

# 3<sup>ra</sup>. Jornada de Seguridad Informática

Colegio de Ingenieros Especialistas

23 Noviembre 2007

Paraná – Entre Ríos - Argentina

---

- **Introducción.**
- **Habeas Data:**
  - Nuestra Ley Nº 25.326 de Protección de datos personales.
  - Alcances y derechos que protege.
  - Usuarios y responsables de archivos, registros y bancos de datos.
  - Control. Sanciones.
  - Acciones judiciales disponibles.
- **Marketing y Cookies. SPAM.**
- **Normas Internacionales relacionadas**

A modo de introducción y con el afán de introducir al auditorio en un vocabulario que compatibilice la técnica informática y la ciencia jurídica vamos a tratar de esbozar unos conceptos básicos que nos resultarán necesarios para comprender el significado y alcances de la ley de protección de datos personales de nuestro orden jurídico. Y ya vamos con la primera frase y algunas palabras sueltas:

1. **'Orden jurídico':** como se indica en su nombre es un sistema de normas que rige las conductas de sus habitantes.
2. **'Norma o ley':** es un precepto racional orientado al bien común y promulgado por quien cuida de la sociedad.
3. **'Constitución Nacional':** es la norma fundamental y de donde surgen todas las demás.
4. **'Legislador':** es el congreso en pleno al dictar la norma o ley. También puede ser el legislador constituyente al reformar la CN.
5. **'Ilícito':** contrario a derecho.
6. **'Derecho Constitucional':** es el conjunto de derechos garantizados por nuestra CN. Ej.: libertad, vida, trabajar, asociarse, entrar y salir, enseñar y aprender, propiedad, etc.
7. **'Amparo':** Es el recurso o remedio judicial disponible de manera expedita para aquellos derechos constitucionales vulnerados, lesionados o atacados por agentes públicos o privados. Ej. Habeas corpus, amparo por violación al derecho de propiedad, de trabajo, etc.
8. **'Derecho Civil':** regula la actividad del hombre en sociedad y en sus relaciones de familia. Reparación.
9. **'Derecho Penal':** es un instrumento de regulación social. Tipos Penales. Delitos. Pena.
10. **'Bien Jurídico':** es todo interés vital para el desarrollo pleno del hombre.

Para concluir con este compendio de vocablos y frases jurídicas aplicables al desarrollo de esta ponencia sobre la ley 25.326 debo decir que la problemática de la regulación de las actividades de Internet no es cosa sencilla. Puesto que no existe una compatibilidad natural entre la norma y el software. La norma es una expresión de deseo de un legislador que promueve la orientación de conductas o comportamientos que favorecen al bien común; que por ende se adapta a un tiempo y lugar o sociedad de personas determinados. En cambio el software es todo lo contrario, es atemporal, no tiene espacio determinado y resulta complejo ligarlo a una conducta dentro de un espacio social y geográfico. A continuación se va a explicar determinados textos que se han esbozado sobre el tema según la referencia al final de esta exposición.

## **Habeas Data. Protección de Datos Personales.**

Con esta ley se persigue garantizar a las personas el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

## **La nueva Ley exige cambios en la Política de Privacidad de los sitios de Internet.**

Hasta tanto no fuera promulgada la Ley de Protección de los Datos Personales en el mes de noviembre del año 2000, los sitios webs argentinos no se encontraban obligados a tratar en forma adecuada los datos personales de sus usuarios. La generalizada costumbre de incluir a pie de página una mención a la "Política de Privacidad" con un enlace a un página que detallaba sus lineamientos era totalmente voluntaria y sus promesas normalmente incumplidas. Además, en la mayoría de los casos, su contenido copiaba textualmente modelos extraídos de sitios extranjeros con mención de normas ajenas a nuestro sistema jurídico y por ende, de difícil exigibilidad. Con la sanción de la Ley 25.326 (vetada parcialmente por el Decreto 995) comienza una nueva etapa para los emprendimientos que basan buena parte de su negocio en la interacción con los usuarios y el manejo de datos personales. Ya no basta con publicar la política relativa a la protección de los datos personales de los usuarios. Ahora hay que cumplirla de acuerdo a lo que exige la nueva Ley. (\*)

## Qué se protege

La 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, 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. Como se ve, el derecho que se trata de proteger no es sólo el de la intimidad, sino algo con mayor profundidad que en el derecho anglosajón se denomina "privacy" y que se ha castellanizado como "privacidad". Lo que se busca es proteger aspectos de la personalidad que individualmente no tienen mayor trascendencia pero que, al unirse con otros, pueden configurar un perfil determinado de las personas. Ante dicha posibilidad surge el derecho de sus titulares a exigir que los datos permanezcan en el ámbito de su privacidad.

Evidentemente, que los archivos, registros o bancos de datos privados que no tengan como finalidad brindar informes no hayan sido incluidos en los artículos 1 de la Ley y 43 de la Constitución, no significa que estén exentos de respetar los principios de finalidad, pertinencia, utilización no abusiva, exactitud, legalidad, publicidad, seguridad, control, consentimiento y defensa de los datos sensibles.

En efecto, existen numerosos archivos, registros o bancos privados que no tienen como finalidad suministrar informes a terceros, pero que recolectan información personal que puede resultar discriminatoria en perjuicio de sus titulares. Basta mencionar, a modo de ejemplo, a los que mantienen las empresas con los datos de sus empleados; a los que administran las empresas aseguradoras con relación a sus asegurados; y a las historias clínicas confeccionadas por los establecimientos de salud, entre muchos otros.

Y no puede admitirse que los derechos de las personas sean vulnerados por el sólo hecho de estar sus datos personales registrados en un archivo, registro o banco de datos que no está destinado a dar informes.

Es por eso que, siguiendo esta línea de pensamiento, el deber de registro que exige el artículo 24 tiene como fin evitar que existan archivos, registros o bancos de datos que incumplan los principios básicos de la protección de datos mencionados en el párrafo anterior, estén destinados a proveer informes o no.

Sin perjuicio de lo expuesto, de aceptarse la interpretación efectuada, cabe destacar que aún cuando las bases de datos no destinadas a brindar informes deban inscribirse en el Registro que al efecto se habilite, ello no implicará que sus titulares deban permitir el ejercicio de los derechos reconocidos por la ley a los ciudadanos, ya que dichos derechos sólo podrán ejercerse contra las categorías de bases de datos especificadas en el artículo 1.

Un ejemplo de dicho límite lo constituye el inciso 1 del artículo 14 que establece que 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.

De acuerdo a esta norma, los responsables de archivos, registros o bancos de datos que no provean datos a terceros, no estarán obligados a proporcionar información a los titulares de los datos personales registrados en sus archivos, ni en la forma ni dentro de los plazos establecidos por los artículos 15 y 14 inciso 2. (\*)

## Qué datos pueden recabarse

Salvo que medien razones de interés general autorizadas por Ley, ninguna persona puede ser obligada a proporcionar datos personales que revelen su [origen racial y étnico](#), [sus opiniones políticas](#), [sus convicciones religiosas, filosóficas o morales](#), [su afiliación sindical](#) e [información referente a su salud o vida sexual](#). Es más, la formación de archivos, bancos o registros que almacenen datos que revelen ese tipo de información - denominada sensible- queda prohibida. La Ley establece que 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. Además, no pueden ser utilizados para fines distintos o incompatibles con los que motivaron su obtención. Cuando no sean exactos, deben actualizarse, suprimirse o sustituirse y si han dejado de ser necesarios o pertinentes a los fines para los cuales fueron recolectados, deben ser [destruidos](#). En cuanto a los datos relativos a la salud, los datos de los pacientes sólo pueden ser recolectados por los establecimientos sanitarios y los profesionales médicos responsables de su tratamiento, siempre y cuando se respeten los principios del secreto profesional. (\*)

## Consentimiento

Como norma general, pueden tratarse datos personales de los usuarios cuando hubieren prestado, por escrito o medio equiparable, su consentimiento libre, expreso e informado. No será necesario el consentimiento cuando los datos se obtengan de fuentes de acceso público irrestricto (como las guías telefónicas), se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal, se deriven de una relación contractual, científica o profesional con el titular de los datos y resulten necesarios para su desarrollo o cumplimiento, o se trate de listados cuyos datos se limiten a registrar el nombre, DNI, CUIT o CUIL, ocupación, fecha de nacimiento y domicilio. Lo que no está del todo claro es si puede entenderse que un usuario, luego de leer la ya famosa "Política de Privacidad", presta su consentimiento por el sólo hecho de pulsar el botón de aceptación que al efecto se coloque en el Web site, o si será necesario que además de la aceptación virtual

envíe por otro medio un documento de aceptación que contenga su firma manuscrita. El acto de pulsar el botón para consentir o aceptar algo en la web se ha convertido en una costumbre entre los internautas. Es por ello que debería aceptarse la validez de esa forma de prestar el consentimiento y establecerse niveles más rigurosos de aceptación para casos en los que estén en juego las clases de datos personales especialmente protegidos por la ley. (4)

## **Formularios**

Más allá de lo que pueda decir el apartado dedicado a la Política de Privacidad, cada vez que un usuario deba completar un formulario en el que se le soliciten datos referidos a su persona, además de obtener su consentimiento se le debe informar claramente cuál es la finalidad para la que serán tratados; quiénes pueden ser sus destinatarios; la existencia del archivo, registro o banco de datos; la identidad y domicilio de su responsable; el carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga; las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos o la posibilidad de conocer, modificar o incluso cancelar los registros referentes a su persona en forma gratuita. (4)

## **Bancos de Datos.**

Evidentemente, que los archivos, registros o bancos de datos privados que no tengan como finalidad brindar informes no hayan sido incluidos en los artículos 1 de la Ley y 43 de la Constitución, no significa que estén exentos de respetar los principios de finalidad, pertinencia, utilización no abusiva, exactitud, legalidad, publicidad, seguridad, control, consentimiento y defensa de los datos sensibles.

En efecto, existen numerosos archivos, registros o bancos privados que no tienen como finalidad suministrar informes a terceros, pero que recolectan información personal que puede resultar discriminatoria en perjuicio de sus titulares. Basta mencionar, a modo de ejemplo, a los que mantienen las empresas con los datos de sus empleados; a los que administran las empresas aseguradoras con relación a sus asegurados; y a las historias clínicas confeccionadas por los establecimientos de salud, entre muchos otros.

Y no puede admitirse que los derechos de las personas sean vulnerados por el sólo hecho de estar sus datos personales registrados en un archivo, registro o banco de datos que no está destinado a dar informes.

Es por eso que, siguiendo esta línea de pensamiento, el deber de registro que exige el artículo 24 tiene como fin evitar que existan archivos, registros o bancos de datos que incumplan los principios básicos de la protección de datos mencionados en el párrafo anterior, estén destinados a proveer informes o no.

Sin perjuicio de lo expuesto, de aceptarse la interpretación efectuada, cabe destacar que aún cuando las bases de datos no destinadas a brindar informes deban inscribirse en el Registro que al efecto se habilite, ello no implicará que sus titulares deban permitir el ejercicio de los derechos reconocidos por la ley a los ciudadanos, ya que dichos derechos sólo podrán ejercerse contra las categorías de bases de datos especificadas en el artículo 1.

Un ejemplo de dicho límite lo constituye el inciso 1 del artículo 14 que establece que 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.

De acuerdo a esta norma, los responsables de archivos, registros o bancos de datos que no provean datos a terceros, no estarán obligados a proporcionar información a los titulares de los datos personales registrados en sus archivos, ni en la forma ni dentro de los plazos establecidos por los artículos 15 y 14 inciso 2. (4)

## **SPAM – El correo basura es uno de los principales problemas de los proveedores y usuarios de Internet.**

*"Este mensaje se envía con la complacencia de la nueva legislación sobre correo electrónico: Por sección 301, párrafo (a) (2) (C) de S.1618. Bajo el decreto S.1618 título 3ro. aprobado por el 105 Congreso, base de las normativas internacionales sobre SPAM, este E-mail no podrá ser considerado SPAM mientras incluya una forma de ser removido".*

Si nunca leyó esta frase al pie de un e-mail recibido de un desconocido, sonría: UD. es un afortunado que todavía no dedica parte de su tiempo y dinero a eliminar mensajes no deseados. (4)

## **¿De qué se trata?**

El spam es la técnica de envío indiscriminado de e-mails a miles de usuarios que no pidieron recibirlos e integra el grupo de los llamados "Abusos en el Correo Electrónico" pues su práctica trasciende los objetivos habituales del servicio y perjudica a proveedores y usuarios. El origen del término es impreciso. Una versión lo relaciona con una canción de una película de Monty Python que repetía sin sentido e incesantemente esa palabra. Otra sostiene que su nombre se inspiró en un tipo de carne de color rosado que se comercializa enlatada en Estados

Unidos y que para muchos es sinónimo de comida chatarra. Más allá del origen exacto del vocablo, lo cierto es que fue en Usenet donde se empezó a llamar así a los mensajes enviados un número inaceptable de veces a uno o más newsgroups. Si bien la práctica habitual consiste en el envío de correo comercial y publicitario, no son pocos los casos en que se lo utiliza con el fin de paralizar el servicio por saturación de las líneas, del espacio en disco o de la capacidad de procesamiento de un servidor. En la mayoría de los casos el spammer - así se denomina a quienes practican esta actividad- es desconocido y la dirección de correo que aparece en el remitente es falsa, lo que impide identificar una dirección de retorno correcta para responder el mensaje.

Enviar infinitos mensajes de correo electrónico es tarea fácil para un spammer. Basta tener una cuenta de correo electrónico y una base de datos con direcciones electrónicas. Aunque los spammers se excusan diciendo que el usuario puede defenderse borrando los mensajes recibidos o solicitando que su dirección se excluya de la lista de destinatarios, el problema es mucho mayor. Según la Comisión de Mercado Interno de la Unión Europea el costo del spam a nivel mundial alcanza varios billones anuales. Cada mensaje enviado por un spammer es transportado por varios sistemas hasta que llega al lugar de destino, generando costos a lo largo de la cadena. El bolsillo de los usuarios es quien paga los pulsos de su cuenta telefónica por el tiempo que ocupan en descargar estos mensajes, además de los recursos de espacio de almacenamiento y tiempo para su lectura y eliminación. Por su parte, los proveedores de servicio consumen ancho de banda para procesarlos y, por ende, la velocidad y calidad de sus servicios disminuye. Finalmente, los costos se transfieren al usuario final, repercutiendo negativamente en la satisfacción de los clientes y en los ingresos económicos de las empresas. (4)

### **Prohibido el SPAM**

El Spam ha sido condenado desde los albores de Internet, especialmente por la Netiquette y las RFCs 2505 y 2635, pero también por las asociaciones que nuclean a los proveedores de servicios de Internet y por diversos pronunciamientos judiciales extrajeros. Esta postura ha sido la adoptada por los redactores del proyecto de Ley sobre "Régimen de Propiedad Intelectual de las Obras de Informática y Regimen Penal" presentado a mediados del año 2000 por el Senador Bauzá, que pretende sancionar con una multa de 1.000 a 10.000 pesos a quienes saturen o carguen indebidamente de mensajes las casillas de correo electrónico o sitios informáticos de un receptor que no hubiera solicitado la publicidad recibida.

No obstante, son pocas las voces que se alzan a favor de la prohibición total. Varios de los proyectos existentes sobre la materia, sobre todo los elaborados en la Unión Europea, consideran apropiado el sistema de opt-out que permite a los usuarios solicitar que sus datos sean excluidos de las bases de datos utilizadas por los spammers. Ese es el criterio que, en concordancia con la Ley 25.326 de Protección de los Datos Personales, sostiene el Anteproyecto de Ley sobre Formato Digital de los Actos Jurídicos y Comercio Electrónico preparado por la Jefatura de Gabinete, que establece que las comunicaciones comerciales no solicitadas deben ser claramente identificadas como tales e incluir una opción automática de exclusión voluntaria de la lista de destinatarios. Lamentablemente este remedio sólo funcionaría localmente, ya que no podría imponerse el sistema a quienes envíen mensajes spam desde otro país.

Resulta claro entonces que los métodos mencionados no impiden que las víctimas del spam puedan evitar totalmente la invasión a su privacidad. Por ello, valiéndose de la técnica del "marketing permission", las organizaciones protectoras de los usuarios y consumidores prefieren el sistema opt-in, según el cual quien pretenda enviar mensajes comerciales deberá contar con la autorización expresa del destinatario.

Más allá de estas propuestas, aún no existe legislación nacional ni internacional que trate el spam. Estados Unidos es el país que más interés ha demostrado en combatirlo, siendo varios los juicios que enfrentaron a gigantes de la industria de Internet como América Online, Prodigy o CompuServe contra empresas dedicadas a realizar campañas publicitarias a través del correo electrónico. Sin embargo, más allá de algunas leyes estatales - como las de Washington, Illinois o Massachusetts -, hasta el momento ningún proyecto con alcance federal ha sido aprobado. Ni siquiera el ya famoso y nunca sancionado Decreto S.1618 del 105 Congreso, que no fue más que un proyecto de enmienda para el Acta de Telecomunicaciones presentado en el año 1998, pero que quedó en el olvido. Sin embargo son varios los proyectos que siguen en pie, entre ellos el H.R. 3113 que pretende que los mensajes comerciales sean identificados como tales e incluyan instrucciones para que quienes los reciban puedan excluirse de la lista de destinatarios, el S.2542 que exige que los spammers proporcionen información correcta que permita localizarlos e identificarlos y prohíbe la distribución de software que permita falsificar la información del emisor, y el H.R. 2162 que faculta a los proveedores de servicio de Internet a demandar a los spammers que no cumplan con las condiciones del servicio contratado con sanciones que oscilan entre 50 y 25.000 dólares. (5)

### **¿Hay solución?**

El mundo sin fronteras creado por Internet impide que intentos de soluciones locales puedan aplicarse a problemas globales. Por el momento la Netiquette y las condiciones de uso de los servicios de correo electrónico surgen como las mejores alternativas para intentar controlar el spam. Los programas utilizados para filtrar automáticamente dichos mensajes disminuyen los problemas, pero no son totalmente eficientes. Los proveedores de servicios de Internet deben adoptar políticas de "tolerancia cero" respecto a los mensajes spam que envíen sus clientes y exigir el cumplimiento de las condiciones de contratación del servicio. [Debe alentarse la aprobación de códigos de conducta que obliguen a las partes involucradas en el negocio a comportarse éticamente. También es recomendable que se prohíba el desarrollo de software que permita enviar mensajes engañosos](#), que se impida que los remailers anónimos sean utilizados con fines publicitarios y que se concientice a las empresas que enviar e-mails no consentidos perjudica su imagen comercial. (6)

## **Acciones disponibles**

Con el fin de tutelar los derechos de los titulares de los datos de carácter personal, la ley establece dos tipos de acciones. Una, mencionada en el artículo 31 inciso 1, permite reclamar los daños y perjuicios que pudieran haberse ocasionado a raíz de la inobservancia de la ley. La otra, más específica, es la denominada "Acción de protección de los datos personales". Regulada en el Capítulo VII (36), tiene como fin tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de su finalidad; y exigir la rectificación, supresión, confidencialidad o actualización de la información cuyo registro se encuentre prohibido o se presuma que sea falsa, inexacta o desactualizada.

Finalmente, se pone de manifiesto que la ley, a través de su artículo 32, define nuevos tipos delictivos y supuestos de responsabilidad penal para la eventualidad de su incumplimiento, cuyo texto incorpora como artículos 117 bis (37) y 157 bis (38) del Código Penal. (4)

## **Normas Internacionales relacionadas:**

La posición legal donde la protección de datos se acomoda no es una menor. Siguiendo un esquema se podría afirmar que:

América ha creado un "proceso constitucional" propio. Un sistema autónomo para Brasil o bien uno derivado como modalidad del amparo en la Argentina);

Europa tiene derechos y deberes a partir de las leyes de tratamiento de datos personales y

Estados Unidos una acción especial que difiere muy poco de las pretensiones destinadas a la defensa de la intimidad.

---

## **Textos de Consulta:**

1. *Constitución Nacional Argentina.*
  2. *Código Penal Argentino.*
  3. *Ley 25.326 de Protección de Datos Personales.*
  4. *Gustavo Daniel Tanús. Artículo publicado en Information Technology, revista editada por Mind Opener S.A. Buenos Aires, Argentina. (4)*
  5. *Diario Judicial. Nota sobre SPAM 18/08/2005 y otros - www.diariojudicial.com.*
  6. *SpamHaus - www.spamhaus.org.*
- 

**Oscar Londero**