos argumentos cobran mayor fuerza en el resto de los fueros y legislaciones.

Es por esto último que en sede comercial, el Juzgado Nacional Comercial N° 18, ha dictado una resolución que reafirma lo sostenido en "Lanata". En "G., D.E.c/ C. SA. s/diligencia preliminar"[13], se dijo que *"no se advierten motivos para que - aún sin existencia de legislación específica - el denominado "correo electrónico" escape a dicha protección* (en relación a la protección constitucional de la correspondencia

[13] G., D. E. c/ C. S.A. s/Diligencia Preliminar, Juzgado Comercial Nº 18, Secretaría 36, Expte. N° 39749, 23/10/2001, publicado en: http://www.hfernandezdelpech.com.ar/JurisprudenciaArgCorreoElectrResolucionJuzComerN18.htm, consultado 10/10/10.
La medida de prueba anticipada solicitada por el demandante tenía por objeto *"la constatación judicial acerca de la existencia en los equipos de computación* (del domicilio del demandado) *de mensajes electrónicos enviados a la bandeja de entradas de Outlook y/o sistema similar donde se archiven los mails" y que lo tengan como "remitente, destinatario o con copia" a él mismo.* El actor justificó la medida en el hecho que la misma *"pueda desaparecer o tornarse impracticable con el transcurso del tiempo, ya que "con sólo apretar una tecla del equipo de computación desaparecerían todos los mails que le han sido enviados a la demandada" al equipo de computación por ella utilizado en esas oficinas. Esos "mails" –según el demandante- acreditarían parte de las razones por las cuales rescindió el contrato que la unía con la recipiendaria de los mensajes" (*del texto del fallo*).*
Si bien el *thema decidendum* de la resolución era la procedencia de la medida procesal, el tribunal se refirió *obiter dictum* a la naturaleza del correo electrónico.
En cuanto al destino de la medida, ésta se rechazó por considerarse que la medida *"ha omitido toda mención al texto de esos correos y los por ella misma recibidos, ni acompañado copia de los mismos, siendo que, por los usos y costumbres comerciales (art. 5 del Título Preliminar del Código de Comercio), la existencia de esas copias puede presumirse tanto en los propios equipos de computación de la accionante como en los de su Proveedor de Servicios de Internet (ISP), a quien tampoco individualizó" (*del texto del fallo*).*

epistolar), *tanto más si así fue admitido jurisprudencialmente en el ámbito del derecho penal, donde la analogía está prohibida"* (en relación a "Lanata"); para argumentar tal analogía, el tribunal consagró el siguiente principio: *"los derechos, garantías, obligaciones y responsabilidades en la red - aun reconociendo la novedosa trama de vínculos jurídicos que ha puesto al descubierto - no pueden ser medidos con diferente vara que los derechos, garantías, obligaciones y responsabilidades fuera de la red".*

En síntesis, la jurisprudencia nacional a través de los casos citados ha equiparado al correo electrónico, a los fines de su protección constitucional, con la correspondencia epistolar (art. 18 C.N.). De este modo, el e-mail merece ser protegido de la misma manera que el tradicional y cualquier violación que sufriera debería ser sancionada tanto civil como penalmente.

2. EL CORREO ELECTRÓNICO NO SOLICITADO O "*SPAM*"

A continuación trataremos el tema del correo electrónico no solicitado o "spam", dando una descripción general del problema, para luego exponer las soluciones que se han dado en el derecho comparado, principalmente en la Unión Europea y en los Estados Unidos, y, finalmente, nos referiremos a las soluciones que - ante la ausencia de legislación que regule específicamente el tema - se han intentado dar desde la doctrina y la jurisprudencia argentina.

2.1. ASPECTOS GENERALES

El llamado "*spam*"[14] es uno de los abusos que pueden cometerse a través del correo electrónico, y consiste en la técnica de enviar indiscriminadamente mensajes de e-mail a usuarios que no pidieron recibirlos.

Si bien el problema descripto aparentemente redundaría en una simple molestia para el usuario que recibe estos mensajes, quien sólo debe eliminar los co-

[14] Según Hocsman (*ob. cit.*, p. 196), la palabra *"spam"* resulta de combinar *"(s)piced (p)ork"* y *"h(am)"*, un producto a base de carne de cerdo, enlatado, al que hacía referencia un sketch televisivo del famoso grupo satírico británico "*Monty Phyton*", en el que una mesera menciona al leerle el menú a su cliente todos los platos con *spam*, "tapando" el contenido relevante de cada ítem del menú. Aplicado a Internet, el *spam* obstruye todos los mensajes relevantes.

rreos "basura" (en inglés también reciben el nombre de "*junk mail*"), la situación es algo más compleja que eso, pues aunque generalmente se lo utiliza con fines comerciales o publicitarios[15], no son pocos los casos en que se lo utiliza con el fin de paralizar el servicio por saturación de la conexión, del espacio en disco o de la capacidad de procesamiento de un servidor[16], o bien simplemente para enviar virus informáticos o archivos engañosos o perjudiciales[17].

Asimismo, se evidencia la complejidad del problema en que los costos de conexión y de tecnología recaen sobre el usuario/destinatario y no sobre el remitente (*spammer*). El que recibe el e-mail es quien soportará los costos de conexión a Internet, es decir, todo el tiempo que le demandará la descarga del contenido del mensaje, privándolo de utilizar el sistema en toda su capacidad, pues el mensaje "controla" parte de la computadora desde que ingresa hasta que es eliminado de la misma[18]. Además, el *spam* implica que el usuario deberá afrontar un costo tecnológico, el cual se traduce en dos aspectos: por un lado, en los gastos en los que el usuario debe incurrir para mantener actualizado su software *antispam* o antivirus; y por otro lado, los gastos que representan los daños físicos en el sistema (se produce un desgaste en el disco rígido del destinatario), pues cuando se borra el correo indeseado quedan "agujeros" en el sistema (técnicamente se denomina fragmentación), haciéndolo lento al procesador[19].

[15] Generalmente se ofrecen productos relacionados con la mejora del rendimiento sexual, con la caída del cabello, pastillas para bajar de peso en tiempo récord, venta de productos tecnológicos a bajo precio, productos farmacéuticos, pornografía, etc.
[16] VANINETTI, Hugo, *ob. cit.*
[17] Hay diferentes tipos de *spam* que pueden llegar a nuestra Bandeja de Entrada. Entre estos se destacan los más perjudiciales como el fraude (el contenido de este mensaje implica un comportamiento deshonesto, cuyo objetivo es hacer dinero, donde alguien se hace pasar por quien no es, o nos hace creer algo que no es cierto, sugiriendo que sigamos un procedimiento por el cual seremos perjudicados económicamente), los *Scams* (se trata de un mail que atrae el interés del usuario y que esconde una maniobra deshonesta. En algunos casos ofrece ganar dinero fácilmente, para lo cual hace una propuesta que, al seguirla, pondrá en grave riesgo el patrimonio del usuario e incluso su buen nombre y honor.) y el *phishing* (se recibe un mail proveniente, en apariencia, de una entidad de reconocida trayectoria y que invita a visitar el *Web Site* de la empresa para actualizar datos. El vínculo en realidad lo remite a una página falsa con la intención de robar datos personales, que puede incluir incluso número de cuenta bancaria y palabra clave). Fuente: http://www.jus.gov.ar/datos-personales/recomendaciones/uso-seguro-de-internet.aspx, consultado: 09/09/2010.
[18] Cfr. FERNÁNDEZ DELPECH, Horacio, "Internet: su problemática jurídica", Editorial Abeledo Perrot, Buenos Aires, 2004, p.325.
[19] Cfr. VANINETTI, Hugo, *ob. cit.*

Quienes también se ven perjudicados son los proveedores de servicio de Internet, ya que estos mensajes consumen ancho de banda[20] al ser procesados y, en una cantidad masiva, pueden generar una disminución en la velocidad y calidad de sus servicios[21]. Para graficar el problema de la masividad de los correos no deseados, debe apuntarse que durante el año 2009, más del 81% de la totalidad de correos electrónicos enviados (247 mil millones) han sido *spam,* y que un proveedor del servicio de correo electrónico promedio, que agrupa más de mil usuarios, debe gastar aproximadamente U$S 1,8 millones al año para gestionar este problema[22].

Como si ello fuera poco, se agrega la dificultad de que en la mayoría de los casos los remitentes son desconocidos, o bien la dirección de correo que aparece es falsa, o sólo se incluye un teléfono o una página web en la que se puede solicitar el producto promocionado, lo que impide identificar una dirección electrónica correcta para solicitar que en un futuro no se envíen mensajes de ese tipo[23].

Por último, a todos estos agravantes, se suma uno no menor: las bases de datos donde se encuentra la dirección de e-mail del destinatario suelen ser ilícitas, en el sentido que se obtiene la misma sin el consentimiento expreso e informado del usuario, además de estar exentas de contralor por autoridad estatal de aplicación alguna. Al respecto, Sobrino considera que *"más allá de que el spam en sí mismo esté prohibido o no, el hecho de mandar junk mails tiene una base ilegal cuando para el envío de ese correo no solicitado se tuvieron que utilizar bases de datos ilegales"*[24]*;* de ello concluye que si los *spammers* no prueban la legalidad de las bases de datos de las cuales obtuvieron las direcciones de e-mail a las cuales enviaron correos no solicitados, y *"al existir una presunción iuris tantum de ilegalidad*", también debe decretarse la antijuridicidad del *spam*[25]. Tal razonamiento responde a la "teoría del fruto del árbol envenenado", sobre la cual volveremos más adelante, al referirnos a las soluciones esbozadas en el derecho nacional.

[20] En conexiones a Internet el ancho de banda es la cantidad de información o de datos que un proveedor de servicio de Internet puede enviar a través de una conexión de red en un período de tiempo dado.
[21] Cfr. VANINETTI, Hugo, *ob. cit.*
[22] Datos según el *"Email Statistics Report*, 2009-2013" de *The Radicatti Group Inc*, publicado en: http://www.radicati.com/?p=3237, consultado: 10/10/10.
[23] Cfr. FERNANDEZ DELPECH, Horacio, *ob. cit.*, p.322.
[24] SOBRINO, Waldo Augusto Roberto, "Internet y la alta tecnología en el derecho de daños", Editorial Universidad, Buenos Aires, 2003, p. 70.
[25] Cfr. SOBRINO, Waldo Augusto Roberto, *ob. cit.*, 72 y 73.

En conclusión, de todo lo expuesto se evidencia que la problemática del *spam* además de afectar la propiedad privada del usuario de Internet, al cargar injustamente con costos de conexión y de tecnología, también importa una flagrante violación a la intimidad, pues el usuario se ve invadido por esta particular forma de publicidad, sin haberla requerido previamente, con productos y servicios que nunca solicitó.

2.2. SOLUCIONES EN EL DERECHO COMPARADO

En los países desarrollados, el *spam* ha sido objeto de preocupación, y por lo tanto se han esbozado distintas soluciones tecnológicas y jurídicas.

Una primera solución se ha dado a nivel de software *antispam*[26], los cuales si bien disminuyen los problemas al filtrar automáticamente los mensajes no deseados, evitando que lleguen a la bandeja de entrada, éstos no utilizados por la mayoría de los usuarios. Además, como se dijo con anterioridad, constituye una carga injusta sobre el usuario, pues debe afrontar el costo del software en cuestión, más el costo de mantener actualizado dicho programa.

Asimismo, tanto los programas de "cliente de correo" (Outlook Express, Eudora, etc.) como los prestadores de servicio de *webmail* (*Hotmail*, *Yahoo!*, AOL, entre los más conocidos) brindan la posibilidad de configurar las opciones a fin de no recibir más correos de este tipo, o bien recibirlos en una carpeta distinta de la bandeja de entrada del usuario. El problema radica en que la mayoría de los usuarios desconoce cómo configurar dichas opciones. Al decir de Sobrino, *"jamás debemos perder de vista, que la gran mayoría de nosotros somos "hipoconsumidores tecnológicos" y "analfabetos funcionales" (de Internet), dado que nuestros conocimientos de computación de Internet, se deben asemejar a los de un niño de jardín de infantes"*[27].

Por otro lado, en relación a las soluciones jurídicas al tema, en las distintas legislaciones se ha promovido un debate en torno a la creación de registros centra-

[26] Los más conocidos son *SpamFighter*, *SpamKiller*, K9, *Xeeon Antispam*, *Mailwasher*, entre otros.
[27] SOBRINO, Waldo Augusto Roberto, *ob. cit.*, p. 63.

lizados de usuarios a fin de determinar quiénes aceptan ("*opt in*"[28]) o no ("*opt out*"[29]) el envío de *spams*. En el primer caso, sólo se permite el envío de correo electrónico publicitario si es que el usuario ha manifestado su consentimiento a favor de recibirlos. En el caso del *opt out,* se da la situación inversa, pues sólo se podrá remitir correo electrónico a todo aquel que no haya expresado con antelación su pretensión de no recibir correo electrónico comercial no solicitado[30].

A continuación, nos referiremos a la situación de los dos grandes sistemas legislativos en el mundo, y que adoptan posturas muy distintas:

A) Unión Europea

A nivel comunitario europeo, la normativa aplicable es la directiva 2000/31/CE[31] y la ya citada 2002/58/CE[32]. La primera de ellas establece lo siguiente:

"Artículo 7: Comunicación comercial no solicitada

1. Además de otros requisitos establecidos en el Derecho comunitario, los Estados miembros que permitan la comunicación comercial no solicitada por correo electrónico garantizarán que dicha comunicación comercial facilitada por un prestador de servicios establecido en su territorio sea identificable de manera clara e inequívoca como tal en el mismo momento de su recepción.

2. Sin perjuicio de los dispuesto en las Directivas 97/7/CE y 97/66/CE, los Estados miembros deberán adoptar medidas para garantizar que los prestadores de servicios que realicen comunicaciones comerciales no solicitadas por correo electrónico consulten regularmente las listas de exclusión voluntaria ("opt-out") en las que se podrán inscribir las personas físicas que no deseen recibir dichas comunicaciones comerciales, y las respeten."

[28] Se pronunciaron en favor de esta postura: España, Inglaterra, Austria, Bélgica, Dinamarca, Irlanda, Canadá, Suiza, Australia, Italia y la directiva de la Unión Europea 2002/58/CE.
[29] Se pronunciaron en favor de esta postura: Estados Unidos, México, Japón, Corea del Sur, y la directiva 2000/31/CE.
[30] Cfr. VANINETTI, Hugo, *ob. cit.*
[31] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. Diario Oficial n° L 178 de 17/07/2000 p. 0001 - 0016. Publicado en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:ES:HTML, consultado: 09 /09/2010.
[32] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 /07/2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Diario Oficial n° L 201 de 31/07/2002 p. 0037 – 0047. Publicado en: http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=CELEX:32002L0058:ES:HTML, consultado 09/09/2010.

Por su parte, la directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas, se refiere expresamente al problema del *spam* de la siguiente forma:

"Artículo 13: Comunicaciones no solicitadas

1. Sólo se podrá autorizar la utilización de sistemas de llamada automática sin intervención humana (aparatos de llamada automática), fax o correo electrónico con fines de venta directa respecto de aquellos abonados que hayan dado su consentimiento previo.

2. No obstante lo dispuesto en el apartado 1, cuando una persona física o jurídica obtenga de sus clientes la dirección de correo electrónico, en el contexto de la venta de un producto o de un servicio de conformidad con la Directiva 95/46/CE, esa misma persona física o jurídica podrá utilizar dichas señas electrónicas para la venta directa de sus propios productos o servicios de características similares, a condición de que se ofrezca con absoluta claridad a los clientes, sin cargo alguno y de manera sencilla, la posibilidad de oponerse a dicha utilización de las señas electrónicas en el momento en que se recojan las mismas y, en caso de que el cliente no haya rechazado inicialmente su utilización, cada vez que reciban un mensaje ulterior.

3. Los Estados miembros tomarán las medidas adecuadas para garantizar, que, sin cargo alguno, no se permitan las comunicaciones no solicitadas con fines de venta directa en casos que no sean los mencionados en los apartados 1 y 2, bien sin el consentimiento del abonado, bien respecto de los abonados que no deseen recibir dichas comunicaciones. La elección entre estas dos posibilidades será determinada por la legislación nacional.

4. Se prohibirá, en cualquier caso, la práctica de enviar mensajes electrónicos con fines de venta directa en los que se disimule o se oculte la identidad del remitente por cuenta de quien se efectúa la comunicación, o que no contengan una dirección válida a la que el destinatario pueda enviar una petición de que se ponga fin a tales comunicaciones.

5. Los apartados 1 y 3 se aplicarán a los abonados que sean personas físicas. Los Estados miembros velarán asimismo, en el marco del Derecho comunitario y de las legislaciones nacionales aplicables, por la suficiente protección de los intereses legítimos de los abonados que no sean personas físicas en lo que se refiere a las comunicaciones no solicitadas".

Como se ve, de la interpretación de ambos artículos debe entenderse que la posición adoptada por la Unión Europea en materia de *spam* ha cambiado, pues en la directiva 2000/31/CE se adopta el enfoque *opt out*, a pesar de no prohibirse que los Estados miembros elijan el sistema *opt in*. En rigor, se deja librado a cada uno de

los estados la posibilidad de adoptar uno u otro sistema, pero garantizando que se consulten y respeten las listas de exclusión voluntaria.

Por otro lado, en la Directiva sobre la privacidad y las comunicaciones electrónicas de 2002, se adopta la posición del *opt in*, pues se prohíbe el envío de mensajes comerciales no solicitados (no sólo se refiere a los mensajes enviados por correo electrónico sino también a los enviados vía SMS o MMS[33]) salvo que se haya obtenido previamente el consentimiento del abonado. Asimismo, se prevé una excepción a este régimen de consentimiento previo, cuando en el marco de la relación proveedor-cliente ya existente, la empresa que obtuvo los datos de un cliente puede utilizarlos con fines de comercialización de productos o servicios similares a los que ya fueron vendidos. No debe perderse de vista que, en todos los casos, se debe otorgar al usuario la posibilidad de oponerse al envío de *spam* de manera sencilla y sin cargo alguno, y que en todos los casos, el remitente deberá identificarse de manera clara e inequívoca, además de proveer una dirección válida a la que el destinatario pueda enviar una petición en la que se solicite se ponga fin a tales comunicaciones.

B) Estados Unidos

En Estados Unidos, las soluciones legislativas han sido variadas en cada uno de sus Estados. Desde leyes que prohíben el correo electrónico comercial no solicitado enviado a una dirección de e-mail de determinado Estado o desde un ordenador de ese mismo Estado (Washington), hasta normas que imponen la obligatoriedad de incluir un número de teléfono gratuito o una dirección de correo electrónico para que el receptor pueda notificar que no desea que le sigan enviando más mensajes no solicitados (*Business and Professsions Code* de California)[34].

A nivel federal, rige desde el año 2003 la "*Controlling the Assault of Non-Solicited Pornography and Marketing Act*"[35] (más conocida como *CanSpam Act*), en la

[33] SMS hace referencia al *"Short Message Service"*, mientras que MMS se refiere al *"Multimedia Message Service"*, ambos servicios de mensajería de texto y multimedia respectivamente que se envían a través de la telefonía móvil.
[34] Cfr. VANINETTI, Hugo, *ob. cit*.
[35] Puede consultarse su texto en inglés en: http://www.legalarchiver.org/cs.htm, consultado 10/10/10.

cual no se prohíbe el *spam*, sino que especifica las condiciones de su envío, so pena de sanciones económicas muy elevadas e incluso penas privativas de libertad. Entre las condiciones de envío, se establecen las siguientes: se prohíbe que se utilicen direcciones falsas o engañosas y que se incluyan textos artificiosos en el "asunto"; que el mensaje explique que se trata de un mensaje publicitario; y que se incluya una dirección física en EE.UU.[36]. En cuanto a las penas, la ley impone multas de hasta U$S 2.000.000 y penas de prisión de hasta 5 años (sección 5).

En cuanto a la disposición más importante de la ley, la *CanSpam Act* establece que la Comisión Federal de Comercio debe encargarse de la creación de un registro nacional (*"Do-Not-E-Mail-Registry"*), en donde podrían inscribirse los usuarios que no desearan recibir mensajes publicitarios; de ello, se evidencia que se adopta una postura de *opt out,* contraria a la tendencia europea comunitaria y estatal mayoritaria.

En otro orden de ideas, la jurisprudencia norteamericana también se ha referido a la cuestión, contando con una copiosa cantidad de fallos. Podemos encontrar dos tipos de casos: aquellos donde quien demanda es el proveedor de servicios de Internet, y aquellos donde quien demanda es el usuario de Internet.

Entre los primeros casos, es menester destacar *"American Online vs. LCGM"* y *"Compuserve vs. Cyber Promotions"*, donde los dos proveedores de servicio de Internet más grandes de los EE.UU demandaron a empresas que enviaron miles de correos electrónicos no solicitados a sus clientes. Se acusó a las empresas de *spam* de haber violado el derecho de propiedad de los proveedores, pues no sólo se aumentan los gastos técnicos por procesar cada transmisión de mensaje no solicitado, sino que también - en estos casos en particular - se utilizaron indebidamente sus nombres como remitentes. La defensa de las demandadas se basó en que el envío de correo electrónico está amparado por la libertad de expresión de la primera enmienda, y que Internet es un "medio público" por el cual pueden ofrecer sus servicios. Finalmente, en su resolución los tribunales intervinientes en cada caso estimaron procedentes ambas demandas, obligando a los demandados a cesar en sus envíos e indemnizar a los demandantes[37].

[36] Cfr. FERNANDEZ DELPECH, *ob. cit.*, p. 322 a 324.
[37] Cfr. PLAZA SOLER, Juan Carlos, "Los correos electrónicos comerciales no solicitados en el derecho europeo y norteamericano", Ponencia II Congreso Mundial de Derecho Informático. Madrid. 2002, publi-

Entre los casos en los que quien demanda es el propio usuario, debe destacarse "*Mark Ferguson vs. FriendFinders Inc*"[38], donde se condenó a la empresa acusada de enviar *spam* a cesar en su actividad y de indemnizar al demandante. Entre los argumentos técnicos para llegar a la sentencia condenatoria, se consideraron los siguientes:

"El envío de un correo electrónico controla parte de la computadora desde que ingresa hasta que es eliminado de la misma mediante la papelera de reciclaje. El spam priva al usuario final de usar el sistema de correo mientras se produce la bajada del mail. Además, del tiempo que se pierde, también se consideran los costos de conexión a cargo del usuario final, quien debe pagar los minutos de tarifa telefónica y de servicio de Internet que lleva el proceso de bajada del correo. Cuando un correo electrónico entra a una computadora desde el servidor de correo, la información que representa queda impresa en la computadora del usuario. Al borrar ese correo, quedan agujeros en el sistema que se llama fragmentación. Esta fragmentación causa daños físicos al sistema, haciendo lento al procesador. Aun cuando se haga correr el programa de desfragmentación, se causa un esfuerzo y desgaste del disco rígido. Por lo tanto, el correo electrónico no solicitado causa daños físicos en la propiedad personal del usuario"[39].

2.3. EL "*SPAM*" EN EL DERECHO ARGENTINO

Nuestro país no es ajeno a la problemática descripta, por el contrario, la Argentina ostenta nada menos que el cuarto lugar dentro de los países productores de *spam,* detrás de Estados Unidos, China y Rusia[40]. Como dato adicional, debe destacarse que los tres proveedores de Internet más populares: *Speedy* de Telefónica, Arnet de Telecom y Fibertel figuran en el top 10 de los peores ISP del mundo, pues son los que más apoyan al *spam,* ya sea vendiendo sus servicios a *spammers* a sa-

cado en: http://www.ieid.org/congreso/ponencias/Plaza%20Soler,%20Juan%20Carlos.pdf, consultado: 10/10/10.

[38] *Ferguson vs FriendFinders Inc*., Corte de Apelaciones de California, Primer Distrito, 02/01/2002. Puede consultarse su texto en inglés en: http://www.spamlaws.com/cases/ferguson.html, consultado: 10/10/10.

[39] La traducción pertenece al Dr. Fernández Delpech, *ob. cit.*, p. 325.

[40] Cfr. http://www.spamhaus.org/statistics/countries.lasso. La organización internacional Spamhouse, presenta el tema de los países con mayor producción de *spam* de la siguiente manera: "La mayor parte del mundo sufre el problema del *spam*. Sin embargo, algunos países hacen muy poco para disuadir a los *spammers* que operan dentro de sus fronteras. Estos países se conviertan en refugios seguros para las operaciones de *spam* que afectan a todo el mundo, incluyendo a sus propios habitantes. Los países con el mayor número de *spammers* que operan dentro de sus redes son por lo general los que tienen leyes de *spam* pobres o inexistentes."

biendas de su accionar ilícito, o bien no haciendo nada para evitar que los *spammers* operen desde sus redes[41].

Esta realidad, a su vez, está motivada no sólo por la connivencia de los ISP que venden sus servicios a los *spammers,* sino principalmente por una causa estrictamente jurídica: la inexistencia de una ley que regule el tema. Creemos que el vacío legal señalado debe suplirse cuanto antes, pues a pesar de que se han propuesto algunos proyectos de ley[42] que regulan el *spam*, aún no se ha dictado una ley *antispam* específica.

Sin embargo, a pesar de la carencia de una legislación particular en Argentina, desde la doctrina informática nacional más calificada[43], se ha dicho que la propia Ley 25.326 de Protección de Datos Personales es hoy por hoy la herramienta jurídica más importante que los usuarios argentinos de Internet que reciben mensajes de correo electrónico no solicitado tienen a su alcance. Resultan aplicables no sólo los principios generales antes señalados, sino específicamente el art. 27, que prescribe lo siguiente:

"*Art. 27.- Archivos, registros o bancos de datos con fines de publicidad:*

1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.

2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.

---

[41] Cfr. http://www.spamhaus.org/statistics/networks.lasso. *Spamhouse* se refiere al top 10 de los peores ISP del mundo de la siguiente forma: "Las redes que aparecen en esta página a sabiendas proveen servicio a las organizaciones criminales de *spam* e ignoran los informes de *spam* de los sistemas *anti-spam* y de los usuarios de Internet. Estas redes son de facto "Paraísos del *Spam*", desde donde los *spammers* operar libremente y con pleno conocimiento de los administradores de red. En el nombre de las ganancias, estas diez redes hacen la vista gorda a las bandas criminales de spam en sus redes".

[42] Se destacan, entre otros, los siguientes: Anteproyecto de Ley de Protección Jurídica del Correo Electrónico" elaborado por la Secretaría de Comunicaciones, a través de la resolución 333/2001, del 10/9/2001(Puede consultarse en: http://www.protecciondedatos.com.ar/, consultado 12/10/2010.); Proyecto de Ley de "Régimen Legal para las Comunicaciones Comerciales por vía Electrónica" del Diputado Guillermo Alchouron (se encuentra en la Cámara de Diputados; puede consultarse en: http://www.hfernandezdelpech.com.ar/ProyectosYanteproyectosArgProyLeyRegimenLegalComuniComerViaElectr.htm, consultado12/10/2010).

[43] Cfr. SOBRINO, *ob. cit.*, p. 73 y ss.; FARINELLA, Favio, "Algunas notas sobre *spamming* y su regulación", Alfa-Redi Revista de Derecho Informático, No. 94, Mayo de 2006, publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=6102, consultado 10/10/10; FERNANDEZ DELPECH, *ob. cit.*, p. 326 y 327; VANINETTI, *ob. cit.;* HOCSMAN, *ob. cit.*, p. 207.

3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo."

En forma coincidente, al reglamentarse este artículo, el decreto 1558/2001[44] dispuso que "*En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información".*

Del juego de estas disposiciones, se infiere que el sistema adoptado por nuestro país es el *opt in,* pues la licitud de la recolección de datos con fines publicitarios o para establecer perfiles de los usuarios/consumidores queda supeditada al consentimiento libre e informado de éstos (o que sus datos figuren en "documentos accesibles al público", que es una excepción prevista en el art. 5). Asimismo, los responsables de dichas bases de datos tienen - para todos los casos - la obligación de informar al usuario la posibilidad de solicitar el "retiro" o "bloqueo" de los datos cuya titularidad le correspondan; también el decreto impone la obligación de informar el nombre del responsable o usuario del banco de datos que proveyó la información, siempre y cuando exista un pedido previo por parte del interesado.

Sobre este tema, Sobrino nos da una particular interpretación del artículo 27. Entiende el autor que no sólo el origen de los datos tiene que ser lícito (en el sentido de que deben figurar "en documentos accesibles al público" o que "hayan sido facilitados por los propios titulares u obtenidos con su consentimiento"), sino que la persona que envía *spams*, tiene que comprobar y verificar que la base de datos (de direcciones de e-mail) que utiliza, ya sea propia o entregada por un tercero, cumple efectivamente con la Ley de Protección de Datos Personales. Si el *spammer* no cumpliera con ello, - concluye el autor - no solamente sería ilegal el envío de *spams*, sino que quien los remitió también resultaría legalmente responsable, dado que es partícipe en la difusión de los datos personales (direcciones de e-mail) obtenidos antijurídicamente[45].

El razonamiento no es más que una aplicación de la "teoría del fruto del árbol envenenado", la cual, en pocas palabras, significa que nadie puede sacar prove-

[44] *B.O.*, 03-XII-2001.
[45] Cfr. SOBRINO, *ob. cit.*, p. 72 a 75.

cho de algo que se obtuvo ilegalmente (si el árbol está envenenado, *ergo* su fruto también lo estará). En este caso, no podría el *spammer* alegar que el envío de *spam* es lícito a pesar de sustentarse en bases de datos obtenidas ilegalmente.

Si bien coincidimos en la aplicación de estas soluciones, también estamos de acuerdo con Vaninetti en que es necesario advertir que *"esta ley sólo sería una solución mínima ante esta práctica pues sólo funcionaría cuando el receptor solicita la eliminación de sus datos incluidos en ese banco. Sería menester, pues, crear una ley más precisa que regulara al spam, porque la publicidad comercial es una actividad perfectamente legítima que se encuentra en nuestro país protegida por la Constitución Nacional, que consagra el derecho a ejercer toda industria lícita"*[46].

En otro orden de ideas, en cuanto a las soluciones esbozadas por la jurisprudencia nacional, ésta ha tenido oportunidad para pronunciarse en "Tanús c. Cosa s/Habeas Data" [47], que fue el primer y único fallo - hasta ahora - en la Argentina sobre *spam*.

En él se ha sentado jurisprudencia de la siguiente forma: "*la actividad de los demandados (spammers) comporta una invasión en la esfera de la intimidad de los actores y de su tranquilidad, por cuanto se ven sometidos a la intromisión en sus datos personales que se ve reflejada en el envío masivo de mensajes no solicitados, y la oferta de comercialización de esos datos que efectúan a terceros, cuando ya habían requerido el cese del envío y el bloqueo de esa información de la base respectiva, conforme lo previsto por el art. 27 de la ley 25.326. Y en esta faceta de la vida íntima de las personas – que se pone de manifiesto con el avance de las comunicaciones – merece el resguardo del ordenamiento jurídico como los otros aspectos de ella, contemplados en el art. 1071 bis del Código Civil*".

En cuanto a los perjuicios causados, se dijo que "*Respecto del daño que los actores alegan que les origina la recepción del mentado correo masivo no solicitado, ya*

[46] VANINETTI, Hugo, *ob. cit.*

[47] Tanús, Gustavo Daniel y Palazzi, Pablo c/ Cosa, Carlos Alberto y otro s/Hábeas Data (art. 43 C.N.), Juzgado Civil y Comercial Federal Nro. 3, Sec. 6, 07/04/06, publicado en: http://www.protecciondedatos.com.ar, consultado: 09/09/2010.
Debe aclararse que los Dres. Gustavo Tanús y Pablo Palazzi son abogados especialistas en derecho informático, y que, basándose en la Ley de Protección de Datos Personales fueron quienes lograron no sólo la primera medida cautelar sino también en primer sentencia condenatoria en Argentina contra un "spammer" o remitente de correo electrónico no solicitado, que ofrecía precisamente bases de datos con el fin de realizar posteriores usos publicitarios.

sea por el costo económico como por el tiempo que esa actividad insume, […] (los informes periciales), *[…] dan cuenta del significado del término "spam" y del daño que se ocasiona a los receptores de los mensajes atento al tiempo de descarga que requiere identificarlos, seleccionarlos y borrarlos, así como también al incremento en el costo de recepción y procesamiento. Ello genera, además, la necesidad de implementar sistemas para bloquear, y aun lograr, la protección de los virus que pueden dispensar*".

Finalmente, se condenó a los demandados a permitir que los actores tengan acceso a los datos personales que figuran en su base de datos, y a su posterior eliminación y cese en el tratamiento de los mismos.

En síntesis, creemos que el tema del correo electrónico no deseado no ha sido resuelto definitivamente en el derecho comparado, teniendo diversas formas de regulación que van desde normas éticas, pasando por normas jurídicas permisivas, hasta llegar a normas prohibitivas. En nuestro derecho, la solución aún se encuentra en estado de gestación, pues no ha tenido recepción en una ley específica, ni tampoco la problemática ha sido lo suficientemente debatida, al margen de que tan sólo unos pocos autores en la doctrina informática nacional, y un solo fallo representativo.

3. EL MONITOREO LABORAL DEL CORREO ELECTRÓNICO

Para finalizar el presente capítulo, proponemos analizar un problema frecuente en el marco de las relaciones laborales, que son los controles a la utilización del correo electrónico como herramienta de trabajo.

A continuación haremos una breve introducción de la situación referida, para luego exponer las posturas que se han elaborado para resolverla tanto en el derecho comparado como en la legislación y jurisprudencia argentina.

3.1. ASPECTOS GENERALES

Una de las situaciones de dudosa resolución en el plano jurídico que suele cometerse a través del correo electrónico, y que ha devenido en una práctica común en estos tiempos es aquella que consiste en el monitoreo de los e-mail recibi-

dos y emitidos por los trabajadores durante su jornada laboral. Debe aclararse que, en la hora actual, puede inscribirse como parte de esta problemática al control de los mensajes enviados y recibidos por el trabajador, ya sea a través del servicio de mensajería instantánea (*Instant Messaging*) o a través de las redes sociales, pues ambas herramientas han proliferado de manera fértil en el ámbito laboral en el último tiempo.

Ahora bien, debe advertirse que de la situación apuntada se plantea una tensión entre dos derechos constitucionales: propiedad e intimidad. Según Hocsman, de la mayor importancia que se le dé a alguno de estos derechos por sobre el otro, obtendremos una respuesta distinta, que da lugar a soluciones totalmente opuestas.

Sostiene el citado autor que, si otorgamos mayor preponderancia al derecho de propiedad, deberemos concluir que el empleador actúa lícitamente ejerciendo su derecho a controlar los bienes de la empresa que dirige. Parte de la idea de que el empleador es titular de los medios de producción, y tanto la computadora, el software como las direcciones de e-mail entran en esa categoría. Así, el trabajador dispondría de esa dirección sólo a efectos de la actividad laboral, y por lo tanto el control sobre ella, en principio, no afectaría su privacidad[48]. A este argumento, deben sumarse otros dos de importancia: por un lado, que el empleador tiene una responsabilidad refleja o indirecta por el hecho de un dependiente, y que por tal motivo puede monitorear el uso de esta herramienta para evitar conductas de parte del trabajador que puedan afectar a su empresa, y además, se advierte que existe una posibilidad de que por este medio pueda facilitarse información confidencial y secretos inherentes a una empresa[49].

Por el contrario, si damos mayor preponderancia al derecho a la intimidad por sobre la propiedad, necesariamente deberemos concluir que la práctica del monitoreo laboral del e-mail constituye efectivamente una ilegalidad si es que no hay motivos razonables para tal intromisión (entra en juego también el principio constitucional de razonabilidad en la reglamentación de los derechos fundamentales)[50].

[48] Cfr. HOCSMAN, *ob.cit.*, p. 184.
[49] Cfr. VANINETTI, *ob. cit.*
[50] Cfr. HOCSMAN, *ob.cit.*, p. 184 y 185.

Tal control, entonces, implicaría, al decir de Vaninetti, *"una injerencia indebida en el derecho a la intimidad del trabajador, pues se contravienen expresas disposiciones tuitivas del secreto de las comunicaciones y de su privacidad"*[51].

3.2. EN EL DERECHO COMPARADO

La situación en el derecho comparado no se ha mantenido al margen de las posturas recientemente reseñadas, y las soluciones normativas han oscilado entre ambos extremos, siendo las leyes europeas las más respetuosas de la privacidad de los trabajadores, mientras que las leyes de la mayoría de los estados norteamericanos son favorables a los intereses empresariales, vale decir, son las políticas internas de cada compañía las que terminan por definir si el trabajador puede o no usar el e-mail como herramienta laboral, y en qué circunstancias[52].

A continuación, pasaremos revista a las principales normas y casos que se han dictado a los fines de regular la cuestión tanto en EE.UU. como en distintos países de Europa:

A) Estados Unidos: según Hocsman, la jurisprudencia está del lado de los empresarios y de su posible control y monitoreo, mientras que a nivel legislativo, existen varias leyes de protección a las comunicaciones – cita la *Federal Wiretapping Act* y la *Electronic Communications Privacy Act* – en las cuales se prohíbe la interceptación de las comunicaciones electrónicas, salvo excepciones, como el consentimiento previo del empleado. A nivel estadual, la tendencia se repite, salvo el Estado de Connecticut, que obliga a las empresas a informar a sus trabajadores tales controles[53].

B) Unión Europea: la situación en Europa no es del todo pacífica. A nivel comunitario europeo no existe una norma que regule específicamente el tema; tam-

[51] VANINETTI, *ob. cit.*
[52] Cfr. VANINETTI, *ob. cit.*
[53] Cfr. HOCSMAN, *ob. cit.*, p. 188.

poco hay una solución que se siga de manera uniforme, por lo cual reseñaremos los distintos criterios que se han sostenido a nivel nacional:

- Francia: en este país es de rigor citar el caso "Omof, Frederic v. Societe Nikon France S.A.". Allí se resolvió que el empleador violaba el derecho a la intimidad de su trabajador al haber accedido a la correspondencia electrónica personal que este último recibía y emitía, aunque mediara prohibición de parte de la empresa. La Corte de Casación dispuso en el aludido fallo *"que el empleado tiene derecho, incluso en tiempo y lugar de trabajo, al respeto de la intimidad de su vida privada; que esto implica en particular el secreto de su correspondencia; que el empleador no puede desde entonces, sin violación de esta libertad fundamental, tomar conocimiento de los mensajes personales emitidos por el dependiente gracias a una herramienta informática puesta a su disposición para su trabajo y esto mismo en caso que el empleador hubiese prohibido una utilización no profesional del ordenador"*[54]. Vale aclarar que, éste no ha sido el criterio predominante en el derecho extranjero.

- España: a nivel legislativo, rige la Ley Orgánica 1/1982, del 5/5/1982, de Protección Civil del Derecho al Honor, la Intimidad Personal y Familiar y a la Propia Imagen[55], que establece en su art. 1 que: *"el derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen garantizado en el art. 18 Constitución Española será protegido civilmente frente a todo tipo de intromisiones ilegítimas de acuerdo a lo establecido en la presente Ley Orgánica"*. Asimismo, el art. 7 inc. 2, proclama que se considerará como intromisión ilegítima a *"la utilización de escuchas, dispositivos ópticos o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción"*.

Si bien la legislación parecería prohibir la intromisión del empleador en el e-mail laboral, la misma no es del todo específica para el caso en análisis, y es por ello que la jurisprudencia española se ha inclinado por la postura de permitir la fiscaliza-

[54] El fallo es citado por VANINETTI, Hugo, *ob. cit.* Asimismo, la traducción es del mencionado autor.
[55] Puede consultarse su texto en: http://noticias.juridicas.com/base_datos/Admin/lo1-1982.html, consultado 10/10/10.

ción de los correos laborales de los empleados, sin que ello vulnere su intimidad ni privacidad[56].

El precedente más importante es "Deutsche Bank". En él, la Sala de lo Social del Tribunal Superior de Justicia de Catalunya resolvió que es viable el despido de un empleado del Deutsche Bank que durante cinco semanas envió 140 correos electrónicos cuyo contenido era de carácter sexista, humorístico y, en algunos casos, obscenos, y que, por supuesto, eran ajenos a la actividad profesional de su empresa. La sentencia admitió que la empresa accediera al correo electrónico de su empleado con la finalidad de comprobar esas irregularidades[57].

Cabe señalar que, si bien la mayoría de los autores citan este ejemplo, Fernández Delpech advierte que en este caso el despido se fundó en el incumplimiento laboral y no en lo relativo a la privacidad. En este sentido, el citado autor entiende que "*se debatió la procedencia de un despido disciplinario, […] y que los motivos alegados* (el uso del correo electrónico en el lugar y horario de trabajo)*, era causal suficiente para justificarlo […] No se entró ni en el análisis de la privacidad del e-mail ni tampoco a determinar si la empresa tenía o no derecho al control que había posibilitado la causal de despido. […] es por ello que, no debemos tomar este fallo como un reconocimiento judicial en España del derecho de las empresas al control laboral del correo electrónico de los trabajadores.* [58]

- Reino Unido: En Inglaterra la Ley de Regulación de Poderes de Investigación permite a los empleadores el "acceso rutinario" al correo electrónico y a las llamadas telefónicas de sus empleados, sin el consentimiento de éstos, en tanto hubiese una finalidad legal para dicho control. La ley incluso va más allá del simple "acceso", y faculta al empleador a borrar los mensajes que el trabajador haya enviado utilizando los medios puestos a su disposición por la empresa. Para llevar a cabo estas inspecciones es necesaria la "sospecha de conducta criminal" o la necesidad de "garantizar el cumplimiento de las normas de conducta internas"[59].

[56] Cfr. GALDÓS, Jorge Mario, "Correo electrónico, privacidad y daños", Revista de derecho de Daños 2001-3-157, publicado en: http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/galdos.pdf, consultado 10/10/10, p. 18.
[57] El caso es citado por GALDÓS, Jorge Mario, *ob. cit.*, p. 18.
[58] FERNÁNDEZ DELPECH, Horacio, *ob. cit.*, p. 312.
[59] Cfr. HOCSMAN, *ob. cit.*, p. 188.

3.3. EN LA LEGISLACIÓN ARGENTINA

En nuestro país no existe ninguna norma legal que expresamente regule las facultades del empleador relativas al monitoreo del e-mail en el ámbito laboral.

Debe recordarse que en nuestro país la Ley de Contrato de Trabajo 20.744[60] es la que rige las relaciones entre empleadores y trabajadores desde el punto de vista contractual individual. Si bien no existe una disposición que se refiera específicamente al supuesto en análisis, creemos que son aplicables sus principios generales.

Como punto de partida, debe tenerse en cuenta que en toda relación laboral debe regir el principio de buena fe recíproca (art. 63 L.C.T.[61]), el cual se extiende no sólo a las conductas a las que las partes expresamente se obligaron en el contrato de trabajo, sino a todos aquellos comportamientos que sean consecuencia del mismo, apreciados con criterio de colaboración y solidaridad (art. 62 L.C.T.[62]). Asimismo, entre las facultades específicas del empleador se encuentran la organización económica y técnica de la empresa como también su dirección (art. 64 y 65 L.C.T.[63]), mientras que entre las obligaciones del trabajador se halla el deber de fidelidad, por el cual debe guardar reserva o secreto de las informaciones a las que tenga acceso (art. 84 L.C.T[64]). Finalmente, también resultan de aplicación las disposiciones relativas a controles que el empleador puede efectuar sobre el trabajador, que si bien no aluden al supuesto del monitoreo laboral de los e-mails, sí se refiere a la salvaguarda

[60] *B.O.*, 27-IX-1974.

[61] *Art. 63. – (Principio de la buena fe). Las partes están obligadas a obrar de buena fe, ajustando su conducta a lo que es propio de un buen empleador y de un buen trabajador, tanto al celebrar, ejecutar o extinguir el contrato o la relación de trabajo.*

[62] *Art. 62. – (Obligación genérica de las partes). Las partes están obligadas, activa y pasivamente, no sólo a lo que resulta expresamente de los términos del contrato, sino a todos aquellos comportamientos que sean consecuencia del mismo, resulten de esta ley, de los estatutos profesionales o convenciones colectivas de trabajo, apreciados con criterio de colaboración y solidaridad.*

[63] *Art. 64. – (Facultad de organización). El empleador tiene facultades suficientes para organizar económica y técnicamente la empresa, explotación o establecimiento.*
Artículo 65. – (Facultad de dirección). Las facultades de dirección que asisten al empleador deberán ejercitarse con carácter funcional, atendiendo a los fines de la empresa, a las exigencias de la producción, sin perjuicio de la preservación y mejora de los derechos personales y patrimoniales del trabajador.

[64] *Art. 85. – (Deber de fidelidad). El trabajador debe observar todos aquellos deberes de fidelidad que deriven de la índole de las tareas que tenga asignadas, guardando reserva o secreto de las informaciones a que tenga acceso y que exijan tal comportamiento de su parte.*

de los bienes y herramientas de trabajo de propiedad de la empresa (arts. 70, 71 y 72 L.C.T.[65]).

En base a este conjunto de normas, surge con claridad que el empleador tiene un derecho de propiedad sobre los medios de trabajo; el e-mail como herramienta para el cumplimiento de la prestación a la que se comprometió el trabajador, forma parte del concepto de medios de trabajo. Ahora bien, ese derecho de propiedad, también implica la facultad de establecer sistemas de control que tengan por objeto salvaguardar los bienes de la empresa, siempre y cuando se respete la dignidad y privacidad del trabajador y se pongan en conocimiento de la autoridad de aplicación, de la organización sindical que represente a los trabajadores, y del propio trabajador.

Ahora bien, esa facultad de fiscalización, como toda facultad del empleador, está supeditada a que su ejercicio no resulte violatorio de los derechos del trabajador. Llevado al caso en particular, la facultad de establecer controles sobe los e-mails es legítima en tanto no se afecte la privacidad e intimidad del trabajador. De este modo, se plantea una tensión entre dos derechos constitucionales en juego: el derecho a la intimidad del trabajador (art. 19 C.N) y el derecho a la libertad de empresa (art. 14 C.N.) y a la propiedad del empleador (art. 14 y 17 C.N.).

De esta tensión, surge un nuevo interrogante: si es posible compatibilizar ambos extremos, o si, deberá elegirse uno por sobre otro. Como se dijo con anterioridad, según Hocsman, tanto en el derecho comparado como la mayoría de los autores de la doctrina nacional se plantea el tema en términos de una disyuntiva, vale decir, que el tema debiera ser regulado o bien a favor del empleador, permitiendo en todo caso el monitoreo de los contenidos del e-mail laboral, o bien en favor del

[65] *Art. 70. – (Controles personales). Los sistemas de controles personales del trabajador destinados a la protección de los bienes del empleador deberán siempre salvaguardar la dignidad del trabajador y deberán practicarse con discreción y se harán por medios de selección automática destinados a la totalidad del personal. Los controles del personal femenino deberán estar reservados exclusivamente a personas de su mismo sexo.*
Art. 71. – (Conocimiento). Los sistemas, en todos los casos, deberán ser puestos en conocimiento de la autoridad de aplicación.
Art. 72. – (Verificación). La autoridad de aplicación está facultada para verificar que los sistemas de control empleados por la empresa no afecten en forma manifiesta y discriminada la dignidad del trabajador.

trabajador, prohibiéndose para todos los casos la intromisión en su correspondencia electrónica, pues se afectaría su derecho a la intimidad[66].

Creemos que la cuestión admite matices, y no debiera ser planteada en términos de oposición; por el contrario, pensamos que se trata de dos derechos absolutamente compatibles. Coincidimos con Fernández Delpech en que "*se mezclan dos temas que tienen que tener dos soluciones normativas diferentes: la garantía de la confidencialidad del trabajador, y las facultades del empleador con relación a las políticas de uso del correo electrónico y de Internet en el lugar de trabajo*"[67].

Es por ello que para llegar a una solución justa, debe partirse del principio de libertad de empresa del empleador para establecer las condiciones de uso de las herramientas de trabajo. De hecho, ya se estila en la práctica resolver el tema a nivel convencional particular o a modo de reglamento de empresa, comunicando al trabajador la política de la empresa en relación al uso del correo electrónico. Según Vaninetti, generalmente, estas cláusulas especifican las condiciones, frecuencia y oportunidad en el envío y recepción de los mensajes de correo electrónico y/o de redes sociales y/o de mensajería instantánea desde los equipos de la empresa, y también prohíben el uso personal y la divulgación de informaciones confidenciales de la empresa[68]. A ello agregamos que la patronal puede establecer sanciones, en tanto sean proporcionadas a la falta o al incumplimiento demostrado por el trabajador (arts. 67 y 68 L.C.T[69]).

Respecto a esto último, entendemos que el despido no es una sanción, y que no forma parte de las facultades disciplinarias del empleador[70]. Por más que se in-

[66] Cfr. HOCSMAN, *ob.cit.*, p. 184.
[67] FERNÁNDEZ DELPECH, Horacio, *ob. cit.*, p. 316.
[68] Cfr. VANINETTI, *ob. cit.*
[69] *Art. 67. – (Facultades disciplinarias. Limitación). El empleador podrá aplicar medidas disciplinarias proporcionadas a las faltas o incumplimientos demostrados por el trabajador. Dentro de los treinta (30) días corridos de notificada la medida, el trabajador podrá cuestionar su procedencia y el tipo o extensión de la misma, para que se la suprima, sustituya por otra o limite según los casos. Vencido dicho término se tendrá por consentida la sanción disciplinaria.*
Art. 68. – (Modalidades de su ejercicio). El empleador, en todos los casos, deberá ejercitar las facultades que le están conferidas en los artículos anteriores, así como la de disponer suspensiones por razones económicas, en los límites y con arreglo a las condiciones fijadas por la ley, los estatutos profesionales, las convenciones colectivas de trabajo, los consejos de empresa y, si los hubiere, los reglamentos internos que éstos dictaren. Siempre se cuidará de satisfacer las exigencias de la organización del trabajo en la empresa y el respeto debido a la dignidad del trabajador y sus derechos patrimoniales, excluyendo toda forma de abuso del derecho.
[70] Cfr. MIROLO, René Ricardo (dir.), "Curso del Derecho del Trabajo y de la Seguridad Social", Editorial Advocatus, Córdoba, 2003, Tomo I, pág. 340 y 341.

cumplan las condiciones de uso del e-mail, no podrá establecerse el despido como sanción. Ello, sin embargo no obsta a que el uso del correo electrónico de forma indebida pueda efectivamente acarrear un despido causado. Para que ello ocurra, la utilización del e-mail debe haber configurado una injuria que, por su gravedad, no consienta la prosecución de la relación laboral (art. 242 L.C.T.[71]).

Ahora bien, la libertad del empleador debe ceder frente a la privacidad del trabajador. En este sentido, creemos que es ilícito bajo el prisma de la legislación nacional que el empleador pueda acceder a los contenidos del e-mail personal y laboral del empleado, pues, como ya se dijo en reiteradas ocasiones, el correo electrónico es asimilado a la correspondencia epistolar en cuanto a su protección constitucional. La única forma para acceder a ellos sería con autorización judicial fundada en ley (art. 18 C.N.)

3.4. EN LA JURISPRUDENCIA ARGENTINA

La jurisprudencia nacional ha tenido oportunidad de pronunciarse sobre la cuestión en varios fallos[72], dando lugar a los siguientes principios:

- Constituye injuria grave utilizar el servicio de Internet para un emprendimiento particular del trabajador, desatendiendo sus obligaciones específicas e incumpliendo la atención a los clientes de la empresa para la cual presta servicios. Por ende, en ese caso el despido es causado, y por su exclusiva culpa[73].

El citado autor entiende que el despido no es *"la máxima sanción disciplinaria, no sólo porque legislativamente en nuestro país no integra el régimen disciplinario, sino también porque cuando la falta es tan grave que no consiente la continuación de la relación, si el empresario quiere separar de la empresa al trabajador que la ha cometido, recurre a su condición de contratante para hacerlo en uso de una facultad que posee por parte de quien ha cumplido con el contrato y quien no lo ha hecho"*. Aclara además que el despido *"no es una sanción que surja del poder disciplinario del patrono, sino una consecuencia de hechos del trabajador que impide, por su causa, que el contrato de trabajo se mantenga. Las sanciones disciplinarias son todas aquellas que no llegan a disolver el vínculo contractual, y por lo tanto, permiten su subsistencia"*.

[71] *Art. 242. – (Justa causa). Una de las partes podrá hacer denuncia del contrato de trabajo en caso de inobservancia por parte de la otra de las obligaciones resultantes del mismo que configuren injuria y que, por su gravedad, no consienta la prosecución de la relación.*
La valoración deberá ser hecha prudencialmente por los jueces, teniendo en consideración el carácter de las relaciones que resulta de un contrato de trabajo, según lo dispuesto en la presente ley, y las modalidades y circunstancias personales en cada caso.

[72] La mayoría de los fallos citados en esta sección están disponibles en: http://www.hfernandezdelpech.com.ar/JurisprudenciaArg.htm, consultado: 10/10/10.

[73] Cfr. Pereyra, Leandro Ramiro c. Servicios de Almacén Fiscal Zona Franca y Mandatos S.A. s/ Despido, Sala VII de la Cámara Laboral de la Ciudad de Buenos Aires, 27/03/2003.

- Se rechazan los argumentos del empleador cuando alega que se trata de un despido con justa causa por uso indebido del correo electrónico en el lugar de trabajo, cuando en ningún momento precisa cuál es el procedimiento que debió observar el trabajador en el cumplimiento de sus funciones específicas ni cuáles eran las normas internas y/o las instrucciones impartidas por la patronal sobre el uso de la red informática y, más concretamente, cuál era el control que había implementado sobre el uso del correo electrónico por parte de sus empleados[74].

- *"Cuando el empleador contrata por tiempo y no por rendimiento, el trabajador no debe distraer parte de ese tiempo en tareas ajenas y utilizar en forma impropia un medio de comunicación como lo es el correo electrónico, el cual no está destinado al esparcimiento ni puede utilizarse para realizar solapadamente tareas paralelas sino que es provisto evidentemente para facilitar el cumplimiento del objeto de contrato y, en última instancia, para alguna comunicación personal urgente"*[75].

- Debe existir algún tipo de advertencia por parte de la empresa antes de comenzar a operar el sistema informático, en el sentido de advertir que la utilización de tal herramienta estaba estrictamente reservada a cuestiones laborales, ya sea por un manual de instrucciones, un reglamento interno o cualquier otro cuerpo normativo con relación a tal instrumento[76].

- Se rechaza la demanda de despido promovido por el trabajador, atento que utilizó repetida y constantemente su horario y herramienta de trabajo (sistema de correo electrónico) pese a las indicaciones que en contrario le fueran reiteradamente impartidas, para recepcionar y reenviar a través del correo electrónico de la empresa archivos, textos y/o fotografías ajenos a la tarea de la accionada y de alto contenido pornográfico[77].

- No es causa de despido suficiente la mera utilización del correo electrónico para enviar material pornográfico[78]. En el mismo sentido, se sostuvo que el envío y

[74] Cfr. Pereyra, Leandro Ramiro c. Servicios de Almacén Fiscal Zona Franca y Mandatos S.A. s/ Despido, Sala VII de la Cámara Laboral de la Ciudad de Buenos Aires, 27/03/2003.
[75] García, Delia María Del Rosario c/ Y.P.F. S.A. s/ Despido, Sala X de la Cámara Nacional de Apelaciones en lo Laboral, expte. Nro. 9.337/2002.
[76] Cfr. P.R.F. c/ Ceteco Argentina SA s/ despido, Sala I de la Cámara Nacional de Apelaciones en lo Laboral, 29/04/2005.
[77] Cfr. V.R.I c/Vestiditos SA s/despido, Juzgado en lo Laboral Nº 24, 27/05/03.
[78] Cfr. B. M. c/ SGS Société Générale de Surveillance S.A. s/ despido, CN Trab, Sala III, 29/08/03, citado por Hocsman, *ob. cit.*, p. 196.

recepción de material pornográfico por medio de mensajes de correo electrónico en horario de trabajo no fue valorado con gravedad suficiente para configurar una injuria laboral, dada la ausencia de sanciones disciplinarias previas[79].

- Para que exista una justa causa de despido, el empleador debe probar que el trabajador violó la política interna de la compañía sobre el uso de tecnología, y que puso en peligro la seguridad informática y el patrimonio de la misma[80].

Si bien la casuística demuestra que mayoritariamente ha habido resoluciones en favor del trabajador, podemos señalar que no existe un criterio jurisprudencial uniforme y categóricamente definido sobre la materia. Las circunstancias de hecho de cada caso en particular son las que determinan la decisión a favor de una u otra parte.

A modo de colofón, en base a lo expuesto se evidencia que la solución a la tensión entre el derecho a la privacidad de la casilla de e-mail del trabajador y el derecho del empleador a controlar los bienes de su empresa no ha sido única. Sin embargo, teniendo en cuenta la unánime aceptación en equiparar el correo electrónico a la correspondencia epistolar, los principios pretorianos, y desde una posición doctrinaria ecléctica, puede afirmarse que ambos derechos no resultan incompatibles, pues el empleador efectivamente puede delinear las políticas de uso del e-mail, siempre y cuando éstas se circunscriban a lo estrictamente profesional o laboral, sean notificadas de manera fehaciente, y no resulten invasivas de la intimidad del empleado. Es así que el empleador no puede acceder y controlar los mensajes personales del trabajador, por más que éste haya transgredido las reglas de uso. En ese caso, debe limitarse en principio a sancionar al trabajador, y en caso de constituir la falta una injuria grave, puede motivar un despido con justa causa. Sólo en éste último caso, y en tanto se cuente con una autorización judicial, podrá el empleador acceder al contenido de los mensajes, pero sólo a los fines de la prueba de lo alegado.

[79] Cfr. U.J.A. c/ Bayern Argentina S.A. s/ despido, CN Trab, Sala I, 10/04/03, citado por Hocsman, *ob. cit.*, p. 196.
[80] Cfr. Romero Walter Daniel c/Comsat Argentina SA s/despido, Sala III de la Cámara Nacional de Apelaciones en lo Laboral, 23/04/2007.

CAPÍTULO VI
RESPONSABILIDAD CIVIL

Como se pudo apreciar a lo largo de la obra, el avasallante desarrollo de Internet como el medio más representativo de la información y la comunicación automatizada, no sólo implica beneficios para la sociedad; por el contrario, debe advertirse que, con frecuencia, los operadores de la red pueden producir detrimentos injustos que requieren una reparación adecuada e integral.

El presente capítulo tendrá por objeto analizar la responsabilidad de los sujetos que intervienen en los diversos servicios que ofrece Internet por los daños producidos como consecuencia de los distintos problemas jurídicos desarrollados en los capítulos anteriores. Vale decir, se tratarán las responsabilidades derivadas de la publicación de contenidos ilícitos y nocivos y de la afectación al derecho a la intimidad de los usuarios, desde la óptica del derecho civil argentino, excluyendo así el aspecto penal - los denominados delitos informáticos- y administrativo.

1. INTERNET EN EL MODERNO DERECHO DE DAÑOS

En los capítulos previos analizamos algunos de los tantos problemas que se derivan de la utilización de los servicios de Internet, y la necesidad de concebir nuevas instituciones jurídicas, o bien *aggiornar* las ya existentes. Ahora es el turno de referirnos a la responsabilidad civil como institución jurídica fundamental para dar solución a aquéllos problemas.

En la actualidad, resulta indiscutible afirmar que la responsabilidad civil ha evolucionado de sistemas basados en la sola idea de culpa (en sentido lato, comprensivo de la culpa y el dolo), y que hacen hincapié en la obligación del dañador de reparar, a sistemas que admiten pacíficamente la idea de responsabilidad objetiva - no sólo en el ámbito extracontractual sino también contractual - y que ponen en

primer plano al derecho de la víctima a una reparación integral. Tal avance, además, ha derivado en que, hoy por hoy, más que de responsabilidad se hable de un derecho de daños, dado que más allá del conjunto de normas que tradicionalmente estaban destinadas al solo efecto de buscar un resarcimiento, se suman ciertas ideas e institutos de gran importancia que la teoría subjetivista clásica no supo conocer. Así, por ejemplo la prevención del daño, los daños punitivos, la flexibilización de la prueba a través de la teoría de las cargas probatorias dinámicas, las medidas autosatisfactivas como nueva herramienta procesal de tutela anticipada, o la obligatoriedad del seguro para ciertos daños en particular, son temas que forman parte de la agenda del derecho de daños actual. Asimismo, ya se comienza a vislumbrar una suerte de "crisis" de la unicidad del fenómeno resarcitorio, pues han proliferado distintos estatutos especiales destinados a la regulación de la prevención y reparación de daños específicos, que no siempre resultan coincidentes con el régimen general (en cuestiones como la medida de la reparación del daño, los factores de atribución, las eximentes y la prueba). Entre estos estatutos se destacan el de daños a los consumidores, ambientales, nucleares, por actos discriminatorios, por riesgos del trabajo, etc.[1]

Es en esta moderna concepción de responsabilidad donde deben inscribirse los daños informáticos, y particularmente los daños derivados del uso de Internet, ya sea por los contenidos ilícitos y nocivos**,** por la afectación al derecho a la intimidad, a la imagen, al honor, por violación a los derechos de autor, por conflictos derivados de los nombres de dominio, etc.

A continuación, se tratarán expresamente los daños producidos por contenidos ilícitos y por afectación al derecho a la intimidad, detallando en cada caso las responsabilidades que les corresponden a los distintos sujetos que participan en la producción de los mismos.

[1] Cfr. PIZARRO, Ramón Daniel – VALLESPINOS, Carlos Gustavo, "Instituciones de Derecho Privado: Obligaciones", Editorial Hammurabi, Buenos Aires, 1999, Tomo 2, p. 458.

2. RESPONSABILIDAD POR CONTENIDOS ILÍCITOS Y NOCIVOS

El primer aspecto que se tratará será el relativo a los contenidos ilícitos y nocivos[2]. En este sentido, debe tenerse en cuenta que atento a la inexistencia de disposiciones legales específicas en nuestro país, deben aplicarse ciertas pautas jurisprudenciales (concebidas en principio para el tema de la libertad de expresión y los medios de prensa) que resultan útiles para establecer las pertinentes responsabilidades.

En principio, hay que distinguir los sujetos que intervienen en el proceso de transmisión de la información, desde su creación hasta su publicación a través de los sitios web:

- proveedores de información o contenido (*information providers*),
- proveedores de almacenamiento o alojamiento (*hosting providers*), y
- proveedores de acceso (*access providers*).

En este punto nos referiremos a la responsabilidad de cada uno de ellos, a la responsabilidad de los *cybers*, y finalmente a otros supuestos especiales relacionados con la libertad de expresión.

2.1. RESPONSABILIDAD DE LOS PROVEEDORES DE INFORMACIÓN O CONTENIDO

En esta primera parte, se hará referencia a la responsabilidad de los proveedores de información. A tal fin, resulta oportuno recordar que se engloba bajo esta denominación a todos aquellos autores, editores y demás titulares de derechos sobre un sitio web, al cual proveen de contenido con información propia o de un tercero con expresa autorización[3].

[2] En su momento se dijo que el contenido ilícito es aquel que infringe alguna norma jurídica, apuntando -más que a la protección del orden público- a la tutela de los derechos personales y personalísimos, mientras que el contenido nocivo o inadecuado es toda información publicada en Internet que, amparada por la libertad de expresión, es legal aunque sea perjudicial para un determinado tipo de personas.
En esta parte de la obra, estas expresiones son utilizadas como contrarias a ciertos derechos como el derecho a la intimidad, a la autodeterminación informativa, el derecho a la identidad, el derecho al nombre, el derecho a la imagen, etc.

[3] Cfr. FERNÁNDEZ DELPECH, Horacio, "Internet: su problemática jurídica", Editorial Abeledo Perrot, Buenos Aires, 2004, p. 17.

Ahora bien, a los fines de imputar responsabilidad a los proveedores de contenido, resulta útil distinguir según se trate de contenidos propios o bien contenidos de terceros:

A) Responsabilidad por contenidos propios: aquí debe hacerse otra diferenciación. Al decir de Sobrino, *"debemos distinguir la responsabilidad del autor de la nota, artículo o comentario, y la responsabilidad del editor de la página web o del site. Así, la responsabilidad del autor es directa y de carácter subjetivo; en cambio, la responsabilidad del editor es indirecta y de carácter objetivo"* [4].

De esta forma, la responsabilidad del autor es atribuida por su propio accionar, y por un factor subjetivo, de modo tal que debe probarse su culpa o dolo (real malicia). Ello, a su vez, le permite al autor poder eximirse de responsabilidad si prueba que fue diligente, en el sentido de haber cumplido *"aquellas diligencias que exigiere la naturaleza de la obligación, y que correspondiesen a las circunstancias de las personas, del tiempo y del lugar"* (art. 512 Código Civil).

Si se comprueba la responsabilidad del autor, entonces, el editor también será responsable (no por su accionar sino por el del autor), y no podrá pretender eximirse alegando su falta de culpa, pues su responsabilidad es objetiva. Deberá en tal caso probar "algo más" que la no culpa, vale decir, el rompimiento del nexo causal entre el hecho dañoso y el resultado del mismo, y que puede ser un supuesto de caso fortuito, fuerza mayor, culpa exclusiva de la víctima o bien de un tercero por quien no se debe responder. Asimismo, su responsabilidad estará calificada por un factor objetivo, que en este caso podrá ser un deber de garantía del principal por el hecho de un dependiente (el autor), o el ejercicio abusivo de un derecho, o, en su caso, el riesgo creado por la actividad desarrollada, según la postura a la que se adhiera[5].

[4] SOBRINO, Waldo Augusto R., "Internet y la alta tecnología en el derecho de daños", Editorial Universidad, Buenos Aires, 2003, p. 29.

[5] En los capítulos XI y XII de la ya citada obra del Dr. Ramón Daniel Pizarro, "Responsabilidad civil de los medios masivos de comunicación", se exponen con claridad las distintas doctrinas relativas al factor de atribución aplicable para los casos de responsabilidad por daños derivados de informaciones inexactas o agraviantes. En el caso que se analiza, puede afirmarse que se aplican, *mutatis mutandi*, las mismas consideraciones.

Por el contrario, si no se acreditare la responsabilidad del autor, no se le puede imputar obligación resarcitoria alguna al editor, pues éste sólo responde por el accionar culposo del autor.

En el caso en el que la calidad de autor y editor de un sitio web coincidan en una misma persona - que por cierto es el más común -, necesariamente deberá probarse la culpa, ya que primeramente debe analizarse la responsabilidad del autor.

B) Responsabilidad por contenidos de terceros: el tema no es tan sencillo. Aquí se discute si se debe responder por los contenidos de terceros que son incluidos a través de hipervínculos (*links*), y qué factor de atribución resulta aplicable.

Al respecto, Sobrino afirma que tanto los autores como los editores efectivamente deben responder, y que en este caso, el factor de atribución es netamente objetivo, dado que si voluntariamente se incluyó esa información, de manera previa tuvo que haber sido estudiada y analizada. Asimismo, advierte que tratándose de hipervínculos de segundo nivel (*links de links*), las causales de exención de responsabilidad deben ser más flexibles, *"dado que estas derivaciones entre links de links técnica y fácticamente pueden llegar hasta lugares impensados en cualquier parte de la red"*[6].

En contra de esta posición, Bolotnikoff, afirma con acierto que, sostener la responsabilidad de los proveedores de información por los contenidos ajenos, ya sean hipervínculos de primer o segundo nivel, sería tanto como hacer responsable al autor de una publicación por los contenidos de las obras que cita[7]. Por tal motivo, coincidimos con el autor en que resultaría un exceso cargar con tal reparación, y por ende, debe mantenerse el principio inverso: el de irresponsabilidad por contenidos ajenos. Sólo en el caso en el que los *information providers* ejerzan algún tipo de control sobre ellos, o se obligaren a hacerlo (por ejemplo colocando en el sitio web una leyenda que asegura su control, o que asegurare la inexistencia de nocividad en los contenidos incluidos en los *links*), cedería el mentado principio.

[6] SOBRINO, Waldo Augusto, *ob. cit.*, p. 31.
[7] BOLOTNIKOFF, Pablo, "Informática y Responsabilidad Civil", Editorial La Ley, Buenos Aires, 2004, página 207.

2.2. RESPONSABILIDAD DE LOS PROVEEDORES DE ALMACENAMIENTO

Las reglas de responsabilidad para los proveedores de almacenamiento son distintas respecto de aquéllas aplicables a los proveedores de información, ya que su función principal es la de conceder a un sitio web alojamiento en sus servidores. De esta forma, los *hosting providers* carecen de injerencia sobre el contenido[8].

Dada esta particularidad, no hay dudas en que la responsabilidad es subjetiva, por lo cual el ISP de alojamiento sólo respondería por dolo o culpa. Para argumentar tal postura, se sostiene que resulta técnicamente imposible controlar los contenidos de todas las páginas web alojadas en un servidor. Sin embargo, ello no significa que no se tenga un deber de supervisar los contenidos, por el contrario, tal deber existe pero sólo respecto de los actos que se encuentran al alcance técnico del *hosting provider*[9].

Desde otra posición, y sin perder de vista las limitaciones de supervisión de los contenidos, Sobrino entiende que, a modo de principio general, la responsabilidad debe ser objetiva. Consecuencia de ello es la aplicación del factor de atribución emergente del artículo 1113, segundo párrafo, segunda parte[10], del Código Civil. Debe advertirse que, si bien se hace referencia al "riesgo o vicio de la cosa", la doctrina ha ampliado dicha responsabilidad para los daños derivados de actividades riesgosas, ya sea que se hayan producido con cosas o sin ellas[11].

De aceptarse esta extensión, los proveedores de alojamiento no podrían excusarse de responder acreditando su falta de culpa; en todo caso deberían probar la ruptura del nexo de causalidad, es decir, caso fortuito, fuerza mayor, culpa exclusiva de la víctima o de un tercero por el cual no se debe responder.

Sin embargo, el autor advierte que el análisis de las causales de eximentes de caso fortuito y fuerza mayor deberá estar supeditado al nivel del estado actual de la técnica (como se dijo anteriormente, hoy resulta imposible un control de todos los contenidos; no obstante, nada impide que en un futuro sea factible crear un softwa-

[8] Cfr. BOLOTNIKOFF, *ob. cit.*, p. 209.
[9] Cfr. SOBRINO, Waldo Augusto, *ob. cit.*, p. 37.
[10] *Art. 1113: "... si el daño hubiere sido causado por el riesgo o vicio de la cosa, sólo se eximirá total o parcialmente de responsabilidad acreditando la culpa de la víctima o de un tercero por quien no debe responder...".*
[11] Cfr. SOBRINO, Waldo Augusto, *ob. cit.*, p. 38 a 44.

re de control de los contenidos)[12]. En otras palabras, para eximirse de responsabilidad debe probarse que, de acuerdo al estado actual de la técnica, ha resultado imposible evitar el daño. Al decir de Sobrino, esta suerte de atenuación en la aplicación rigurosa de la responsabilidad objetiva implica *"una válvula de escape, muy flexible, que abreva en la realidad tecnológica cambiante"*[13].

Por último, no debe dejar de tenerse en cuenta que el artículo 902 del C.C.[14], también resulta un parámetro objetivo aplicable al caso. Así, por ejemplo, cuanto mayor sea la capacidad operativa y técnica de la empresa de *hosting*, o cuanto mayor sea la probabilidad de que un sitio web afecte derechos de terceros[15], mayor será la obligación de obrar con cuidado y previsión.

2.3. RESPONSABILIDAD DE LOS PROVEEDORES DE ACCESO

En este supuesto, resulta evidente que, dado que la única función que cumplen los proveedores de acceso es brindar la estructura técnica para que los proveedores de almacenamiento tengan acceso a la red, estas empresas no tienen ningún tipo de responsabilidad respecto de los contenidos ilícitos o nocivos[16].

Debe aclararse que, es común que una misma empresa preste el servicio de proveedor de acceso y de proveedor de almacenamiento de manera conjunta e inescindible[17]. En estos casos, surge con evidencia la responsabilidad legal de la empresa, pero no por el hecho de brindar acceso a Internet sino por el servicio de *hosting* prestado, siendo aplicables las consideraciones expuestas *ut supra*.

[12] Cfr. SOBRINO, Waldo Augusto, *ob. cit.*, p. 38.
[13] SOBRINO, Waldo Augusto, *ob. cit.*, p. 39.
[14] *Artículo 902. "Cuanto mayor sea el deber de obrar con prudencia y pleno conocimiento de las cosas, mayor será la obligación que resulte de las consecuencias posibles de los hechos".*
[15] Por ejemplo una página web pornográfica tendrá mayores probabilidades de que en su contenido se incluya pornografía infantil que una página web de un diario reconocido.
[16] Cfr. BOLOTNIKOFF, *ob. cit.*, p. 208.
[17] En nuestro país es el caso de los ISP más importantes: Fibertel, Arnet deTelecom y *Speedy* de Telefónica.

2.4. RESPONSABILIDAD DE LOS *CYBERS*

Cabe preguntarse si los famosos "*cybers*" tienen algún tipo de responsabilidad por los contenidos ilícitos o nocivos.

Para aclarar la situación, es necesario entender que bajo la denominación *cybers* se comprende a todo establecimiento que proveen a sus clientes de computadoras conectadas a Internet, para que sean usadas por un tiempo, contra el pago de un precio cierto en dinero.

De ello se infiere que los *cybers* se limitan a poner a disposición de sus clientes el hardware y el software necesario para navegar por Internet, sin tener injerencia alguna en los contenidos de los sitios web a los que pueden acceder cualquiera de sus clientes. En otras palabras, no son proveedores de contenido, sino meros intermediarios en la oferta del servicio de acceso a la red[18].

Ahora bien, en nuestro país se han dictado - a nivel provincial y/o municipal - normas que imponen a los titulares o responsables de este tipo de establecimientos, la obligación de instalar en todas sus computadoras software de filtrado de contenidos, y de activar dicho filtro sobre páginas nocivas o inadecuadas para menores de edad. Tal es el caso de la ley provincial 9.174[19] y de su decreto reglamentario 378/2004[20], que contienen disposiciones en el sentido apuntado.

Indudablemente que el incumplimiento de dichas normas genera responsabilidad, pero ésta será administrativa y no civil. Es decir, las sanciones que puedan imponerse estarán a cargo de las autoridades de contralor provinciales o municipales destinadas a la aplicación de las normas de policía relativas a estos establecimientos comerciales.

[18] Cfr. BOLOTNIKOFF, *ob. cit.*, p. 234.
[19] *B.O.* Pcia. Cba., 15/12/2004.
[20] *B.O.* Pcia. Cba., 30/04/2004.

2.5. SUPUESTOS ESPECIALES DE RESPONSABILIDAD

A continuación analizaremos dos casos de responsabilidad íntimamente vinculados con la libertad de expresión en Internet, y que, por sus particularidades, merecen un tratamiento especial:

A) Responsabilidad por la actividad anónima de los usuarios: tal como dijimos oportunamente en el capítulo II, uno de los presupuestos de la libertad de expresión del usuario es el derecho al anonimato en Internet, entendiendo por ello a "*la posibilidad de acceder a la red, y de usar sus servicios, sin necesidad de identificarse, ni ser controlado por ello, y sin que sea posible localizar o rastrear las actividades en línea*"[21].

Ahora bien, la posibilidad de operar en la red sin una identificación, genera una situación de tensión entre el anonimato y la responsabilidad civil, ya que el usuario puede realizar de manera oculta una serie de actividades dañosas, y por ende, eximirse de toda responsabilidad derivada de sus actos. Cabe aclarar que ello es posible, dado que la dirección IP asignada por el proveedor de acceso no es una identificación personal del usuario sino una identificación técnica de cada ordenador que accede a la red[22].

Las actividades de los usuarios que generan tal tensión son básicamente aquellas que consisten en introducir a la red contenidos ilícitos o nocivos, destacándose dos casos:

a) incorporación anónima de contenidos a un servidor de alojamiento: este primer caso no reviste demasiada dificultad, ya que la víctima siempre encontrará un responsable: el prestador del servicio de alojamiento. Ello es así, ya que, el hecho de permitir que cualquier usuario anónimo aloje información dañina para terceros en su *hosting server* implica una negligencia grave.

[21] Cfr. ROIG BATALLA, Antoni, "El anonimato y los límites a la libertad en Internet". En COTINO HUESO, Lorenzo (coord.), *ob. cit* , p. 321.
[22] Afirma esta posición el hecho de que las computadoras a las que les fueron asignadas IP fijas, pueden ser operadas por cualquier persona que tenga acceso al lugar en que ellas se encuentran. Pero, además, las IP pueden ser asignadas en forma dinámica, de modo tal que pueden ser otorgadas a distintos ordenadores en forma sucesiva.

De esta forma, si se adopta la postura subjetiva respecto del factor de atribución aplicable al proveedor de alojamiento, para este caso en particular, la culpa debe presumirse.

Por otro lado, si se asume la tesis objetiva, al decir de Parellada, *"debe interpretarse que el prestador de hosting no es un simple locatario de espacio en un servidor en el que ha de alojarse un sitio web, sino alguien que ha encarado lucrativamente una actividad que ha sido organizada de manera que puede resultar dañosa para terceros, y que la creación de ese riesgo de empresa compromete su responsabilidad. Tal responsabilidad, parecería radicar en el defecto de la organización cuando otorga la posibilidad del anonimato a quien tiene derecho al hospedaje de la página"*[23].

b) difamación en páginas web que permiten realizar comentarios anónimos: ciertos sitios web, como ser foros, *blogs*[24], portales de noticias, etc., permiten a sus usuarios realizar comentarios respecto de un hecho, noticia, tema o pregunta en los llamados "libros de visitas". Ahora bien, en los casos en los que dichos comentarios resulten injuriosos o calumniosos respecto de un tercero, éste podrá accionar civilmente – y penalmente si se configuran sendos tipos – a los fines de un resarcimiento por los daños patrimoniales y morales causados.

En un principio, no se discute que el autor de los comentarios tendría una responsabilidad extracontractual, directa y subjetiva, aun siendo anónimo al momento de interponer la demanda. Es así que, nuestra jurisprudencia, en el caso "N. N. s/calumnias e injurias, denunciante S. B." hace lugar a la medida cautelar solicitada por la querellante pues, *"conforme surge de documentación certificada por notario, estaría siendo desacreditada y vulnerada su moral por alguna persona o personas que han publicado mensajes en el blog de Internet sobre su actividad profesional"*. Por ello, el tribunal ordena a la empresa prestataria del servicio del blog que *"extraiga del espacio cibernético, temporariamente y, hasta tanto se esclarezcan los hechos de-*

[23] PARELLADA, Carlos A., *ob. cit.*

[24] Ambos son espacios dentro de un sitio web, propio o de un tercero, en los que se permite a los usuarios expresarse respecto de un tema propuesto por el administrador. En cuanto a las diferencias, los foros de discusión tienen por objeto permitir el debate de distintos temas, con el afán de buscar soluciones y tratar de llegar a una respuesta que resuelva el problema en cuestión; los blogs, por otro lado, se utilizan más para comunicar a una gran audiencia acontecimientos que van sucediendo cronológicamente, permitiendo a los usuarios introducir comentarios.

nunciados, los contenidos que la querella describe como injuriosos y calumniosos, con el objeto de hacer cesar los efectos del delito"[25].

Más allá de la responsabilidad del autor, nada obsta a que el administrador del foro, *blog* o portal de noticias tenga también una obligación de reparar, ya que son ellos quienes tienen el control sobre los comentarios ofensivos o denigrantes, pues dentro de sus facultades pueden modificarlos o eliminarlos. Aquí, la responsabilidad será extracontractual, indirecta (se responde por el hecho del usuario) y objetiva (al decir de Parellada, "*quien organiza este tipo de páginas, ciertamente no ignora que encierran un serio riesgo para que a través de ellas se difame a terceros, pues una norma de experiencia indica que la impunidad que garantiza el anonimato incentiva la malsana decisión de calumniar o injuriar a terceros*"[26]). Asimismo, el administrador será responsable no sólo cuando se desconozca al autor de los comentarios, sino también cuando éste pueda ser identificado, sin perjuicio de su derecho de repetición.

La jurisprudencia nacional ha tenido oportunidad de referirse a este tema en el famoso caso "Jujuy.com"[27], donde se condenó al titular del aludido sitio web al pago de una indemnización por su actividad omisiva y negligente frente a un contenido agraviante o injurioso (en referencia a comentarios vertidos por un visitante anónimo). En este caso en particular, si bien se siguió la tesis objetiva de responsabilidad, el argumento fue distinto al que expusimos con anterioridad (a que es una "actividad riesgosa", y por ende aplicable el 1113 segundo párrafo, segunda parte), pues se asimiló a la informática como una "nueva forma de energía", por ende a una "cosa riesgosa". Se dijo que "*por reunir la informática estos caracteres similares a los de la energía eléctrica, es que creemos que debe aplicarse idéntico régimen. Téngase presente que respecto a los daños causados por la energía se han aplicado los principios de la responsabilidad objetiva, por razón de la potenciación del peligro ínsito en su empleo*".

[25] N. N. s/calumnias e injurias, denunciante S. B., Sala I de la Cámara Criminal y Correccional de la Capital Federal, Causa 38.471, 22/06/2010. Puede descargarse el texto de la resolución en: http://www.diariojudicial.com/contenidos/2010/07/21/noticia_0006.html#, consultado 10/10/10.
[26] PARELLADA, Carlos A., *ob. cit.*
[27] "S.M. y otro c/Jujuy Digital y/o Jujuy.com y/o Sr. Omar Lozano s/ daños y perjuicios", Sala I de la Cámara Civil y Comercial de la Pcia. De Jujuy, 30/06/2004. Publicado en: http://www.hfernandezdelpech.com.ar/JurisprudenciaArgCondenaSitioWeb.htm, consultado 10/10/10.

Si bien compartimos la aplicación de la teoría objetiva, no compartimos la mentada asimilación de la informática a una nueva forma de energía en el sentido del 2311 segunda parte[28], pues creemos que es un argumento rebuscado y que nada tiene que ver con el concepto jurídico de "energía". En todo caso, debió buscarse justificación en que la actividad que lleva adelante la demandada puede considerarse como riesgosa, pues la posibilidad cierta de introducir comentarios escudándose bajo el anonimato entraña un riesgo cierto de difamación e injurias.

En conclusión, ante las distintas actividades anónimas de los usuarios, al margen del respeto al principio de libertad de contenido y de que resulta muy difícil determinar la identidad personal a partir de una identificación técnica, queda claro que Internet no es un espacio donde reine la elusión de las responsabilidades provenientes de situaciones que exceden el derecho de expresión.

B) Responsabilidad de los buscadores de Internet: debe entenderse por buscadores de Internet a "*todos los sitios web que permiten a los usuarios la búsqueda de otros sitios web, a través de un software que rastrea la información que se va agregando a la World Wide Web*"[29].

En estos motores de búsqueda, los usuarios escriben palabras clave, y el buscador, de forma automática las relaciona con el contenido de ciertos sitios web. Cabe aclarar que, previamente, el buscador realiza una exploración permanente de los sitios de Internet, creando un índice de todas las páginas exploradas, así como de su contenido (es lo que técnicamente se conoce como "indexación"). De esta forma, cuando se realiza una consulta, el motor de búsqueda se dirige al índice para localizar los elementos deseados, arrojando así resultados precisos.

En este orden de ideas, se entiende que los buscadores no son proveedores del contenido y en general no tienen ninguna relación con los sitios que arrojan los resultados de la búsqueda. De hecho, sólo se muestran unas pocas líneas del conte-

[28] *Artículo 2311. Se llaman cosas en este Código, los objetos materiales susceptibles de tener un valor. Las disposiciones referentes a las cosas son aplicables a la energía y a las fuerzas naturales susceptibles de apropiación.*

[29] Cfr. GINI, Santiago Luis, "Internet, buscadores de sitios web y libertad de expresión", Sup. Act. 23/10/2008, 1, publicado en: www.laleyonline.com.ar, consultado: 09/09/2010.

nido de los sitios encontrados, y si el usuario desea leer más, debe abandonar el sitio del buscador. En este sentido, se evidencia que los buscadores se limitan a dar a conocer en qué sitios se encuentran las palabras buscadas, sin hacer un análisis subjetivo de esa información[30].

De ello se desprende que, pese a los reiterados fallos de condena a buscadores web de nuestros tribunales (los llamados "casos de las modelos" [31]), debe sostenerse que éstos no son responsables por los contenidos de otros sitios que se muestran como resultado de las búsquedas, salvo que se demuestre que fueron negligentes en bloquear resultados claramente ilegales. Esto último, se dará cuando el buscador no da de baja un contenido pese a haberse ordenado dentro de un proceso concreto el bloqueo de un sitio específico por una autoridad competente.

Refuerza nuestra postura el reciente fallo "Da Cunha" de segunda instancia, que sigue los argumentos enunciados en un meduloso análisis. Entre los puntos más salientes de la sentencia se destaca que *"no basta que la información o el contenido existente en la web y encontrado a través de los buscadores sea erróneo o aun lesivo para el honor, la imagen o la intimidad de una persona para que ésta tenga derecho a que le sea reparado el perjuicio causado. Comprobado el exceso o la ilegalidad, quien pretende el resarcimiento deberá demostrar la culpa o negligencia en que incurrió el buscador conforme al régimen general de responsabilidad por el hecho propio"* [32].

De todo lo expuesto, se infiere que la responsabilidad de los buscadores será directa (pues responderá por el hecho propio) y subjetiva (ya que quien pretenda el resarcimiento deberá demostrar la culpa o negligencia en que incurrió el buscador).

---

[30] Cfr. GINI, Santiago Luis, *ob. cit.*

[31] Por ejemplo: "Da Cunha Virginia c/ Yahoo! de Argentina S.R.L. s/Daños y Perjuicios", Juzgado Nacional de Primera Instancia en lo Civil N° 75, Buenos Aires, 29 de julio de 2009; "Rodríguez María Belén c/ Google Inc. s /Daños y Perjuicios", Juzgado Nacional de Primera Instancia en lo Civil N 95, Buenos Aires, marzo 4 de 2010. Publicados en: http://www.hfernandezdelpech.com.ar/JurisprudenciaArg.htm, consultado 10/10/10.
Recordemos que las actoras son modelos famosas, y que en ambos casos la pretensión en contra de los buscadores Google y Yahoo! de Argentina no sólo fue la de dar de baja el contenido del buscador ("desindexar" el contenido) sino que también se solicitó una indemnización por daños materiales y morales, al sentirse afectadas en su buen nombre, honor e imagen cuando al escribir sus nombres en los buscadores se muestran como resultado sitios web de contenido erótico, sexual o pornográfico.

[32] Da Cunha, Virginia c/Yahoo! de Argentina S.R.L. s/Daños y Perjuicios, Sala D de la Cámara Nacional de Apelaciones en lo Civil, 19/08/10. Puede descargarse el texto completo de la sentencia en: http://www.hfernandezdelpech.com.ar/JurisprudenciaArg.htm, consultado 15/10/10.

3. RESPONSABILIDAD POR AFECTACIÓN AL DERECHO A LA INTIMIDAD

En esta última parte del presente capítulo, analizaremos el tema de la responsabilidad por afectación al derecho a la intimidad, donde se destacan los supuestos que implican al titular de una base de datos, a los ISP y al Estado por captación y derivación de comunicaciones electrónicas, al administrador de una red social, y a todos aquellos sujetos que se sean responsables por la utilización de *"cookies"* o bien por la utilización del correo electrónico.

3.1. RESPONSABILIDAD DEL TITULAR DE UNA BASE DE DATOS

Del tratamiento de datos personales pueden surgir innumerables daños, y consecuentemente la obligación de repararlos. Según exista o no una relación contractual entre el titular de los datos personales y el responsable de su tratamiento, habrá responsabilidad en el ámbito contractual o extracontractual:

A) Responsabilidad contractual: de la situación en la que una persona consiente que sus datos personales sean almacenados en un banco de datos para determinado fin, pueden derivarse diversos resultados dañosos, como por ejemplo, cuando esos datos son utilizados con fines diferentes, o si resultan falseados, o utilizados con fines discriminatorios, o cedidos sin autorización de su titular. De ello, se deriva una responsabilidad objetiva en cabeza del responsable de la base de datos, dado que existe una obligación tácita de seguridad en la conservación de los datos[33]. De este modo, la única forma de eximirse de responsabilidad es demostrando caso fortuito, fuerza mayor, culpa de la víctima o de un tercero ajeno. Asimismo, en cuanto a la extensión del daño, son resarcibles los daños materiales y morales que sean consecuencia inmediata en todo caso, y los que sean consecuencia mediata prevista o previsible, en tanto haya dolo (arts. 520 y 521 del C.C.[34]).

[33] Cfr. BOLOTNIKOFF, Pablo, *ob. cit.*, pág. 115.
[34] *Artículo 520. "En el resarcimiento de los daños e intereses sólo se comprenderán los que fueren consecuencia inmediata y necesaria de la falta de cumplimiento de la obligación".*
Artículo 521. "Si la inejecución de la obligación fuese maliciosa los daños e intereses comprenderán también las consecuencias mediatas".

Por último, si el incumplimiento contractual configura a la vez un delito del derecho criminal, en virtud del art. 1107[35], la víctima tendrá la opción de elegir entre el régimen de responsabilidad contractual o extracontractual[36].

B) Responsabilidad extracontractual: surge de un resultado dañoso derivado de la utilización y explotación abusiva o ilícita de un banco de datos, siempre y cuando no haya existido una relación contractual previa entre el titular de los datos y el responsable de su tratamiento. La extensión del resarcimiento en este caso será mayor puesto que se responde por las consecuencias inmediatas, mediatas en todo caso, e inclusive las casuales que hayan sido previstas y queridas al tiempo de ejecutar el hecho (arts. 903 a 905[37]).

Debe señalarse que, la ley de protección de datos personales 25.326 sólo regula la acción de hábeas data; por lo tanto, es menester remitirse a las disposiciones generales del Código Civil a los efectos de resolver la cuestión. Sin embargo, la interpretación de cuáles son las normas a las que deben remitirse, y por ende qué tipo de factor de atribución resulta imputable, no ha sido pacífica. La doctrina se ha dividido en aquellos que sostienen una tesis subjetiva, y aquellos que defienden una tesis objetiva.

a) Tesis subjetiva: esta postura es sostenida, entre otros, por Bustamante Alsina, quien afirma que *"tratándose del ámbito extracontractual la responsabilidad sería subjetiva, o sea que el factor sería la culpa o el dolo de quien opera el sistema automatizado o por cuenta de quien realiza la operación, pues por mucho que los tratamientos automatizados emplearen cosas, como los ordenadores o computadoras y todos los elementos magnéticos que forman el sistema, la recolección de datos, el procesamiento de la información y el tratamiento por medios interconectados, así como*

[35] *Artículo 1107. "Los hechos o las omisiones en el cumplimiento de las obligaciones convencionales, no están comprendidos en los artículos de este título, si no degeneran en delitos del derecho criminal"*.

[36] Las diferencias esenciales entre ambos regímenes radican en el plazo de prescripción (10 para la responsabilidad contractual y 2 años para la extracontractual) y en la extensión del daño (en el régimen contractual se responde por las consecuencias inmediatas y mediatas previsibles si ha mediado dolo, mientras que en el régimen extracontractual se responde por las inmediatas, mediatas en todo caso, e inclusive las casuales que hayan sido previstas y queridas al tiempo de ejecutar el hecho).

[37] *Artículo 903. Las consecuencias inmediatas de los hechos libres, son imputables al autor de ellos.*
Artículo 904. Las consecuencias mediatas son también imputables al autor del hecho, cuando las hubiere previsto, y cuando empleando la debida atención y conocimiento de la cosa, haya podido preverlas.
Artículo 905. Las consecuencias puramente casuales no son imputables al autor del hecho, sino cuando debieron resultar, según las miras que tuvo al ejecutar el hecho.

los programas e instrucciones del software y su resultado o información final son obra de la voluntad y la acción del hombre" [38]. De ello se infiere que resulta de aplicación la primera parte del segundo párrafo del art. 1113[39], vale decir, se trata de una responsabilidad directa por el hecho del hombre con las cosas que le sirven de instrumento, y tal como lo sugiere el texto legal, la culpa se presume a los fines de la prueba. Es decir, contrariamente al principio general de que quien alega debe probar, se invierte la carga probatoria, y será el dañador quien, para enervar su obligación de reparar, deba acreditar que fue diligente o que hubo una ruptura en el nexo causal.

b) Tesis objetiva: desde la posición opuesta, otros autores, como Alejandro Borda[40], entienden que la responsabilidad es objetiva, pues el procesamiento electrónico de datos constituye una actividad riesgosa, debiéndose aplicar lo dispuesto en la segunda parte del segundo párrafo del 1113, con fundamento en la teoría del riesgo creado (en tanto se acepte que dicha norma es aplicable no sólo a las cosas riesgosas sino también a las actividades riesgosas). En efecto, el responsable de la base de datos sólo se eximiría de su obligación de resarcimiento si probare caso fortuito, fuerza mayor, culpa de la víctima o de un tercero por el cual no se debe responder.

3.2. RESPONSABILIDAD POR INTERVENCIÓN DE COMUNICACIONES

Otro de los supuestos de responsabilidad puede darse como consecuencia de la captación y derivación ilegítima de comunicaciones electrónicas. En este punto, debemos recordar que en nuestro país rige la ley 25.873, la cual establece en su artículo 3 el régimen de responsabilidad para estos casos: *"El Estado nacional asume la responsabilidad por los eventuales daños y perjuicios que pudieran derivar para terceros, de la observación remota de las comunicaciones y de la utilización de la información de los datos filiatorios y domiciliarios y tráfico de comunicaciones de clientes y usuarios, provista por los prestadores de servicios de telecomunicaciones".*

[38] BUSTAMANTE ALSINA, Jorge, "Teoría General de la Responsabilidad Civil", Novena Edición, Editorial Abeledo Perrot, Buenos Aires, 1997, págs. 689 a 690.
[39] *Art. 1113. "…En los supuestos de daños causados con las cosas, el dueño o guardián, para eximirse de responsabilidad, deberá demostrar que de su parte no hubo culpa…"*
[40] Citado por BOLOTNIKOFF, Pablo, *ob. cit.*, p. 123.

Como ya comentáramos en su momento, en la interpretación de este artículo, coincidimos con Viegener en que "*la deficiente redacción del precepto no puede derivar, en entender que se ha pretendido "socializar" - con cargo al Tesoro Público - las consecuencias patrimoniales que pudieran derivarse de los daños causados a terceros por el hecho propio de las empresas de telecomunicaciones, responsabilidad ésta respecto a la cual la ley nada innova y que, por lo tanto, sólo será enjuiciable por el Poder Judicial de la Nación bajo el prisma de las normas y principios que rigen la responsabilidad civil*"[41].

Es decir, lejos de introducir una solidaridad legal o un principio especial de responsabilidad, la norma termina siendo redundante, pues no hace más que repetir un principio harto conocido, cual es el de responsabilidad del Estado por el funcionamiento irregular o defectuoso de su función administrativa (resulta de aplicación subsidiaria el art. 1112 del Código Civil).

Por último, en relación al tema, no debe dejar de resaltarse que más allá de que se reconozca la responsabilidad del Estado, nada obsta a que los proveedores de servicios que deban registrar y sistematizar los datos de tráfico también resulten responsables. No dudamos en que en este caso tal responsabilidad será la que le compete al titular de una base de datos; es así que la responsabilidad será directa, extracontractual, y podrá ser subjetiva u objetiva según la tesis a la que se adhiera.

3.3. RESPONSABILIDAD DERIVADA DE LAS REDES SOCIALES

Como ya se dijo, el auge que experimentan los servicios de redes sociales en la actualidad ha propiciado un nivel de divulgación de datos personales (muchos de ellos de carácter "sensible"), fotografías, videos y demás contenidos propios de los usuarios o bien de terceros, que no registra precedentes. Tal problemática, puede tener como causa la falta de conciencia real por parte de los usuarios de que sus datos personales serán accesibles por cualquier persona y del valor que éstos pueden llegar a alcanzar en el mercado; o bien en el hecho de que, a través de las con-

[41] VIEGENER, Federico, "El derecho a la Intimidad y los límites a la injerencia estatal", Alfa-Redi: Revista de Derecho Informático No. 116, Marzo del 2008, publicado en: http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/viegener.pdf, consultado: 04/10/2010.

diciones de registro aceptadas unilateral y hasta casi inconscientemente por los usuarios, éstos cedan derechos plenos e ilimitados sobre todos aquellos contenidos propios que alojen en la plataforma, de manera que pueden ser explotados de forma ilícita por parte de la red social.

Lo cierto es que pueden producirse daños a la intimidad, ya sea que éstos provengan de la actividad de los administradores de redes sociales o de los propios usuarios.

En cuanto a la responsabilidad de los administradores, entendemos que deben aplicarse las mismas consideraciones respecto de los proveedores de servicio de alojamiento[42], ya que en esencia ambos prestan un servicio de almacenamiento de contenidos (casi la totalidad de ellos son ajenos), en este caso particular de datos personales, imágenes, videos y demás contenidos "subidos" por el propio usuario. Es decir, según qué postura se asuma, la responsabilidad podrá ser subjetiva (imputable a título de dolo o culpa, ya que resulta técnicamente imposible controlar los contenidos de todos los perfiles, contenidos y actividades dentro de la red social; ello, en absoluto significa que no se tenga un deber de supervisar los contenidos, por el contrario, tal deber existe pero sólo respecto de los actos que se encuentran al alcance técnico del administrador) u objetiva (se aplicará la doctrina de la actividad riesgosa que surge de la segunda parte del segundo párrafo del artículo 1113).

Finalmente, de la misma forma, creemos que los usuarios también deberían quedar equiparados a los proveedores de contenido, siendo aplicable el régimen de responsabilidad ya comentado *ut supra* en el punto 2.1 del presente capítulo.

[42] Tal analogía se funda en que los administradores de redes sociales son más que meros titulares de bases de datos, ya que, por la multiplicidad de servicios que pueden desarrollarse en las mismas, su actividad trasciende la sola custodia de datos para un fin determinado. En otras palabras, los administradores de redes sociales son más parecidos a los ISP que a los titulares de bases de datos (al margen que en ambos casos, pero con distintos argumentos, se llega a la misma disyuntiva: responsabilidad subjetiva u objetiva).
Tampoco pueden ser asimilados a los buscadores de Internet, pues si bien las redes sociales realizan actividades de indexación con los perfiles de los usuarios registrados, sus servicios no se agotan en ello, pues a diferencia de los buscadores, las redes sociales facilitan a través de su plataforma un espacio en el cual pueden compartir archivos, aplicaciones, mensajes instantáneos, etc.

3.4. RESPONSABILIDAD DERIVADA DE LA UTILIZACIÓN DE "*COOKIES*"

Otro de los supuestos susceptibles de reparación es aquél derivado de la violación a la intimidad a través de *cookies* "ilegales", es decir, cuando, sin consentimiento del usuario, se obtiene información de navegación de las páginas web visitadas, contraviniendo el artículo 27 inciso 1 de la ley 25.326, que se aplica analógicamente ante la inexistencia de una norma particular.

La responsabilidad que surge en este caso para quien utiliza las *cookies* es la de un titular de bases de datos, ya que la relación entre éste y el usuario, ante una evidente laguna normativa, se rige por la ley de protección de datos personales y el Código Civil. Se aplica lo dicho respecto de la responsabilidad extracontractual para cuando la obtención de datos sea ilegal, ya que por hipótesis una *cookie* ilegal implica la falta de consentimiento del titular de los datos; de allí que no pueda haber relación contractual alguna (ver punto 3.1).

3.5. RESPONSABILIDAD DERIVADA DEL CORREO ELECTRÓNICO

La utilización del correo electrónico puede generar distintos supuestos de responsabilidad, entre los que se destacan los siguientes:

A) E-mail como instrumento para producir daños: es posible causar daños a la intimidad de terceros al igual que ocurre con los demás medios de comunicación (vgr. cuando se producen calumnias o injurias). En esta situación, se ha dicho que "*se utiliza el correo electrónico como instrumento para realizar un acto jurídico o un hecho ilícito, sin que el daño sea causado en forma directa por el propio mensaje, dado que éste es consecuencia directa de un hecho del hombre*"[43].

De esta forma, el emisor del mensaje tendrá una responsabilidad directa, extracontractual, y que, para todos los casos será subjetiva. Si éste utilizara la casilla de correo electrónico de otra persona, ésta última deberá responder en forma refleja o indirecta por su carácter de dueño o guardián (vgr. el dependiente usa la casilla

[43] HOCSMAN, Heriberto Simón, "Negocios en Internet", Editorial Astrea, Buenos Aires, 2005, p. 178.

de correo de la empresa para la que presta servicio). Por último, tanto para el emisor del mensaje como para el titular de la casilla de correo electrónico, resulta de aplicación la presunción *iuris tantum* de culpa que emerge del art. 1113, segundo párrafo, primera parte; así, deberá probarse que hubo un actuar diligente o una interrupción no imputable del nexo causal para enervar cualquier tipo de reparación[44].

B) "*Spoofing*": se conoce bajo este nombre a una especie particular de utilización fraudulenta del correo electrónico como instrumento, y que puede consistir en la usurpación de una cuenta de e-mail ajena para enviar mensajes haciéndose pasar por el titular, o bien en la utilización de una cuenta que se preste a confusión respecto del verdadero titular.

El *spoofing* genera responsabilidad civil, debiéndose aplicar lo expuesto en el apartado anterior, pero con la particularidad de que resulta muy difícil, de acuerdo al estado de la ciencia y de la técnica actual, identificar al autor del engaño; por este motivo, habrá una gran cantidad de daños que deberán ser soportados por el damnificado[45].

C) Envío de "*spam*": cuando se utiliza el correo electrónico para el envío de publicidad no solicitada, se está conculcando la privacidad, dado que el usuario se ve invadido por e-mails que ofrecen todo tipo de productos y/o servicios que jamás requirió. Compartimos con Sobrino que la ilicitud de tal conducta, independientemente de que un ordenamiento jurídico, en principio, la permita (*opt out*) o prohíba (*opt in*), recae en que, la mayoría de las veces, la dirección de correo electrónico del usuario se incluye en una base de datos ilegal, es decir, en el caso del derecho argentino, contraria a las disposiciones de la ley 25.326 sobre recolección de datos. De esta forma, se ha dicho que "*si el sustrato en que se basa el 'spam' (v.gr. la 'base de datos') es ilegal, no existe otra alternativa que declarar la ilegalidad de todo aquello*

[44] Cfr. HOCSMAN, Heriberto Simón, *ob. cit.*, p. 179.
[45] Cfr. HOCSMAN, Heriberto Simón, *ob. cit.*, p. 182.

que deriva de una base ilegal"[46], es decir, resulta aplicable la doctrina del fruto del árbol envenenado cuando se intenta acreditar la antijuridicidad.

En cuanto a los daños resarcibles, se argumenta, por un lado, el costo económico del tiempo de descarga que insume la identificación, selección y eliminación de los correos "basura", y por otro, los costos en tecnología, representados por los gastos de reparación del sistema y de protección informática ante eventuales virus.

Finalmente, coincidimos con el citado autor en cuanto a que el factor de atribución aplicable será siempre subjetivo, al margen de que la culpa de quien envíe los *spams* debe presumirse. Esto último, implicará una inversión de la carga probatoria, obligando al *spammer* a probar que la base de datos que utilizó tiene un origen lícito[47].

[46] SOBRINO, Waldo Augusto Roberto, "Las Cookies y el Spam (y la violación de la Privacidad y la Intimidad)", Junio de 2001, publicado en http://www.alfa-redi.org/rdi-articulo.shtml?x=710, consultado: 09/09/10.
[47] Cfr. SOBRINO, Waldo Augusto Roberto, *ob. cit.*

CAPÍTULO VII
CONCLUSIÓN

"Internet: origina un nuevo Derecho, el Derecho de Internet;
cambia la vida del hombre y, por ende, impacta en el Derecho;
cambia al mismo Derecho; cambia a los operadores del Derecho".
Lynch, Horacio[1]

A modo de colofón, luego de abordado algunos de los problemas jurídicos que plantea Internet en relación al derecho a la intimidad, resulta ineludible en este punto final, reiterar ciertas conclusiones y propuestas dadas a lo largo del presente desarrollo:

1) En primer término, debe dejarse en claro que Internet es el paradigma de las nuevas tecnologías, y que se erige como el nuevo gran medio de comunicación de la actual Sociedad de la Información, diferenciándose del resto por su versatilidad e interactividad. Asimismo, como toda tecnología, es axiológicamente neutral, por lo cual el buen o mal uso que de ella se haga dependerá siempre de la conducta del hombre. Este razonamiento, lleva a la conclusión de que el espacio virtual que abre Internet es un espacio social, y como tal debe necesariamente ser regulado por el derecho. No es cierto que Internet sea "tierra de nadie", como sostienen algunos, ni que sería imposible regularlo, so pretexto de que las leyes alteran su esencia o impiden su progreso.

Ahora bien, el ciberespacio tiene particularidades jurídicamente relevantes, como lo son la descentralización, la deslocalización de sus partícipes, su carácter transnacional, y su constante avance tecnológico, que lo convierten en un espacio

[1] LYNCH, Horacio citado por GALDÓS, Jorge Mario, "Responsabilidad civil e Internet: Algunas aproximaciones", JA 2001-III-819, publicado en: http://www.abeledoperrot.com.ar, consultado 10/10/10.

único, que no registra precedentes en la historia. Es por ello que, hoy en día resulta excesivo exigir al derecho que dé soluciones totalmente satisfactorias. Lo que sí podrá exigírsele son mejores soluciones que las existentes, para lo cual sería necesario que los institutos jurídicos tradiciones se ajusten a esta nueva problemática, y que otros nuevos se implementen a fin de brindar soluciones a una realidad tan cambiante.

2) Es indudable que el fenómeno de Internet ha influido notablemente en la forma de concebir la libertad de expresión. En la hora actual, parecerían haberse eliminado algunas barreras que la limitaban, pues la relativa facilidad de para crear una página web, amplió considerablemente el espectro de opiniones e informaciones. Así, la libertad de expresión en la era de Internet adquiere un nuevo significado: es ahora un derecho verdaderamente "universal", en cuanto a que permite un espacio en el que se oyen más voces y se leen otros puntos de vista, democratizando el acceso a los medios de comunicación. Asimismo, la libertad de expresión no sólo implica un derecho de libertad para que cualquiera pueda producir contenidos, sino también una correlativa libertad para que los usuarios puedan emplear todos servicios de Internet sin restricciones de ningún tipo.

Sin embargo, la influencia de Internet no ha sido sólo positiva, pues existen algunos problemas que afectan a los medios de comunicación tradicionales, como ser el riesgo de concentración en el manejo de la información, los daños por noticias inexactas o agraviantes, o la posibilidad de recurrir a la censura previa como remedio excepcional, y que tienen implicancias en el derecho. Además, aparecen otros nuevos problemas como lo son la identificación de los usuarios anónimos cuando realizan actividades dañosas, o las técnicas de filtrado como forma de control, y a la vez de censura previa de ciertos contenidos que se consideran inadecuados o ilícitos, sobre todo cuando son utilizadas por los Estados.

En el derecho nacional tanto el decreto 1279/1997 como la ley 26.032 han extendido a Internet la garantía constitucional de los artículos 14, 32, 42 y 75 inc. 22, que amparan la libertad de expresión. Esto significa que el principio general adoptado para los contenidos en Internet es el de absoluta libertad, y que en ningún caso puede haber censura previa, salvo la única excepción prevista por el artículo 13 inci-

so 4 del Pacto San José de Costa Rica relativa a la pornografía infantil. En todo caso, el remedio para los excesos en el ejercicio de la libertad de expresión será la responsabilidad ulterior a la que deben atenerse los autores de dichos abusos. De esta forma, serán responsables aquellos que "suban" a la red contenidos que puedan afectar legítimos intereses, como ser derechos de autor, derechos de propiedad sobre una marca o nombre comercial, o bien contenidos que sean calumniosos o injuriosos o puedan implicar una incitación a cometer delitos o actos discriminatorios, o finalmente -y en lo que nos interesa- que afecten a la intimidad o privacidad de las personas.

3) Oportunamente dijimos que el concepto de "derecho a la intimidad" que surge del juego de los arts. 18, 19, 43 y 75 inc. 22 de la Constitución Nacional debe entenderse en un sentido amplio; en el sentido que nuestra Corte Suprema le ha dado en "Ponzetti de Balbín", al sostener que "*protege jurídicamente un ámbito de autonomía individual constituido por los sentimientos, hábitos y costumbres, las relaciones familiares, la situación económica, las creencias religiosas, la salud mental y física y, en suma, las acciones, hechos o datos que, teniendo en cuenta las formas de vida aceptadas por la comunidad están reservadas al propio individuo y cuyo conocimiento y divulgación por los extraños significan un peligro real o potencial a la intimidad*"[2]. Vale decir, es un derecho personalísimo que comprende una amplia gama de garantías: la protección del secreto o reserva de actos de la vida privada de toda persona (datos sobre su salud, sus prácticas religiosas, su sexualidad, su ideología política, etc.), el secreto de la correspondencia epistolar, electrónica y de otros papeles privados, la inviolabilidad del domicilio, el derecho a la imagen, el derecho al buen nombre y honor, y el derecho al secreto profesional.

El concepto de intimidad, así entendido, permite ser *aggiornado* a los tiempos actuales, donde a partir de la cuasi-masificación del uso de Internet, los riesgos de afectación se multiplican, dada la mayor cantidad de información que circula por la red, y la mayor complejidad de los sistemas informáticos que se utilizan para su recolección.

[2] Ponzetti de Balbín, Indalia c. Editorial Atlántida S.A, CSJN, 11/12/1984 (Fallos, 306:1892).

4) Uno de los aspectos más importantes por los cuales el derecho a la intimidad puede verse seriamente afectado es aquél que se refiere a la utilización indebida de los datos personales que de una persona pueden obtenerse por los hábitos de navegación de los usuarios. Las actividades que una persona realiza en Internet pueden ser monitoreadas externamente y sin su consentimiento, a través de terceros que, deseosos de desentrañar cuáles son los gustos personales del usuario, utilizan mecanismos para recopilar datos orientativos que puedan conformar perfiles de los mismos. A lo largo del presente trabajo se fueron plasmando detalladamente las diferentes maneras y los dispositivos que permiten hoy en día afectar seriamente la intimidad de los usuarios en su navegación por Internet.

Entre las diversas transgresiones que los datos personales pueden sufrir a través de Internet, analizamos las llamadas redes sociales, las "*cookies*", y la captación de los datos de tráfico en las comunicaciones electrónicas.

Del estudio de estos supuestos, quedó en evidencia que no existen en el ordenamiento jurídico argentino soluciones eficaces. En materia de redes sociales, vimos que la temática, debido a su reciente aparición, aún no ha sido abordada por los autores nacionales, y por lo tanto todavía presenta más preguntas que respuestas, más dudas que certezas. En el caso de las *cookies*, tampoco han sido expresamente reguladas; empero, la doctrina es conteste en afirmar la aplicación analógica del art. 27 de la ley de protección de datos personales. Finalmente, tratándose de la captación de las comunicaciones, si bien el dictado de la ley 25.873 fue un paso adelante para combatir las ilegalidades que puedan cometerse a través de Internet, obligando a los ISP a retener los datos de tráfico de las comunicaciones electrónicas, para su posterior remisión como prueba al Poder Judicial, dicha ley ha estado muy por debajo de los estándares internacionales pues no garantiza de modo suficiente el derecho a la intimidad. Al margen de la gran cantidad de críticas que hemos expuesto en relación a esta ley y a su decreto reglamentario, y teniendo en cuenta que la misma ha sido declarada inconstitucional en "Halabi"[3], y a la vez suspendida por el propio Poder Ejecutivo, creemos de fundamental importancia que

[3] Halabi, Ernesto c/ P.E.N. s/Amparo, CSJN, 24/02/2009. Puede consultarse el texto del fallo en: http://www.csjn.gov.ar/cfal/fallos/cfal3/ver_fallos.jsp, consultado 02/10/2010.

finalmente se haga un nuevo análisis del problema, y se dicte una nueva ley teniendo en cuenta los lineamientos de la directiva 2006/24/CE de la Unión Europea.

5) En materia de correo electrónico, dijimos que la utilización de esta nueva herramienta de comunicación como uno de los servicios más importantes que ofrece Internet, puede dar lugar conflictos jurídicos vinculados al derecho a la intimidad. Es así que se expusieron principalmente tres cuestiones, a saber: la violación del e-mail como manifestación actual de la privacidad de la correspondencia, el correo electrónico no solicitado o *"spam",* y las facultades del empleador de controlar el e-mail laboral de sus dependientes.

Respecto de cada una de estas cuestiones, quedó en claro que los distintos mecanismos de protección que se han esbozado en otros sistemas jurídicos más sofisticados, como lo son la normativa europea y estadounidense, aún no han sido receptados por la legislación argentina. Sin embargo, las soluciones no se han hecho esperar demasiado, y han venido de la mano de la doctrina y la jurisprudencia nacional, principalmente desde la reinterpretación de normas ya existentes. Es así que, ante la evidente falta de una legislación que regule integralmente los problemas del correo electrónico, resultan de aplicación algunas normas generales, cuya flexibilidad les permite adaptarse a estos nuevos supuestos: la ley 25.326 de datos personales, el art. 1071 bis y los principios generales de responsabilidad del Código Civil, los arts. 109 y ss. relativos a calumnias e injurias y los arts. 153 y ss. relativos a la violación de secretos en el Código Penal, y, finalmente, los principios y disposiciones de ley 20.744 de contrato de trabajo.

6) En materia de responsabilidad civil frente a los daños y perjuicios materiales y morales causados por los distintos partícipes de la red, también se ha acudido a la aplicación de la analogía y de los principios generales del derecho, en todo aquello que sea compatible con el régimen jurídico del Código Civil.

La determinación de si corresponde una responsabilidad contractual o extracontractual, objetiva o subjetiva, directa o indirecta, por actividades ilícitas o lícitas, con las cosas o por el vicio o riesgo de las cosas, dependerá de cada supuesto en particular. Sin embargo, deberá tenerse en cuenta que los daños derivados del uso

de Internet se inscriben dentro del actual Derecho de Daños, donde se destaca un sistema de atribución de responsabilidad objetivo, en el cual debe primar el derecho a la víctima a una reparación integral y justa.

7) Para concluir, creemos que es evidente que, ante los aspectos aquí tratados, y que revelan la faz negativa de Internet en su vinculación con la privacidad, el Derecho no puede quedar al margen, a pesar de que, de hecho, muchas veces se manifiesta estático ante la velocidad de los avances tecnológicos.

Tampoco el Derecho podrá mantenerse al margen aduciendo que no hay unanimidad en cuanto al criterio de cómo regular Internet y sus problemas jurídicos. Creemos que la existencia de distintas posturas frente a un mismo problema no es algo ajeno al Derecho, pues en materia jurídica todo es objeto de discusión. Es así que vemos que en otras ramas del Derecho no hay respuestas únicas ni unánimes; mucho menos podemos pretender que las haya cuando se trata de una materia tan compleja, novedosa y dinámica. Ello no constituye en modo alguno un obstáculo para su regulación.

De esta forma, creemos que es menester concebir nuevas instituciones jurídicas, o bien *aggiornar* las ya existentes. Hasta ahora, el vacío legal en los Estados que no han regulado los distintos problemas jurídicos que plantea la red ha sido integrado a través de la aplicación de la analogía y de los principios generales del derecho en lo que sea compatible con el régimen jurídico interno. Sin embargo, en mucho otros temas se han dictado normas que regulan con especificidad y rigor las nuevas realidades.

El principal problema frente a estas nuevas instituciones se produce por el carácter supranacional de Internet. Dado que la Red establece relaciones entre seres humanos, colocados virtualmente muchas veces en lugares muy distantes entre sí, y que en esas relaciones se pueden presentar conflictos de derechos, será necesario que se haga el dictado, más que de normas pertenecientes a ordenamientos jurídicos nacionales, de una regulación internacional, atendiendo a la universalidad propia de Internet, que no entiende de límites estatales. La globalización del problema hace necesaria esta regulación internacional, pues las leyes nacionales pue-

den burlarse desde verdaderos "paraísos informáticos" donde la ley nada dice acerca de los problemas aquí expuestos.

Hoy en día la Argentina es indiscutiblemente un paraíso informático, y ello se refleja no sólo en su casi inexistente legislación en materia de Internet, sino también en otras deficiencias extrajurídicas, que incluso pueden ser más graves, como por ejemplo, la falta de educación de los usuarios y operadores jurídicos.

Quizás esta carencia resulte más común a nivel de los usuarios que utilizan los servicios de Internet, quienes al decir de Sobrino son "hipoconsumidores tecnológicos", es decir, personas que son propensas al consumo indiscriminado de todas aquellas innovaciones tecnológicas sin saber ni remotamente los peligros que ellas conllevan, pues solamente buscan su utilización sin importarles cómo es su funcionamiento y los peligros que ellas entrañan.

Ahora bien, ello resulta grave a nivel de los propios operadores del derecho, particularmente a nivel de los jueces y funcionarios públicos que deben aplicar las normas. En la actualidad, la mayoría de quienes ostentan dicha responsabilidad son personas poco avezadas en las nuevas tecnologías, y suelen ser reacias hacia la actualización permanente que requiere una materia dinámica y cambiante como el derecho de Internet.

Por último, más allá de que consideramos fundamentales las soluciones legislativas, creemos que las soluciones a las deficiencias extrajurídicas apuntadas son igualmente importantes, sobre todo en lo que tiene que ver con la formación de nuevos juristas especialistas en el tema. Será labor de las nuevas generaciones capacitarse y aportar ideas para que la comunidad jurídica enriquezca los escasos lineamientos que se han expuesto en la presente obra, procurando que maduren en soluciones útiles y eficaces en un futuro.

Como corolario, quiero ampararme en un pensamiento esgrimido por el distinguido doctrinario Lynch: *"Internet: origina un nuevo Derecho, el Derecho de Internet; cambia la vida del hombre y, por ende, impacta en el Derecho; cambia al mismo Derecho; cambia a los operadores del Derecho"*[4].

[4] LYNCH, Horacio citado por GALDÓS, Jorge Mario, *ob. cit.*

ANEXO

DECRETO 554/1997
TELECOMUNICACIONES

Declárase de Interés Nacional el acceso de los habitantes de la República Argentina a la red mundial INTERNET. Autoridad de Aplicación.

Bs. As., 18/6/97
B.O.: 23/06/97

VISTO el artículo 42 de la Constitución Nacional, los Decretos N° 62/90, 1185/90 y 1620/96, y la Resolución N° 97 del 16 de setiembre de 1996 del registro de la SECRETARIA DE COMUNICACIONES DE LA PRESIDENCIA DE LA NACION, y el expediente N° 906/97 del registro de la misma Secretaría, y

CONSIDERANDO:
Que el artículo 42 de la CONSTITUCION NACIONAL establece que "... Las autoridades proveerán a la protección de esos derechos, a la educación para el consumo, a la defensa de la competencia contra toda forma de distorsión de los mercados, al control de los monopolios naturales y legales, al de la calidad y eficiencia de los servicios públicos, y a la constitución de asociaciones de consumidores y de usuarios".
Que la Resolución SC N° 97/96 señala en sus considerandos que "siendo la INTERNET un claro fenómeno autopoíetico, desarrollado sin el impulso de autoridad regulatoria alguna (...), es necesario dictar una reglamentación que aclare la vigencia de tal principio (como servicio de Valor Agregado)".
Que tal condición de autogeneración transforma a INTERNET en un fenómeno digno de reflexión, precisamente por su configuración descentralizada, con arquitectura abierta, masividad de acceso y autorregulación normativa.
Que INTERNET representa un claro paradigma de las mejores promesas de la sociedad global, esto es, la existencia de un soporte ubicuo, flexible, abierto y transparente para el intercambio y difusión de ideas, información, datos y cultura, sin cortapisas ni censura de ninguna especie.
Que esta red mundial no puede ser sospechada, de manera alguna, como un elemento de control social o de indebida injerencia en la intimidad de las personas o familias debido, fundamentalmente, a dos grandes factores constitutivos: a) su interactividad, y b) la libre elección de contenidos e información.
Que el factor de la interactividad despeja cualquier intento de manipulación sistemática sobre la opinión de las personas, ya que, en el ambiente interactivo de INTERNET, el mensaje del emisor es optado, evaluado, decodificado, analizado, procesado, aceptado, modificado o rechazado por parte del receptor, mediante tecnologías, procesos e interfaces diseñados deliberadamente para la interacción.
Que la libre elección de contenidos es condición propia de la democracia. y que INTERNET satisface plenamente este requisito, al proporcionar contenidos de gran diversidad, con idénticas oportunidades de acceso y competitivos entre sí.

Que en todo el mundo las tecnologías de la informática y las comunicaciones están generando una nueva y profunda revolución basada en la información, que es en sí misma la expresión del conocimiento humano.
Que tal progreso tecnológico permite hoy en día, procesar, almacenar, recuperar y transmitir información en cualquiera de sus formas, tanto oral, escrita como visual, independientemente de los tiempos, las distancias y el volumen, convirtiéndose en un recurso que modifica el modo de trabajar, enseñar, aprender y convivir.
Que el conocimiento del hombre ha reconocido, a través del tiempo, variados medios para su difusión y almacenamiento, desde el papiro hasta las modernas redes virtuales y desde los templos hasta las bibliotecas populares.
Que, de esta manera, es posible suponer que el conocimiento, aunque reconozca reglas y métodos de producción relativamente homogéneos a través del tiempo, requiere técnicas, sistemas de almacenamiento, sistematización y difusión mediante tecnologías propias de cada momento histórico.
Que INTERNET es una red global de redes de computación que permite la interrelación entre más de cincuenta millones de usuarios facilitando el intercambio de datos, imágenes y sonidos.
Que es fácilmente deducible que lo que ayer constituyeron las bibliotecas populares como centro de concentración y de difusión del conocimiento, hoy puede ser complementado eficazmente por INTERNET.
Que es posible advertir que la misión de aquellas bibliotecas populares hoy puede ser actualizada mediante la masiva difusión de INTERNET, sirviendo de soporte de bajo costo y gran calidad para la libre circulación del conocimiento humano, los productos de la cultura, la interacción creativa de los hombres, mujeres y niños de la República Argentina y el mundo y el incremento de la comprensión mediante la mutua transferencia de información y el intercambio de ideas allende las fronteras y los sistemas de gobierno.
Que al inaugurarse en 1874 el primer cable submarino entre Europa y el Río de la Plata se tuvo una clara visión de futuro al enviarse un "saludo cordial a todos los pueblos, que se hacen por intermedio del cable, una familia sola y un barrio", visión que fue graficada apenas unos años atrás en la expresión "aldea global".
Que esta nueva expresión de la sociabilidad humana, devenida tras la eclosión de la aceleración del cambio y la revolución en las comunicaciones, crea oportunidades reales, beneficios y desafíos para las sociedades y gobiernos de todo el mundo, los que deberán replantear sus políticas de acción, sus estrategias regulatorias, opciones empresariales y sus concepciones sobre el desarrollo humano.
Que aquellos países que puedan integrarse a esta nueva realidad y establezcan como prioritarias las políticas a seguir en el sector, serán los que recojan los mayores beneficios, y que el aprovechamiento de los instrumentos que la moderna tecnología ofrece, posibilitará la construcción de una sociedad más justa y equilibrada, ofreciendo la información global a mayores sectores de la población.
Que es posible inferir que uno de los principales cometidos del Gobierno Nacional para aprovechar las oportunidades de esta revolución tecnológica es impedir que se concrete su mayor amenaza, esto es, la formación en el seno de su sociedad de grupos humanos que no tienen la información y grupos que si la tienen.
Que el Gobierno Nacional esta convencido que es mejor anticipar los problemas antes que se produzcan efectivamente, y que el tema de la sociedad de la información no es menor de cara al futuro de millones de argentinos y que es función del Estado proveer el acceso equitativo a esta moderna infraestructura de comunicaciones para toda la población.
Que, asimismo, todos los organismos internacionales de comunicaciones recomiendan garantizar una completa aceptación, uso y distribución de las tecnologías soportes de INTERNET, teniendo como objetivos primordiales la difusión de la información y garantizando la educación y promoción de la cultura.

Que no obstante, el preparar la infraestructura de comunicaciones argentinas para el advenimiento de la sociedad de la información no es tan solo una cuestión de anhelos ni de sanas intenciones de colaboración entre áreas del estado, si no que discurre por una adecuada tarea de incentivo a la formación de redes de gran calidad y apegadas a estándares internacionales, claras reglas de interconexión e interoperabilidad de servicios.
Que el Gobierno Nacional quiere avanzar decididamente en esta dirección, promoviendo la competencia en la provisión de INTERNET a precios razonables y equitativos.
Que el fomento del uso de INTERNET posibilitará que la información que en ella circula sea accesible de manera masiva a todos los habitantes del país, superando los factores existentes, en especial resguardando a aquellos usuarios que por sus ubicaciones geográficas tienen limitaciones para acceder a la misma.
Que, paralelamente, el desarrollo de esta red es fundamental para la industria de las telecomunicaciones, lo que favorecerá el incremento de inversiones en el sector y el desarrollo de nuevas tecnologías aplicadas al software.
Que conforme a la competencia asignada, la SECRETARIA DE COMUNICACIONES DE LA PRESIDENCIA DE LA NACION coordinará con otros organismos estatales las acciones tendientes al desarrollo y calidad de la prestación del servicio de INTERNET.
Que es intención del PODER EJECUTIVO NACIONAL generar un amplio marco de debate sobre los beneficios y alcances que la utilización de INTERNET posean para la población en general, así como también remover los obstáculos técnicos o regulatorios que se interpusieran para su libre desenvolvimiento.
Que, en definitiva, el Gobierno Nacional entiende que posee la obligación de promover un servicio universal, especialmente a aquellos con recursos limitados, que asegure que las escuelas, bibliotecas, centros de atención médica, y áreas rurales, entre otros, se beneficien con INTERNET y que la nueva revolución que representa, constituya uno de los grandes cambios de comienzos del nuevo siglo, con la colaboración del sector privado para asegurar que la red este constituida de la mejor y más eficiente manera.
Que, en función de las características aludidas, INTERNET merece ser declarada como de Interés Nacional por parte del Gobierno de la Nación Argentina.
Que esta declaración supone que INTERNET es un servicio de telecomunicaciones de características tales que involucra y se proyecta sobre vastos sectores de la vida educativa, sanitaria, cultural, científica e industrial del país.
Que, por lo tanto, esta realidad debe ser abordada conforme a pautas estratégicas para su desarrollo y fomento, fundadas en la competencia y el incremento de la calidad de las redes.
Que la presente medida se dicta conforme a lo dispuesto por los Decretos Nros. 731/89, 62/90, 1185/90 y sus modificatorios, por la Ley 19.798 y en uso de las atribuciones conferidas por el artículo 99, inciso 1° de la Constitución Nacional.

Por ello,
EL PRESIDENTE DE LA NACION ARGENTINA
DECRETA:

Artículo 1°-Declárase de Interés Nacional el acceso de los habitantes de la República Argentina a la red mundial INTERNET, en condiciones sociales y geográficas equitativas. con tarifas razonables y con parámetros de calidad acordes a las modernas aplicaciónes de la multimedia.

Art. 2°-La SECRETARIA DE COMUNICACIONES DE LA PRESIDENCIA DE LA NACION será la Autoridad de Aplicación del presente decreto.

Art. 3°-Facúltase a la Autoridad de Aplicación a tomar las siguientes medidas de política:
a) Desarrollar un plan estratégico para la expansión de INTERNET en la República Argentina.
b) Analizar la incorporación de INTERNET dentro de los parámetros de análisis y características definitorias del servicio universal.
c) Analizar y proponer alternativas de política tarifaria a los efectos de estimular y diversificar la utilización de INTERNET.
d) Fomentar el uso de INTERNET como soporte de actividades educativas, culturales, informativas, recreativas y relativas a la provisión de servicios de salud.

Art. 4°-La Autoridad de Aplicación coordinará sus actividades en lo relativo al cumplimiento del presente con las áreas del Estado Nacional cuyo quehacer se encuentre ligado, en forma directa al desarrollo de INTERNET. Asimismo, se encuentra facultada para celebrar convenios con todas las entidades, públicas o privadas, nacionales, provinciales o municipales que estén relacionados con la provisión, utilización o desarrollo de la red, o que posean algún interés objetivo para con el cumplimiento del plan estratégico que dicha Autoridad diseñe de conformidad al presente.

Art. 5°-El Plan Estratégico elaborado por la Autoridad de Aplicación deberá incluir, entre otras, las siguientes metas de política pública:
a) Integración a la red incorporando sitios propios, de las bibliotecas argentinas.
b) Promoción del acceso a la Red de INTERNET del Sistema Educativo.
c) Promoción del desarrollo de una red nacional de telemedicina que optimice la utilización de los recursos disponibles.

Art. 6°-Los prestadores de servicios de telecomunicaciones deberán adecuar las características, calidad y prestaciones de sus redes a los efectos de conformar soportes físicos que permitan el desarrollo y expansión de INTERNET. La Autoridad de Aplicación dictará las disposiciones técnicas pertinentes a estos efectos, incluyendo la total y absoluta interoperabilidad e interconectividad.

Art. 7°-La Autoridad de Aplicación fomentará el desarrollo de redes alternativas con aptitud para la implementación, difusión y provisión de INTERNET en todo el ámbito geográfico de la República Argentina.

Art. 8°-La Autoridad de Aplicación dictará los reglamentos necesarios para el cumplimiento de los objetivos fijados en el presente.

Art. 9°-Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese.

DECRETO 1279/1997
TELECOMUNICACIONES

Declárase comprendido en la garantía constitucional que ampara la libertad de expresión al servicio de INTERNET.

Bs. As., 25/11/97
B.O: 1/12/97

VISTO los artículos 14, 32 y 42 de la CONSTITUCION NACIONAL, la Ley N° 23.054, el Decreto N° 554/97 y el expediente N° 1596/ 97 del registro de la SECRETARIA DE COMUNICACIONES de la PRESIDENCIA DE LA NACION, y

CONSIDERANDO:
Que el artículo 14 de la norma fundamental establece que: "Todos los habitantes de la Nación gozan de los siguientes derechos ... de publicar sus ideas por la prensa sin censura previa; ..."
Que el artículo 32 de la citada norma prescribe que: "El Congreso federal no dictará leyes que restrinjan la libertad de imprenta o establezcan sobre ella la jurisdicción federal."
Que finalmente el artículo 42 de la Carta Magna preceptúa que: "... Las autoridades proveerán a la protección de ... los derechos de los usuarios y consumidores ...", con la finalidad de garantizar el bienestar general.
Que por Decreto N° 554/97 se declaró de Interés Nacional el acceso de los habitantes de la República Argentina a la red mundial de INTERNET, en condiciones sociales y geográficas equitativas, con tarifas razonables y con parámetros de calidad acordes a las modernas aplicaciones de la multimedia.
Que el servicio INTERNET permite a los habitantes de la República Argentina acceder a un amplio intercambio de información y centro de datos mundiales sin censura previa.
Que el servicio de INTERNET es un medio moderno por el cual la sociedad en su conjunto puede expresarse libremente, como asimismo recabar información de igual modo.
Que el progreso tecnológico permite en la actualidad procesar, almacenar, recuperar y transmitir información en cualquiera de sus formas, tanto oral, escrita como visual, acortando las distancias físicas y convirtiéndose en un recurso que modifica en forma revolucionaria el modo de informarse, trabajar, aprender y enseñar.
Que en tal sentido, el Gobierno Nacional favorece y fomenta el desarrollo de este servicio en todo el país, instrumentando las medidas conducentes para remover los obstáculos que frenan su crecimiento, pero sin interferir en la producción, creación y/o difusión del material que circula por INTERNET de conformidad con el actual marco regulatorio aplicable.
Que dada la vastedad y heterogeneidad de los contenidos del servicio de INTERNET es posible inferir que el mismo se encuentra comprendido dentro del actual concepto de prensa escrita, el cual no se encuentra sujeto a restricción ni censura previa alguna.
Que la garantía constitucional que ampara la libertad de expresarse por la prensa cubre las manifestaciones vertidas a través de la radio y la televisión en tanto estas constituyen medios aptos para la difusión de las ideas.
Que el más Alto Tribunal ha sostenido que "La libertad de expresión que consagran los artículos 14 y 32 de la Constitución Nacional contiene la de dar y recibir información." (conf. F. Gutheim c/J. Alemann, del 15/04/93 Fallos 316:703).
Que en tal sentido la doctrina nacional sostiene que el especial status previsto para la prensa escrita por nuestros legisladores, único medio de expresión al tiempo del dictado de la legislación, es aplicable también para todos los medios modernos tales como radio y televisión.

Que el servicio de INTERNET es otro medio moderno que resulta plenamente apto para la difusión masiva de las ideas tanto para darlas a conocer como para recibirlas en beneficio del conocimiento del hombre.
Que el derecho comparado también ha coincidido con los lineamientos señalados.
Que en este sentido, la Corte Suprema de Justicia de los Estados Unidos de América se ha pronunciado in re "Reno Attorney General of United States et al . v. American Civil Liberties et al., N° 96-511, 26 june 1997" al decir: "... no se debería sancionar ninguna ley que abrevie la libertad de expresión ... la red INTERNET puede ser vista como una conversación mundial sin barreras. Es por ello que el gobierno no puede a través de ningún medio interrumpir esa conversación ... como es la forma más participativa de discursos en masa que se hayan desarrollado, la red INTERNET se merece la mayor protección ante cualquier intromisión gubernamental."
Que la presente reforma de 1994 ha incorporado al texto de la CONSTITUCION NACIONAL los Tratados Internacionales, entre ellos el Pacto de San José de Costa Rica, Convención Americana de Derechos Humanos, aprobada por Ley N° 23.054, que en su artículo 13 inciso 1° contempla el derecho de toda persona a la libertad de pensamiento y expresión, declarando como comprensiva de aquella "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".
Que no escapa al Gobierno Nacional que una de las características esenciales del servicio INTERNET es su interconectividad, por la cual los usuarios tienen la libertad de elegir la información de su propio interés, resultando por ello que cualquier pretensión de manipular, regular o de censurar los contenidos del servicio, se encuentra absolutamente vedada por la normativa vigente.
Que por los motivos señalados, resulta conveniente establecer que el servicio de INTERNET se encuentra amparado por la especial tutela constitucional que garantiza la libertad de expresión.
Que la presente medida se dicta en ejercicio de las facultades conferidas por el artículo 99, incisos 1) y 2) de la CONSTITUCION NACIONAL.
Por ello,
EL PRESIDENTE DE LA NACION ARGENTINA

DECRETA:

Artículo 1°-Declárase que 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.

Art. 2°-Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese.

LEY 26.032
SERVICIO DE INTERNET

Establécese que la búsqueda, recepción y difusión de información e ideas por medio del servicio de Internet se considera comprendida dentro de la garantía constitucional que ampara la libertad de expresión.

Sancionada: Mayo 18 de 2005
Promulgada de Hecho: Junio 16 de 2005
El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ARTICULO 1° — 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.

ARTICULO 2° — La presente ley comenzará a regir a partir del día siguiente al de su publicación en el Boletín Oficial.

ARTICULO 3° — Comuníquese al Poder Ejecutivo.

LEY 25.326
PROTECCION DE LOS DATOS PERSONALES

Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales.

Sancionada: Octubre 4 de 2000.
Promulgada Parcialmente: Octubre 30 de 2000.
El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

Ley de Protección de los Datos Personales

Capítulo I

Disposiciones Generales

ARTICULO 1° — (Objeto).
La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.
Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.
En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.

ARTICULO 2° — (Definiciones).
A los fines de la presente ley se entiende por:
— Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
— Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.
— Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.
— Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.
— Responsable de archivo, registro, base o banco de datos: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.
— Datos informatizados: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.

— Titular de los datos: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.
— Usuario de datos: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.
— Disociación de datos: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

Capítulo II

Principios generales relativos a la protección de datos

ARTICULO 3° — (Archivos de datos – Licitud).
La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia.
Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

ARTICULO 4° — (Calidad de los datos).
1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.
2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.
3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.
5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.
6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

ARTICULO 5° — (Consentimiento).
1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.
El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.
2. No será necesario el consentimiento cuando:
a) Los datos se obtengan de fuentes de acceso público irrestricto;
b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;
e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

ARTICULO 6° — (Información).
Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara:
a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;
b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;
c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;
d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

ARTICULO 7° — (Categoría de datos).
1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.
3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas.

ARTICULO 8° — (Datos relativos a la salud).
Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

ARTICULO 9° — (Seguridad de los datos).
1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

ARTICULO 10. — (Deber de confidencialidad).
1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

ARTICULO 11. — (Cesión).
1. Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo.
2. El consentimiento para la cesión es revocable.
3. El consentimiento no es exigido cuando:
a) Así lo disponga una ley;
b) En los supuestos previstos en el artículo 5° inciso 2;
c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;
d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;
e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.
4. El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate.

ARTICULO 12. — (Transferencia internacional).
1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.
2. La prohibición no regirá en los siguientes supuestos:
a) Colaboración judicial internacional;
b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior;
c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;
d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;
e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Capítulo III

Derechos de los titulares de datos

ARTICULO 13. — (Derecho de Información).
Toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables.
El registro que se lleve al efecto será de consulta pública y gratuita.

ARTICULO 14. — (Derecho de acceso).
1. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.
2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente.
Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista en esta ley.
3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto.
4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.

ARTICULO 15. — (Contenido de la información).
1. La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen.
2. La información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales. En ningún caso el informe podrá revelar datos pertenecientes a terceros, aun cuando se vinculen con el interesado.
3. La información, a opción del titular, podrá suministrarse por escrito, por medios electrónicos, telefónicos, de imagen, u otro idóneo a tal fin.

ARTICULO 16. — (Derecho de rectificación, actualización o supresión).
1. Toda persona tiene derecho a que sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos.
2. El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.
3. El incumplimiento de esta obligación dentro del término acordado en el inciso precedente, habilitará al interesado a promover sin más la acción de protección de los datos personales o de hábeas data prevista en la presente ley.
4. En el supuesto de cesión, o transferencia de datos, el responsable o usuario del banco de datos debe notificar la rectificación o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato.
5. La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos.
6. Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá o bien bloquear el archivo, o consignar al proveer información relativa al mismo la circunstancia de que se encuentra sometida a revisión.
7. Los datos personales deben ser conservados durante los plazos previstos en las disposiciones aplicables o en su caso, en las contractuales entre el responsable o usuario del banco de datos y el titular de los datos.

ARTICULO 17. — (Excepciones).

1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.
2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.
3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad en que el afectado tenga que ejercer su derecho de defensa.

ARTICULO 18. — (Comisiones legislativas).
Las Comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o las que las sustituyan, tendrán acceso a los archivos o bancos de datos referidos en el artículo 23 inciso 2 por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales Comisiones.

ARTICULO 19. — (Gratuidad).
La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.

ARTICULO 20. — (Impugnación de valoraciones personales).
1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.
2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.

Capítulo IV

Usuarios y responsables de archivos, registros y bancos de datos

ARTICULO 21. — (Registro de archivos de datos. Inscripción).
1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes debe inscribirse en el Registro que al efecto habilite el organismo de control.
2. El registro de archivos de datos debe comprender como mínimo la siguiente información:
a) Nombre y domicilio del responsable;
b) Características y finalidad del archivo;
c) Naturaleza de los datos personales contenidos en cada archivo;
d) Forma de recolección y actualización de datos;
e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;
f) Modo de interrelacionar la información registrada;

g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;
h) Tiempo de conservación de los datos;
i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.
3) Ningún usuario de datos podrá poseer datos personales de naturaleza distinta a los declarados en el registro.
El incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en el capítulo VI de la presente ley.

ARTICULO 22. — (Archivos, registros o bancos de datos públicos).
1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el Boletín Oficial de la Nación o diario oficial.
2. Las disposiciones respectivas, deben indicar:
a) Características y finalidad del archivo;
b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas;
c) Procedimiento de obtención y actualización de los datos;
d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán;
e) Las cesiones, transferencias o interconexiones previstas;
f) Órganos responsables del archivo, precisando dependencia jerárquica en su caso;
g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.
3. En las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción.

ARTICULO 23. — (Supuestos especiales).
1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.
2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.
3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

ARTICULO 24. — (Archivos, registros o bancos de datos privados).
Los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21.

ARTICULO 25. — (Prestación de servicios informatizados de datos personales).

1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.
2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

ARTICULO 26. — (Prestación de servicios de información crediticia).
1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento.
2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés.
3. A solicitud del titular de los datos, el responsable o usuario del banco de datos, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y y el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión.
4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hace constar dicho hecho.
5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios.

ARTICULO 27. — (Archivos, registros o bancos de datos con fines de publicidad).
1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.
2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.
3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo.

ARTICULO 28. — (Archivos, registros o bancos de datos relativos a encuestas).
1. Las normas de la presente ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas relevadas conforme a Ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable.
2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna.

Capítulo V

Control

ARTICULO 29. — (Órgano de Control).
1. El órgano de control deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley. A tales efectos tendrá las siguientes funciones y atribuciones:
a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la presente y de los medios legales de que disponen para la defensa de los derechos que ésta garantiza;
b) Dictar las normas y reglamentaciones que se deben observar en el desarrollo de las actividades comprendidas por esta ley;
c) Realizar un censo de archivos, registros o bancos de datos alcanzados por la ley y mantener el registro permanente de los mismos;
d) Controlar la observancia de las normas sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos. A tal efecto podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos a fin de verificar infracciones al cumplimiento de la presente ley;
e) Solicitar información a las entidades públicas y privadas, las que deberán proporcionar los antecedentes, documentos, programas u otros elementos relativos al tratamiento de los datos personales que se le requieran. En estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados;
f) Imponer las sanciones administrativas que en su caso correspondan por violación a las normas de la presente ley y de las reglamentaciones que se dicten en su consecuencia;
g) Constituirse en querellante en las acciones penales que se promovieran por violaciones a la presente ley;
h) Controlar el cumplimiento de los requisitos y garantías que deben reunir los archivos o bancos de datos privados destinados a suministrar informes, para obtener la correspondiente inscripción en el Registro creado por esta ley.
2. El órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación.
3. El órgano de control será dirigido y administrado por un Director designado por el término de cuatro (4) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.
El Director tendrá dedicación exclusiva en su función, encontrándose alcanzado por las incompatibilidades fijadas por ley para los funcionarios públicos y podrá ser removido por el Poder Ejecutivo por mal desempeño de sus funciones.

ARTICULO 30. — (Códigos de conducta).
1. Las asociaciones o entidades representativas de responsables o usuarios de bancos de datos de titularidad privada podrán elaborar códigos de conducta de práctica profesional, que establezcan normas para el tratamiento de datos personales que tiendan a asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios establecidos en la presente ley.
2. Dichos códigos deberán ser inscriptos en el registro que al efecto lleve el organismo de control, quien podrá denegar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

Capítulo VI

Sanciones

ARTICULO 31. — (Sanciones administrativas).

1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.
2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

ARTICULO 32. — (Sanciones penales).
1. Incorpórase como artículo 117 bis del Código Penal, el siguiente:
"1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.
2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.
3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.
4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".
2. Incorpórase como artículo 157 bis del Código Penal el siguiente:
"Será reprimido con la pena de prisión de un mes a dos años el que:
1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.
Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

Capítulo VII

Acción de protección de los datos personales

ARTICULO 33. — (Procedencia).
1. La acción de protección de los datos personales o de hábeas data procederá:
a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquéllos;
b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización.

ARTICULO 34. — (Legitimación activa).
La acción de protección de los datos personales o de hábeas data podrá ser ejercida por el afectado, sus tutores o curadores y los sucesores de las personas físicas, sean en línea directa o colateral hasta el segundo grado, por sí o por intermedio de apoderado.
Cuando la acción sea ejercida por personas de existencia ideal, deberá ser interpuesta por sus representantes legales, o apoderados que éstas designen al efecto.
En el proceso podrá intervenir en forma coadyuvante el Defensor del Pueblo.

ARTICULO 35. — (Legitimación pasiva).
La acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes.

ARTICULO 36. — (Competencia).
Será competente para entender en esta acción el juez del domicilio del actor; el del domicilio del demandado; el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.
Procederá la competencia federal:
a) cuando se interponga en contra de archivos de datos públicos de organismos nacionales, y
b) cuando los archivos de datos se encuentren interconectados en redes interjurisdicciones, nacionales o internacionales.

ARTICULO 37. — (Procedimiento aplicable).
La acción de hábeas data tramitará según las disposiciones de la presente ley y por el procedimiento que corresponde a la acción de amparo común y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo.

ARTICULO 38. — (Requisitos de la demanda).
1. La demanda deberá interponerse por escrito, individualizando con la mayor precisión posible el nombre y domicilio del archivo, registro o banco de datos y, en su caso, el nombre del responsable o usuario del mismo.
En el caso de los archivos, registros o bancos públicos, se procurará establecer el organismo estatal del cual dependen.
2. El accionante deberá alegar las razones por las cuales entiende que en el archivo, registro o banco de datos individualizado obra información referida a su persona; los motivos por los cuales considera que la información que le atañe resulta discriminatoria, falsa o inexacta y justificar que se han cumplido los recaudos que hacen al ejercicio de los derechos que le reconoce la presente ley.
3. El afectado podrá solicitar que mientras dure el procedimiento, el registro o banco de datos asiente que la información cuestionada está sometida a un proceso judicial.
4. El Juez podrá disponer el bloqueo provisional del archivo en lo referente al dato personal motivo del juicio cuando sea manifiesto el carácter discriminatorio, falso o inexacto de la información de que se trate.
5. A los efectos de requerir información al archivo, registro o banco de datos involucrado, el criterio judicial de apreciación de las circunstancias requeridas en los puntos 1 y 2 debe ser amplio.

ARTICULO 39. — (Trámite).
1. Admitida la acción el juez requerirá al archivo, registro o banco de datos la remisión de la información concerniente al accionante. Podrá asimismo solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente.
2. El plazo para contestar el informe no podrá ser mayor de cinco días hábiles, el que podrá ser ampliado prudencialmente por el juez.

ARTICULO 40. — (Confidencialidad de la información).
1. Los registros, archivos o bancos de datos privados no podrán alegar la confidencialidad de la información que se les requiere salvo el caso en que se afecten las fuentes de información periodística.

2. Cuando un archivo, registro o banco de datos público se oponga a la remisión del informe solicitado con invocación de las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la presente ley o por una ley específica; deberá acreditar los extremos que hacen aplicable la excepción legal. En tales casos, el juez podrá tomar conocimiento personal y directo de los datos solicitados asegurando el mantenimiento de su confidencialidad.

ARTICULO 41. — (Contestación del informe).
Al contestar el informe, el archivo, registro o banco de datos deberá expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no evacuó el pedido efectuado por el interesado, de conformidad a lo establecido en los artículos 13 a 15 de la ley.

ARTICULO 42. — (Ampliación de la demanda).
Contestado el informe, el actor podrá, en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente a tenor de la presente ley, ofreciendo en el mismo acto la prueba pertinente. De esta presentación se dará traslado al demandado por el término de tres días.

ARTICULO 43. — (Sentencia).
1. Vencido el plazo para la contestación del informe o contestado el mismo, y en el supuesto del artículo 42, luego de contestada la ampliación, y habiendo sido producida en su caso la prueba, el juez dictará sentencia.
2. En el caso de estimarse procedente la acción, se especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial, estableciendo un plazo para su cumplimiento.
3. El rechazo de la acción no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante.
4. En cualquier caso, la sentencia deberá ser comunicada al organismo de control, que deberá llevar un registro al efecto.

ARTICULO 44. — (Ámbito de aplicación).
Las normas de la presente ley contenidas en los Capítulos I, II, III y IV, y artículo 32 son de orden público y de aplicación en lo pertinente en todo el territorio nacional.
Se invita a las provincias a adherir a las normas de esta ley que fueren de aplicación exclusiva en jurisdicción nacional.
La jurisdicción federal regirá respecto de los registros, archivos, bases o bancos de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.

ARTICULO 45. — El Poder Ejecutivo Nacional deberá reglamentar la presente ley y establecer el organismo de control dentro de los ciento ochenta días de su promulgación.

ARTICULO 46. — (Disposiciones transitorias).
Los archivos, registros, bases o bancos de datos destinados a proporcionar informes, existentes al momento de la sanción de la presente ley, deberán inscribirse en el registro que se habilite conforme a lo dispuesto en el artículo 21 y adecuarse a lo que dispone el presente régimen dentro del plazo que al efecto establezca la reglamentación.

ARTICULO 47. — Los bancos de datos prestadores de servicios de información crediticia deberán suprimir, o en su caso, omitir asentar, todo dato referido al incumplimiento o mora

en el pago de una obligación, si ésta hubiere sido cancelada al momento de la entrada en vigencia de la presente ley.

ARTICULO 48. — Comuníquese al Poder Ejecutivo.

LEY 25.873
TELECOMUNICACIONES

Modifícase la Ley N° 19.798, en relación con la responsabilidad de los prestadores respecto de la captación y derivación de comunicaciones para su observación remota por parte del Poder Judicial o Ministerio Público.

Sancionada: Diciembre 17 de 2003.
Promulgada de Hecho: Febrero 6 de 2004.
El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ARTICULO 1° — Incorpórase el artículo 45 bis a la Ley 19.798 con el siguiente texto:
"Todo prestador de servicios de telecomunicaciones deberá disponer de los recursos humanos y tecnológicos necesarios para la captación y derivación de las comunicaciones que transmiten, para su observación remota a requerimiento del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente.
Los prestadores de servicios de telecomunicaciones deberán soportar los costos derivados de dicha obligación y dar inmediato cumplimiento a la misma a toda hora y todos los días del año.
El Poder Ejecutivo nacional reglamentará las condiciones técnicas y de seguridad que deberán cumplir los prestadores de servicios de telecomunicaciones con relación a la captación y derivación de las comunicaciones para su observación remota por parte del Poder Judicial o el Ministerio Público."

ARTICULO 2° — Incorpórase el artículo 45 ter a la Ley 19.798 con el siguiente texto:
"Los prestadores de servicios de telecomunicaciones deberán registrar y sistematizar los datos filiatorios y domiciliarios de sus usuarios y clientes y los registros de tráfico de comunicaciones cursadas por los mismos para su consulta sin cargo por parte del Poder Judicial o el Ministerio Público de conformidad con la legislación vigente. La información referida en el presente deberá ser conservada por los prestadores de servicios de telecomunicaciones por el plazo de diez años."

ARTICULO 3° — Incorpórase el artículo 45 quáter a la Ley 19.798 con el siguiente texto:
"El Estado nacional asume la responsabilidad por los eventuales daños y perjuicios que pudieran derivar para terceros, de la observación remota de las comunicaciones y de la utilización de la información de los datos filiatorios y domiciliarios y tráfico de comunicaciones de clientes y usuarios, provista por los prestadores de servicios de telecomunicaciones."

ARTICULO 4° — Comuníquese al Poder Ejecutivo.

Decreto 1563/2004
TELECOMUNICACIONES

Reglaméntanse los artículos 45 bis, 45 ter y 45 quáter de la Ley N° 19.798 y sus modificaciones, con la finalidad de establecer las condiciones técnicas y de seguridad que deberán cumplir los prestadores de servicios de telecomunicaciones en relación con la captación y derivación de las comunicaciones para su observación remota por parte del Poder Judicial o del Ministerio Público. Obligaciones de los operadores y licenciatarios de servicios de telecomunicaciones. Reclamos administrativos y vía judicial. Adecuación del equipamiento y tecnologías que se utilizan para la prestación de servicios de telecomunicaciones, a los efectos de la presente normativa. Plazos referidos a los requerimientos de interceptación y de información que se efectúen. Sanciones. Reglaméntase asimismo el artículo 34 de la citada Ley en relación con la competencia del órgano del Estado legalmente encargado de las verificaciones e inspecciones.

Bs. As., 8/11/2004
VISTO la Ley N° 25.873, modificatoria de la Ley Nacional de Telecomunicaciones N° 19.798, y sus modificaciones, y la Ley N° 25.520 y su Decreto Reglamentario N° 950/02, y

CONSIDERANDO:
Que la Ley N° 25.873 incorporó a la Ley Nacional de Telecomunicaciones los artículos 45 bis, 45 ter y 45 quáter.
Que el objetivo de la ley es combatir el delito, y a la par servir al esquema de seguridad colectivo de la Nación, ello mediante la utilización de modernas herramientas de captación y monitoreo de comunicaciones de las redes públicas y/o privadas de telecomunicaciones, cualquiera sea su naturaleza, origen o tecnología, en tanto operen en el territorio nacional, orientado a desbaratar las amenazas que resultan factibles de vislumbrar.
Que las actividades ilícitas son un flagelo que se vale de múltiples herramientas para su ejecución, entre las cuales sobresale el uso de sistemas de telecomunicaciones de la más variada gama, evidenciado en la utilización de modernas tecnologías, particularmente, y a sólo título de ejemplo, en los casos de secuestros extorsivos y narcotráfico.
Que, asimismo, y en el marco también de los objetivos apuntados, resulta conveniente y necesario establecer temperamentos de acción concretos y dinámicos, que hagan factible al órgano estatal legalmente encargado de materializar la interceptación de las telecomunicaciones, formular los requerimientos del caso a los prestadores, orientados al objeto de esta normativa, con sustento en las incumbencias que emanan de la Ley N° 25.520 y su reglamentación, en un marco de máxima celeridad, sencillez y eficacia.
Que el tercer párrafo del artículo 45 bis incorporado a la Ley N° 19.798 y sus modificaciones establece que el PODER EJECUTIVO NACIONAL reglamentará las condiciones técnicas y de seguridad que deberán cumplir los prestadores de servicios de telecomunicaciones con relación a la captación y derivación de las comunicaciones para su observación remota por parte del Poder Judicial o del Ministerio Público.
Que otros países ya han normado sobre la materia, con resultados eficaces tanto en el ámbito público como el privado.
Que ha tomado la intervención de su competencia el Servicio Jurídico pertinente.
Que la presente medida se dicta en virtud de lo dispuesto en el artículo 99, inciso 2 de la Constitución Nacional.
Por ello,
EL PRESIDENTE DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — A los efectos del presente decreto, se adoptan las siguientes definiciones:

Telecomunicaciones: Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, cable eléctrico, atmósfera, radio electricidad, medios ópticos y/u otros medios electromagnéticos, o de cualquier clase existentes o a crearse en el futuro.
Prestador: Es el licenciatario del servicio de Telecomunicaciones, en cualquiera de sus formas o modalidades, presentes o futuras.
Usuario: Es toda persona física o jurídica que utiliza los servicios de un prestador.
Captación de la telecomunicación: Es la obtención e individualización, a través de medios técnicos, del contenido de una telecomunicación que se produce entre dos o más puntos o destinos.
Derivación de la telecomunicación: Es la modificación de la ruta de la telecomunicación con el fin de permitir su observación remota, sin modificar su contenido y características originales.
Observación remota: Es la observación de las telecomunicaciones efectuada desde las centrales de monitoreo del órgano del Estado encargado de ejecutar las interceptaciones.
Lugar de observación remota: Son los centros de monitoreo del órgano del Estado encargado de ejecutar las interceptaciones, desde los cuales se efectúa la observación de las telecomunicaciones.
Información asociada: Debe entenderse por tal, toda la información original, no alterada por proceso alguno, que permita individualizar el origen y destino de las telecomunicaciones, tales como registros de tráfico, identificación y ubicación del equipo utilizado, y todo otro elemento que torne factible establecer técnicamente su existencia y características.
Órgano del Estado encargado de ejecutar las interceptaciones: Conforme a la Ley N° 25.520 es la DIRECCION DE OBSERVACIONES JUDICIALES de la SECRETARIA DE INTELIGENCIA de la PRESIDENCIA DE LA NACION.
Autoridad de Aplicación: Es la COMISION NACIONAL DE COMUNICACIONES, dependiente de la SECRETARIA DE COMUNICACIONES del MINISTERIO DE PLANIFICACION FEDERAL, INVERSION PUBLICA Y SERVICIOS.
Autoridad de Regulación: Es la SECRETARIA DE COMUNICACIONES dependiente del MINISTERIO DE PLANIFICACION FEDERAL, INVERSION PUBLICA Y SERVICIOS.

Art. 2° — Reglaméntase el artículo 45 bis de la Ley N° 19.798 y sus modificaciones:
a) En todos los casos, la obligación establecida en el artículo 45 bis de la Ley N° 19.798 y sus modificaciones abarcará la información inherente a las telecomunicaciones y la información asociada a las telecomunicaciones, incluyendo la que permita establecer la ubicación geográfica de los equipos involucrados en ellas, como asimismo todo otro dato que pudiera emanar de los mismos.
b) Cuando, por el tipo de tecnología o estructura de redes seleccionado u otras razones técnicas, resulte necesario utilizar herramientas o recursos técnicos, inclusive software o hardware específicos, para la interceptación y derivación de las comunicaciones, las compañías licenciatarias de servicios de telecomunicaciones deberán disponer de estos recursos desde el mismo momento en que el equipamiento o tecnología comience a ser utilizado. A tal fin, previo a ello, se deberán realizar las pruebas técnicas operativas del equipamiento que se trate y será un requisito ineludible su consecuente aprobación por parte de las autoridades públicas intervinientes, quienes a los fines de la presente normativa, tendrán facultades de supervisión e inspección. Los prestadores deberán mantener informados a dichos organismos acerca de sus innovaciones tecnológicas y operativas, y sobre la aplicación de nuevos servicios que tengan implicancias técnicas.
c) Los prestadores de servicios de telecomunicaciones serán responsables por el uso que se dé a los recursos mencionados en el punto anterior fuera del marco del cumplimiento de la

presente norma. Dicha responsabilidad comprende a todo acto realizado por sí, por sus dependientes o por terceros de cuyos servicios se valgan.
d) Los prestadores de servicios de telecomunicaciones deberán mantener la confidencialidad de las actividades técnicas y administrativas que deban realizar a fin de cumplir con los requerimientos que se le efectúen en el marco de la presente norma, y deberán guardar secreto aun respecto de la existencia misma de los requerimientos que les sean efectuados. Serán aplicables con relación a lo aquí dispuesto las normas penales que tutelan el secreto.
e) Los prestadores de servicios de telecomunicaciones no podrán, bajo ningún concepto, incorporar arquitectura de redes, tecnología ni equipamiento que impida la interceptación en forma remota de las comunicaciones conforme a los procedimientos legalmente establecidos. Tampoco podrán incorporar servicios que pudieren entorpecer, limitar o disminuir, de cualquier manera, la obtención de la interceptación y de toda la información que se prevé en el presente.
f) Los operadores arriendan infraestructura a terceros deberán contar con los medios técnicos que permitan la observación de todas las comunicaciones que se cursan por sus redes, aun las de otras licenciatarias o usuarios que utilizan su estructura.
g) Todas las comunicaciones originadas en redes de telecomunicaciones, sin excepción alguna, deben ser cursadas sólo si el operador que las origina envía un número que identifique al usuario y al prestador de origen, siempre que no provenga de una llamada desviada.
Los prestadores de servicios de telecomunicaciones de larga distancia internacional que reciban tráfico de terceros operadores internacionales con destino a redes locales, deberán identificar igualmente dichas llamadas de modo de establecer su origen, prestador y abonado de origen.
La autoridad de regulación, puede establecer excepciones para los casos de llamadas internacionales entrantes de países que no transmitan el ANI Número de A con formato de número internacional.
h) La información que se intercambiará en tiempo real en la señalización para la interconexión entre redes deberá incluir:
El número de "A", entendiéndose por tal al "Número que identifica el origen de una llamada", con formato de "número nacional", de acuerdo a lo dispuesto en la Resolución N° 47 de fecha 13 de enero de 1997 de la SECRETARIA DE COMUNICACIONES (Plan Fundamental de Señalización Nacional), o la normativa que la reemplace en el futuro.
Lo expuesto es aplicable a las llamadas de servicios montados sobre redes inteligentes, como tarjetas y cualquier otra modalidad actual o futura, siendo a tal fin insuficiente la sola identificación de plataforma del operador.
La categoría de "A" deberá contener al menos: operadora, teléfono público o abonado normal.
El número de "B", entendiéndose por tal al "Número que identifica al destino de una llamada" con formato de número nacional o número internacional, según corresponda.
El estado de "NB", deberá contener al menos: abonado libre, abonado ocupado y contestación (conexión).
i) Asimismo, los operadores deben poner a disposición los medios técnicos y humanos necesarios para que esa información pueda ser recibida en tiempo real y en condiciones de ser interpretada por el órgano del Estado encargado de ejecutar las interceptaciones, salvedad hecha, en su caso, de una comunicación que se encuentre en curso, al momento mismo de la efectivización de la interceptación.
j) Las interceptaciones y derivaciones que deben efectuar las compañías licenciatarias de servicios de telecomunicaciones a requerimiento del órgano del Estado encargado de ejecutarlas, deberán hacerse efectivas de inmediato, a través de sistemas de gestión de conexión directa, salvedad hecha de aquellos prestadores que merezcan un tratamiento particular justificado por parte del Órgano del Estado encargado de ejecutar las interceptaciones y de manera tal que:

1- Permitan la observación aun cuando el usuario intervenido desvíe las llamadas hacia otros servicios de telecomunicaciones o equipos terminales, incluidas las llamadas que atraviesen más de una red o que estén procesadas por más de un operador de red/ proveedor de servicio.
2- En el caso de abonados de telefonía móvil, permitan su observación desde la central de monitoreo designada por el órgano del Estado encargado de ejecutar las interceptaciones, aun cuando el usuario intervenido se encuentre en tránsito en el área de cobertura de otro prestador que le brinde servicio. Cuando el servicio a observar se encuentre en tránsito fuera del ámbito nacional, el prestador deberá informar en forma inmediata, en cuanto sus sistemas lo permitan, cual es el proveedor del exterior que ha adquirido acceso a esas comunicaciones y resguardar toda la información de tasación y tráfico que registre.
3- Se obtenga y transmita para su observación en tiempo real, el contenido de la telecomunicación en formato y calidad original, y en forma simultánea, toda la información asociada con que cuente la compañía y que pueda resultar útil al organismo estatal para cumplir con su cometido; como ser: número de "A", número de "B", hora de inicio, finalización y duración de la comunicación o conexión, señalización de acceso a estado disponible; número de "B" para conexiones salientes aún en los casos en los que no haya una conexión establecida en forma satisfactoria; número de "A" para conexiones entrantes aún en los casos en los que no haya una conexión establecida en forma satisfactoria; todas las señales emitidas por el objetivo, incluídas aquellas emitidas para activar servicios tales como la llamada en conferencia y la transferencia de llamadas; destino actual y otros números en los casos en los que se haya desviado la llamada, identificación y ubicación del receptor (celda, sector, radio de acción de la celda).
4- Permita lograr una correlación exacta de los datos mencionados en el punto anterior con el contenido de las llamadas.
5- La interceptación incluya todos los servicios y facilidades brindados al cliente.
6- La medida se realice sin que se produzcan alteraciones en el servicio que puedan alertar al causante.
7- Sean provistas sólo las telecomunicaciones desde y hacia un servicio tomado como objetivo, con exclusión de cualquier telecomunicación que no esté incluida dentro del alcance de la autorización de interceptación.
8- Las comunicaciones interceptadas serán derivadas decodificadas, descomprimidas y desencriptadas para el caso de que los operadores de red/ proveedores de servicio codifiquen, compriman o encripten o de cualquier otro modo, modifiquen a efectos de la transmisión o tráfico, el contenido de las telecomunicaciones que cursan. Esta obligación subsistirá para el caso en que la codificación, compresión, encriptado o modificación sea realizada por el usuario o cliente con herramientas o recursos técnicos provistos por el prestador.
9- Sin perjuicio de lo establecido en los apartados precedentes, las prestatarias proporcionarán al órgano del Estado encargado de ejecutar las interceptaciones los medios técnicos necesarios para que, al recepcionarse la orden judicial, éstas sean efectivizadas en forma inmediata por el propio organismo estatal desde su centro de monitoreo, ello con la salvedad prevista en primer párrafo del presente apartado, adoptando las medidas de resguardo y conservación a que hubiere lugar, debiendo luego darse estricto cumplimiento al procedimiento establecido en el artículo 22 de la Ley N° 25.520 y en el artículo 15 del Anexo I del Decreto N° 950/02. A tal fin, los prestadores deberán adecuar equipamiento y tecnología necesarios de conformidad con lo previsto en el primer párrafo del artículo 5° del presente.
k) Las compañías licenciatarias de servicios de telecomunicaciones deberán suministrar al órgano del Estado encargado de ejecutar las interceptaciones, la información asociada a sus abonados que les sea requerida para el cumplimiento de su cometido.
l) Los prestadores de servicios de telecomunicaciones deberán instrumentar los recursos pertinentes para recibir y dar respuesta a las solicitudes de aquél órgano estatal que requie-

ran su inmediata instrumentación, las VEINTICUATRO (24) horas del día y todos los días del año.
m) Los prestadores deberán contar con la capacidad necesaria para llevar adelante las obligaciones que emanan de la presente normativa. Asimismo, los prestadores deberán coordinar con el órgano del Estado encargado de ejecutar las interceptaciones, los procedimientos conducentes al desarrollo de las tareas técnicas necesarias para el cumplimiento de la presente normativa.
n) La autoridad de contralor garantizará el cumplimiento de estas medidas y estará facultada en su caso, de oficio o a pedido de parte, a sancionar el incumplimiento mediante la aplicación del régimen pertinente, sin perjuicio de las responsabilidades personales a que hubiere lugar conforme a las normas legales vigentes.
o) Los prestadores de servicios de comunicaciones, deberán soportar los costos de todo equipamiento, elemento tecnológico (software o hardware), vinculación, línea o trama, nueva o existente, necesaria para la captación de las comunicaciones y conexión efectiva entre sus centrales y el lugar de observación remota, y la obtención de los datos asociados en las condiciones establecidas en la presente norma. Asimismo, deberán tomar a su cargo los costos de equipamiento, personal, insumos y todo otro gasto que resulte necesario para el cumplimiento de las obligaciones establecidas en la ley conforme al presente decreto, incluyéndose los servicios que se presten al órgano encargado de ejecutar la interceptación para transportar las telecomunicaciones, y los del tendido de cualquier vínculo con dicho propósito, como asimismo la totalidad de los servicios o actividades que fueran necesarios para el cumplimiento de las tareas que impone para la materia la normativa aplicable.
Para los casos previstos en la salvedad incluida en el artículo 2°, apartado j), se admitirán vínculos conmutados.
p) A los efectos de la presente normativa, el órgano del Estado legalmente encargado de ejecutar la interceptación deberá indicar el lugar de observación remota en el requerimiento de interceptación. Dicho organismo podrá determinar otros lugares físicos hacia los cuales se deberán efectuar las derivaciones, según las necesidades operativas propias de cada requerimiento.

Art. 3° — Reglaméntese el artículo 45 ter de la Ley N° 19.798 y sus modificaciones:
a) Los operadores deberán dar acceso a los datos contractuales actualizados que con relación a sus clientes posean, inclusive la ubicación geográfica y demás datos respecto de los abonados, incluyendo la ubicación geográfica exacta de abonados públicos y semipúblicos.
b) Los licenciatarios de servicios de telecomunicaciones deben arbitrar los medios técnicos y humanos necesarios para que la información esté disponible de inmediato, a toda hora y todos los días del año. Los requerimientos serán realizados por el órgano del Estado encargado de ejecutar las interceptaciones en el marco de la legislación vigente y con sustento en las normas que establece la Ley N° 25.520 y su reglamentación.
c) Para dar respuesta a los requerimientos aludidos, los licenciatarios deberán establecer mecanismos que permitan la inmediatez de su respuesta. A tal fin, los pedidos y sus contestaciones podrán ser canalizados a través de medios electrónicos u otros medios fehacientes, siempre que guarden la debida tutela de la información, y en tanto resulten idóneos conforme a la celeridad y certeza que la tarea exige.
d) Los licenciatarios de servicios de telecomunicaciones deberán conservar los datos filiatorios de sus clientes y los registros originales correspondientes a la demás información asociada a las telecomunicaciones, por el término de DIEZ (10) años.

Art. 4° — Reglaméntase el artículo 45 quáter de la Ley N° 19.798 y sus modificaciones:
1- Será requisito previo la formulación del pertinente reclamo administrativo por ante los órganos mencionados en la presente reglamentación. Una vez agotada dicha vía quedará expedita la acción judicial.

2- La responsabilidad atribuida al Estado Nacional será declinada en los prestadores o terceros cuando resulte manifiesta la responsabilidad de estos últimos, sin que ello obste a las defensas que aquel pueda ejercitar tanto en sede administrativa como judicial, o a las investigaciones internas a que hubiere lugar, y sin perjuicio de la posibilidad de la acción de regreso del Estado Nacional contra los prestadores que por acción u omisión hubieran ocasionado un daño a un tercero.

Art. 5° — Los prestadores deberán adecuar el equipamiento y tecnologías que utilizan para la prestación de los servicios de telecomunicaciones, a los efectos de la presente normativa, antes del 31 de julio de 2005. La autoridad de contralor deberá velar por el cumplimiento de lo dispuesto, y podrá sólo en casos excepcionales otorgar un plazo de gracia cuando razones técnicas atendibles así lo justifiquen, el cual no podrá extenderse en ningún caso más allá del 30 de septiembre de 2005. En tal supuesto, se deberá efectuar un estricto seguimiento de los planes de adecuación.
Las únicas salvedades a la pauta temporal expuesta serán:
1- La relativa a las modificaciones y adecuaciones tendientes a dar respuesta a los requerimientos de información registral, las cuales deberán hacerse efectivas en un lapso improrrogable de NOVENTA (90) días hábiles administrativos, contados a partir de la entrada en vigencia de esta norma.
2- Las tecnologías y equipamiento incorporados con posterioridad a la entrada en vigencia de la presente reglamentación, para los cuales, el cumplimiento será obligatorio desde su implementación (conforme a lo previsto por el inciso b) del artículo 2).

Art. 6° — Los requerimientos de interceptación y de información que se efectúen conforme al presente régimen deberán responderse en forma adecuada, oportuna y veraz, en los siguientes plazos:
a) Los requerimientos de interceptación calificados como "urgente", deberán hacerse efectivos en forma inmediata, con los tiempos mínimos que técnicamente resulten necesarios para la implementación de la derivación.
b) Los restantes requerimientos de interceptación deberán hacerse efectivos en el plazo de en UN (1) día a partir de la recepción del requerimiento.
c) Los requerimientos de información relativos a los datos filiatorios de usuarios de servicios vigentes deberán ser respondidos de inmediato.
d) Los requerimientos de información calificados como "urgente", correspondientes a telecomunicaciones que están siendo observadas, y relativos al período de observación o a los TREINTA (30) días anteriores al pedido, deberán ser respondidos de inmediato.
e) Los restantes requerimientos de información, calificados como "urgente" según el período comprendido deberán ser respondidos en los siguientes plazos:
- De hasta TRES (3) meses anteriores al requerimiento: en el término de UNA (1) hora.
- De más de TRES (3) meses y hasta DOS (2) años: en el término de SEIS (6) horas.
- De más de DOS (2) años: en el término de DOS (2) días.
f) Los restantes requerimientos según el período comprendido, deberán ser respondidos en los siguientes plazos:
- De abonados conectados y relativos al período de intervención: en el término de UNA (1) hora.
- Del mes del requerimiento: en el término de UN (1) día.
- De más de TRES (3) meses y hasta DOS (2) años: en el término de DOS (2) días.
- De más de DOS (2) años: en el término de CINCO (5) días.

Art. 7° — La potestad sancionatoria será ejercida por la autoridad de aplicación. Cualquier violación a las disposiciones de la presente normativa, imputable a un prestador, verificada

de oficio o a pedido de parte, será susceptible de ser sancionada de acuerdo a lo establecido en la respectiva licencia y en el artículo 38 del Decreto N° 1185/90 y sus modificatorios, adecuándose a la norma del presente artículo cuando así proceda.
La Autoridad de Aplicación verificará los incumplimientos denunciados y una vez comprobada la falta, evaluará la sanción a aplicar considerando las siguientes circunstancias:
a) La gravedad de la falta.
b) Los antecedentes del prestador con relación al presente régimen.
c) Sus antecedentes generales, particularmente sus recursos tecnológicos.
d) Las reincidencias.
e) Los elementos del caso, la actitud asumida por el prestador y el perjuicio causado por su acción u omisión.
f) El grado de afectación del interés público.

Art. 8° — Reglaméntase el artículo 34 de la Ley 19.798 y sus modificaciones:
A los efectos de las verificaciones e inspecciones relativas al cumplimiento de las obligaciones legales relativas a las interceptaciones de las telecomunicaciones, será competente el órgano del Estado legalmente encargado de ejecutarlas, con el concurso de la Autoridad de Aplicación.

Art. 9° — Comuníquese, publíquese, dése a la DIRECCION NACIONAL DEL REGISTRO OFICIAL y archívese. — KIRCHNER. — Alberto A. Fernández. — Julio M. De Vido**. —** Aníbal D. Fernández.

Decreto 357/2005
TELECOMUNICACIONES

Suspéndese la aplicación del Decreto N° 1563 del 8 de noviembre de 2004.
Bs. As., 22/4/2005
VISTO la Ley N° 25.873, modificatoria de la Ley Nacional de Telecomunicaciones N° 19.798 y el Decreto N° 1563 del 8 de noviembre de 2004, y

CONSIDERANDO:
Que la Ley N° 25.873 incorporó a la Ley Nacional de Telecomunicaciones N° 19.798 los artículos 45 bis, 45 ter y 45 quáter, los que oportunamente fueron reglamentados a través del Decreto que se cita en el Visto.
Que dicha reglamentación se dictó en el marco de los objetivos tenidos en mira por ese cuerpo legal, esto es combatir el delito y servir al esquema de seguridad colectivo de la Nación, mediante la utilización de modernas herramientas de captación y monitoreo de comunicaciones de las redes públicas y/o privadas de telecomunicaciones, cualquiera sea su naturaleza, origen o tecnología, en tanto operen en el territorio nacional.
Que en esta instancia, razones que son de público conocimiento aconsejan suspender la aplicación del citado decreto, a los fines de permitir un nuevo análisis del tema y de las consecuencias que el mismo implica.
Que la presente medida se dicta en uso de las atribuciones conferidas por el artículo 99, incisos 1 y 2 de la CONSTITUCION NACIONAL.
Por ello,
EL PRESIDENTE DE LA NACION ARGENTINA
DECRETA:

Artículo 1° — Suspéndese la aplicación del Decreto N° 1563 del 8 de noviembre de 2004.

Art. 2° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — KIRCHNER. — Alberto A. Fernández. — Aníbal D. Fernández. — Julio M. De Vido.

LEY 26.388
CÓDIGO PENAL. MODIFICACIÓN.

Sancionada: Junio 4 de 2008
Promulgada de Hecho: Junio 24 de 2008
El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ARTÍCULO 1° — Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes:
El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

ARTICULO 2° — Sustitúyese el artículo 128 del Código Penal, por el siguiente:
Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.
Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

ARTICULO 3° — Sustitúyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente:
"Violación de Secretos y de la Privacidad"

ARTICULO 4° — Sustitúyese el artículo 153 del Código Penal, por el siguiente:
Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el 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.
En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.
La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.
Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

ARTICULO 5° — Incorpórase como artículo 153 bis del Código Penal, el siguiente:
Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin

la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.
La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

ARTICULO 6° — Sustitúyese el artículo 155 del Código Penal, por el siguiente:
Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el 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.

ARTICULO 7° — Sustitúyese el artículo 157 del Código Penal, por el siguiente:
Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

ARTICULO 8° — Sustitúyese el artículo 157 bis del Código Penal, por el siguiente:
Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:
1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.
Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

ARTICULO 9° — Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente:
Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

ARTICULO 10. — Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente:
En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

ARTICULO 11. — Sustitúyese el artículo 184 del Código Penal, por el siguiente:
Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:
1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;
2. Producir infección o contagio en aves u otros animales domésticos;
3. Emplear substancias venenosas o corrosivas;
4. Cometer el delito en despoblado y en banda;
5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas,

cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;
6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

ARTICULO 12. — Sustitúyese el artículo 197 del Código Penal, por el siguiente:
Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

ARTICULO 13. — Sustitúyese el artículo 255 del Código Penal, por el siguiente:
Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el 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 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.
Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

ARTICULO 14. — Deróganse el artículo 78 bis y el inciso 1° del artículo 117 bis del Código Penal.

ARTICULO 15. — Comuníquese al Poder Ejecutivo.

BIBLIOGRAFÍA

- LIBROS, ARTÍCULOS Y PONENCIAS:

ALFONSO, Carlos A.; "Gobernanza de Internet. Un Análisis en el Contexto de la CMSI", publicado en: www.wsispapers.choike.org, Julio de 2005.

BARBER, Benjamín R. y otros, "Internet, Derecho y Política. Las transformaciones del Derecho y la Política en 15 artículos", Editorial UOC, Barcelona, 2009.

BIDART CAMPOS, Germán J., "Manual de la Constitución Reformada", Tomo I y II, Editorial Ediar, Buenos Aires, 1996.

BOLOTNIKOFF, Pablo, "Informática y Responsabilidad Civil", Editorial La Ley, Buenos Aires, 2004.

ALTMARK, Daniel R. (dir.), BIELSA, Rafael A. (coord.) y otros, "Informática y Derecho", Volumen 8: Internet, Editorial Lexis Nexis, Buenos Aires, 2002.

BUSTAMANTE ALSINA, Jorge, "Teoría General de la Responsabilidad Civil", Novena Edición, Editorial Abeledo Perrot, Buenos Aires, 1997.

CASTRO BONILLA, Alejandra, "La regulación de Internet: un reto jurídico", publicado en: http://www.uned.ac.cr/redti/documentos/regulacion.pdf

COTINO HUESO, Lorenzo (coord.) y otros, "Libertad en Internet. La red y las libertades de expresión e información", Editorial Tirant Lo Blanch, Valencia, 2007.

CROVI DRUETTA, Delia María; "¿Es Internet un medio de comunicación?". Revista Digital Universitaria [en línea]. 10 de junio 2006, Vol. 7, No. 6. Publicado en: www.revista.unam.mx/vol.7/num6/art46/int46.htm

FARINELLA, Favio, "El correo electrónico y el *spam*, sometidos a una consulta sobre su regulación", Alfa-Redi: Revista de Derecho Informático, No. 041, Diciembre del 2001, publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=1005

– "Algunas notas sobre *spamming* y su regulación", Alfa-Redi Revista de Derecho Informático, No. 94, Mayo de 2006, publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=6102

FERNANDEZ DELPECH, Horacio, "Internet: Su problemática jurídica", Editorial Abeledo Perrot, Buenos Aires, 2004.

GALDÓS, Jorge Mario, "Correo electrónico, privacidad y daños", Revista de derecho de Daños 2001-3-157, publicado en: http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/galdos.pdf

– "Responsabilidad civil e Internet: Algunas aproximaciones", JA 2001-III-819, publicado en: http://www.abeledoperrot.com.ar

GINI, Santiago Luis, "Internet, buscadores de sitios web y libertad de expresión", publicado en: http://www.laleyonline.com.ar

GONZÁLEZ FREA, Leandro, "Un breve Análisis Jurídico de las Redes Sociales en Internet en la óptica de la normativa Argentina", publicado en: http://www.gonzalezfrea.com.ar/derecho-informatico/aspectos-legales-redes-sociales-legislacion-normativa-facebook-regulacion-legal-argentina/265

GRÜN, Ernesto, "Una visión sistémica y cibernética del derecho en el mundo globalizado del siglo XXI", Editorial Lexis Nexis, Buenos Aires, 2005.

HOCSMAN, Heriberto Simón, "Negocios en Internet", Editorial Astrea, Buenos Aires, 2005.

JIJENA LEIVA, Renato Javier, "Contenidos de Internet: Censura o Libertad de Expresión", publicado en: http://www.mass.co.cl/acui/leyes-jijena2.html

LAMARCA LAPUENTE, María Jesús, "Hipertexto: El nuevo concepto de documento en la cultura de la imagen", Tesis doctoral, Universidad Complutense de Madrid, publicada en http://www.hipertexto.info/ documentos/serv_internet.htm

MANILI, Pablo Luis (coord.) y otros, "Derecho Procesal Constitucional", Editorial Universidad, Buenos Aires, 2005

MIROLO, René Ricardo (dir.), "Curso del Derecho del Trabajo y de la Seguridad Social", Tomo I, Editorial Advocatus, Córdoba, 2003.

MOEREMANS, Daniel E. y CASAS, Manuel Gonzalo, "Protección del e-mail como extensión del derecho a la intimidad", publicado en: http://www.laleyonline.com.ar

MOLINA QUIROGA, Eduardo, "Internet y la libertad de expresión. A propósito de la ley 26032", publicado en: http://www.abeledoperrot.com.ar

OLIVERA, Noemí L., "Reflexiones en torno al sistema jurídico de la Sociedad de la Información", publicado en: http://www.abeledoperrot.com.ar

PANDIELLA, Juan Carlos, "El bien jurídico tutelado por el hábeas data", publicado en: http://www.foroabogadossanjuan.org.ar/Doctrina_Provincial/pandiella.htm

PARELLADA, Carlos A., "Responsabilidad por la actividad anónima en Internet", publicado en: http://www.laleyonline.com.ar

PIACENZA, Diego Fabio, "El derecho a la intimidad y los medios de comunicación", agosto de 2009, publicado en: http://www.alfa-redi.org/rdiarticulo.shtml?x=16099

– "Delitos Informáticos", Alfa-Redi: Revista de Derecho Informático, No. 127, Febrero del 2009, publicado en: http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/piacenza_2.pdf

PIZARRO, Ramón Daniel, "Responsabilidad civil de los medios masivos de comunicación. Daños por noticias inexactas o agraviantes.", Editorial Hammurabi, Buenos Aires, 1999.

PLAZA SOLER, Juan Carlos, "Los correos electrónicos comerciales no solicitados en el derecho europeo y norteamericano", Ponencia II Congreso Mundial de Derecho Informático. Madrid. 2002, publicado en: http://www.ieid.org/congreso/ponencias/Plaza%20Soler,%20Juan%20Carlos.pdf

PRENAFETA, Javier, "Protección de datos y secreto de las comunicaciones en las redes P2P", publicado en: http://www.jprenafeta.com/2008/06/06/proteccion-de-datos-y-secreto-de-las-comunicaciones-en-las-redes-p2p

PUENTE DE LA MORA, Ximena, "Privacidad de la Información Personal y su Protección Legal en Estados Unidos", Alfa-Redi: Revista de Derecho Informático, No. 97, Junio del 2006, publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=6956

SAN JUAN, Andrés, "Comentarios sobre la Ley de Delitos Informáticos", Alfa-Redi: Revista de Derecho Informático, No. 119, Junio del 2008, publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=10653

SANTOS, Estefanía, "¿Que Herramientas Legales Existen contra Contenidos Dañosos en Redes Sociales?", mayo de 2010, publicado en: http://www.estefaniasantos.com.ar

SOBRINO, Waldo Augusto Roberto, "Internet y la alta tecnología en el derecho de daños", Editorial Universidad, Buenos Aires, 2003.

– "Las Cookies y el *Spam* (y la violación de la Privacidad y la Intimidad)", publicado en: http://www.alfa-redi.org/rdi-articulo.shtml?x=710, Junio de 2001.

TREJO GARCIA, María del Carmen, "Investigación Parlamentaria sobre Regulación jurídica de Internet", publicado en: http://www.diputados.gob.mx /cedia/sia/spe/SPE-ISS-12-06.pdf, mayo de 2006.

TRIGO ARANDA, Vicente; "Historia y evolución de Internet", publicado en página web de Autores Científico-Técnicos y Académicos (ACTA), http://www.acta.es

TRONCOSO ÁLVAREZ, Elizabeth, RIESTRA HERRERA, Eduardo y GARCÍA DEL VALLE MÉN-DEZ, Alejandro, "Web 2.0. Regulación legal: Acciones de marketing y redes sociales", publicado en: http://www.riestra-abogados.com, 2009.

UICICH, Rodolfo D., "El derecho a la intimidad en Internet y en las comunicaciones electrónicas", Editoral Ad Hoc, Buenos Aires, 2009.

VANINETTI, Hugo A., "Derecho a la intimidad e Internet", publicado en: http://www.abeledoperrot.com.ar, Enero de 2005.

VIBES, Federico Pablo, "¿Qué ley gobierna Internet?", publicado en: http://www.abeledoperrot.com.ar, Junio de 2005.

VIEGENER, Federico, "El derecho a la Intimidad y los límites a la injerencia estatal", Alfa-Redi: Revista de Derecho Informático No. 116, Marzo del 2008, publicado en: http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954 b7a344761/viegener.pdf

- PÁGINAS WEB:

– http://europa.eu/legislation_summaries/ index_es.htm
– http://www.abeledoperrot.com.ar
– http://www.acta.es
– http://www.alfa-redi.org
– http://www.eff.org
– http://www.hfernandezdelpech.com.ar
– http://inadi.gob.ar
– http://www.infoleg.gov.ar
– http://www.internetworldstats.com
– http://www.itu.int
– http://www.laleyonline.com.ar
– http://www.mit.edu
– http://www.protecciondedatos.com.ar
– http://www.rsf-es.org
– http://www.spamlaws.com
– http://www.jus.gov.ar/datos-personales

Formulario descriptivo del Trabajo Final de Graduación

Identificación del Autor

Apellido y nombre del autor:	**Dorado, John Grover**
E-mail:	**johnidorado@hotmail.com**
Título de grado que obtiene:	**Abogado**

Identificación del Trabajo Final de Graduación

Título del TFG en español	**El derecho a la intimidad en Internet**
Título del TFG en inglés	**The right to privacy on the Internet**
Integrantes de la CAE	**Eduardo Flores – Cristina González Unzueta**
Fecha de último coloquio con la CAE	**15/11/2010**
Versión digital del TFG: contenido y tipo de archivo en el que fue guardado	**El derecho a la intimidad en Internet.pdf**

Autorización de publicación en formato electrónico

Autorizo por la presente, a la Biblioteca de la Universidad Empresarial Siglo 21 a publicar la versión electrónica de mi tesis (marcar con una cruz lo que corresponda).

☐ **Publicación electrónica: Inmediata** ☐ **Después de..... mes(es)**

Firma del alumno