



UNIVERSIDAD DE BELGRANO

Las tesinas de Belgrano

**Facultad de Derecho y Ciencias Sociales
Carrera de Abogacía**

**En la búsqueda de una legislación idónea en
materia de Spam**

Nº 112

Andrea Jordán Camus

Tutor: Carlos Acquistapace

Departamento de Investigación

Abril 2004

Indice

Capítulo I	5
1. Objeto de éste trabajo	5
2. Concepto de Spam. Obtención de datos	6
3. Problemas provocados por el spam	6
4. Estadística. El Spam en números	7
5. El Decreto S. 1618	8
6. Necesidad de legislar el Spamming. Bien jurídico tutelado	8
Capítulo II	9
7. Legislación	9
7.1. Constitución Nacional	9
7.2. Habeas Data	10
7.3. Tratados	12
7.4. Código Civil	13
7.5. Código Penal	13
Capítulo III	13
8. Proyectos de Ley con tratamiento en el Congreso de la Nación Argentina	13
8.1. Proyecto de ley de la Cámara de Diputados. Exp. 325-D-2002. Régimen de protección del correo electrónico de los senadores Fontdevila y Ubaldini ¹	13
8.2. Régimen de delitos informáticos. Exp. 1815-D-2002. Penalización de delitos informáticos ²	14
Capítulo IV	15
9. Legislación Extranjera	15
9.1. Comunidad Europea	15
9.1.1. España	15
9.1.2. Inglaterra	16
9.2. Chile	17
9.3. México	17
9.4. Ecuador	18
9.5. Venezuela	18
9.6. Estados Unidos	19
9.7. Australia	20
9.8. Japón	20
10. Conclusión	21
Capítulo V	22
11. Jurisprudencia	22
11.1. Argentina	22
11.2. Brasil	23
11.3. España	24
11.4. Estados Unidos	25
11.5. Japón	27
12. Glosario	28
13. Bibliografía	33
14. Información Web	34
15. Documentación complementaria	38

Capítulo I

1. Objeto de este trabajo

El mundo actual está rodeado de informática, personas dependientes de las nuevas tecnologías quizás sin darse cuenta. Todos son parte de esta sociedad de la información, producto de la Era digital y de la Era Tecnológica, impactando día a día provocando grandes cambios en los negocios y en la industria, y en la vida cotidiana en general.

Sin la informática la vida habitual podría volverse caótica. Gracias a Internet la comunicación con todo el mundo es sin fronteras.

La red se ha transformado en el medio por excelencia de los tiempos que vienen. Internet constituye sin lugar a dudas un elemento basal de la sociedad en que nos toca desarrollarnos. Es la herramienta fundamental que nos permitirá ingresar en la Era del Conocimiento, en la Nueva Sociedad de la Información.³

El derecho, como orden regulador de conductas, no queda exento del impacto de las nuevas tecnologías, el daño causado no es indemnizado, y ciertas conductas quedan impunes ya que no encuadran dentro de los tipos penalizados en la legislación. Una de esas conductas impunes se ve día a día, cuando las personas ven invadidas sus casillas de correo, consecuencia de ello, vulnerada la privacidad, violada la intimidad a costa de la sociedad, todo ello por el Spam o correo electrónico no deseado. Toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito de sus datos personales, tiene derecho a obtener del responsable del tratamiento la reparación del daño sufrido.⁴

Las nuevas tecnologías de la información han modificado la forma en que la gente se comunica, siendo realmente trascendente el fenómeno alcanzado en tal aspecto por la utilización del correo electrónico. Efectivamente, la utilización de esta nueva forma de comunicación entre las personas ha beneficiado enormemente a las organizaciones, facilitando la comunicación interna entre sus miembros y también con el exterior. De hecho, la implementación del correo electrónico en la empresa ha provocado grandes cambios en la forma de trabajar. No sólo se ha convertido en una nueva y muy importante herramienta de trabajo sino que, además su correcta utilización permite que las empresas puedan reducir costos, implementar nuevas formas de trabajo y lograr una más eficiente y productiva actividad laboral. Como contrapartida, el envío y recepción masiva de mensajes de correo electrónico publicitarios no solicitados. Pero no sólo el spam es materia de conflicto. El uso del correo electrónico en el ámbito laboral, puede suscitar conflictos entre el derecho a la intimidad del trabajador con respecto al contenido de los mensajes por él enviados y el derecho del empresario a ejercer el debido control sobre los bienes de la empresa y controlar que los recursos que pone a disposición del empleado se utilicen única y exclusivamente para desempeñar más eficientemente su labor.⁵

La realidad exige de manera urgente una promulgación de normas jurídicas dirigidas a proteger la utilización abusiva de la información, reunida y procesada mediante el uso de ordenadores, como así también un órgano de control especializado que proteja los derechos de los ciudadanos amenazados por el uso indebido de las computadoras y aplique sanciones pecuniarias en concepto de resarcimiento por los daños que ocasionen a los usuarios.

Como consecuencia de la Revolución Tecnológica, surgen una nueva clase de delitos, los llamados delitos informáticos que obliga a tipificarlos, clasificarlos e incorporarlos en la legislación tanto nacional como internacional para no ver vulnerados uno de los derechos más preciados de la humanidad.

Mediante este trabajo mi intención es investigar sobre como penalizar esta conducta susceptible de reproche tanto civil como penal, conocida como spamming, aplicable a todas aquellas personas que utilizan indebidamente la información privada de todos los ciudadanos, bombardeando periódicamente con mensajes de e-mail que nunca fueron pedidos, simples propagandas; cadenas de mensajes de la suerte; informaciones sobre peligrosísimos virus; o avisos que en nada interesan, usando los recursos de sus víctimas y de los servidores de Internet.

1. <http://www.hfernandezdelpech.com.ar/Leyes/Anteproyecto%20ley%20Proteccion%20Correo%20Elect.htm>

2. <http://www.hfernandezdelpech.com.ar/Leyes/Proyecto%20ley%20delitos%20informaticos%20con%20media%20sancion.htm>

3. Resumen de ideas para considerar el desarrollo de INTERNET en la Argentina, Secretaría de Comunicaciones de la Presidencia de la Nación (SECOM) para el día 6 de agosto de 1997, Guillermo Bort, Impsat.

4. Artículo 23 DIRECTIVA 95/46/CE http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=ES&numdoc=31995L0046&model=quichett

5. <http://www.geocities.com/SiliconValley/Circuit/4888/principal.htm>

2. Concepto de Spam. Obtención de datos

El SPAM es el envío masivo de mensajes a través de correo electrónico. Se atribuye el origen de la palabra «spam» a la canción ⁶de la comedia británica Monty Python donde los vikingos comen un menú que sólo incluye spam (en inglés, carne de cerdo enlatada). Se escucha de forma repetida y con volumen creciente “spam spam spam...” hasta ahogar toda conversación. La metáfora reside en el hecho de que los vikingos deben tragar el spam, quieran o no, ya que no se les ofrece otra alternativa. Los mensajes spam funcionan de la misma manera: se reciben le guste o no al destinatario.⁷

El spam viene sin anunciarse y sin ser solicitado por medio del correo electrónico (*email*), satura los registros de correo, destruye servidores de correspondencia y demora la entrega de *e-mail* por horas. Aumenta también los costos de usuarios y de proveedores de servicios de Internet. Es el correo electrónico basura, y se lo llama *Spam*, un nuevo término cibernético para un evento considerado como la próxima gran amenaza del Internet y el *e-mail*. Oficialmente como *e-mail* comercial no solicitado, el *spam* es el equivalente de la correspondencia indeseada *junk mail* que suele llegar por medio del correo regular.⁸ También es denominado como Spamming, correo basura, UCE (unsolicited commercial email). Todas estas expresiones se refieren al envío de muchas copias de un mismo mensaje, a través de Internet, a personas desconocidas, que no han solicitado recibirlo. SPAM es cualquier mensaje, destinado a una audiencia en general que se envía a la gente por e-mail sin que lo soliciten.⁹

Hoy en día es una práctica muy utilizada por empresas que comienzan en Internet, páginas de pornografía, usuarios sin escrúpulos que intentan promocionar su página web o engañabobos vendiendo productos milagrosos.

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. 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.¹⁰

El spam se difunde mediante la siguiente manera: el remitente, llamado spammer, armado de listas masivas de direcciones de correo y de software especial, envía muchas copias de un mismo mensaje a multitud de usuarios desconocidos. Estos mensajes sirven, generalmente, para hacer publicidad de productos, eventos, una página web, un servicio o una idea.¹¹

Los Spammers obtienen los emails de sus víctimas de diversas maneras:

- **Compra de direcciones:** existen muchas empresas dedicadas a la venta de bases de datos que contienen infinidad de emails recopilados de diversas formas.
- **Suscripciones a listas de distribución falsas:** Este método aparentemente legal, pero por sus consecuencias ilegales, consiste en suscribirse a una lista de algo que nos interesa, pero en realidad estamos cayendo en una trampa para recibir publicidad sin parar.
- **Robots que escanean las paginas web:** los datos se obtienen con un software que previa configuración de pagina webs, filtran las paginas y recolectan todos los emails que existan, obteniendo una infinidad de emails.
- **Robots que escanean los grupos de noticias:** De manera similar a la anterior, el software recolecta direcciones de correo electrónico, pero esta vez las consigue de los grupos de noticias.

3. Problemas provocados por el spam

La invasión de spams causa grandes molestias, una de las principales es la necesidad de leer algo que no interesa en absoluto por miedo a perder comunicaciones importantes.

Este tipo de publicidad tiene algo en particular, ya que si la comparamos con la publicidad por correo tradicional, los costos son totalmente al revés. Si, en el caso del correo tradicional el costo es asumido por el remitente, en cambio en el spam el costo es asumido por el destinatario. El spam invierte la relación costo beneficio. El anunciante ahorra enviando spams, ya que si lo hiciera por correo postal el costo sería muy elevado.

6. Net-abuse-faq

<http://www.saulo.net/pub/articulo.php?cod=spam>

7. <http://www.rompecadenas.com.ar/porquespam.htm>

8. <http://www.antispam-argentina.8m.net/>

9. <http://www.antispam-argentina.8m.net/paginas/info.htm#Definiciones>

<http://www.x-extrainternet.com/news1.html>

10. <http://www.geocities.com/SiliconValley/Circuit/4888/principal.htm>

11. <http://www.sinectis.com.ar/seguridad/spam.html#spam>

También trae aparejado la pérdida de tiempo de la víctima del spam, como así también la capacidad de almacenamiento en el buzón del usuario y en el del servidor de dicho usuario. El spammer utiliza recursos del servidor de su víctima, como así también de la propia víctima, para transmitir su publicidad. También los cargos van para el servidor, porque los Proveedores de Servicio de Internet (ISP) deben soportar el costo de los spams dirigidos a su dominio, por el uso del servidor, uso de los canales de comunicación, horas adicionales del personal, reparación de los equipos en caso de sufrir algún daño, productividad y oportunidades de negocio perdidas. Dicho costo muchas veces se vé reflejado en las facturas de las víctimas, en el incremento del abono. Se le debe sumar a la lista de perjuicios de la víctima el tiempo de conexión a Internet en el caso de acceder por vía telefónica para poder bajar este correo basura de su servidor.

Según la opinión de Vinton Cerf, Chairman de la Internet Society y Miembro del Directorio de ICANN (Internet Corporation for Assigned Names and Numbers); considerado uno de los padres de Internet «El spamming es la maldición del correo electrónico y los newsgroups en Internet. Puede interferir seriamente con los servicios públicos, además del efecto que puede tener sobre el sistema de email de un individuo. Los spammers, en efecto, están robándoles recursos a los usuarios y a los proveedores de servicio sin compensación ni autorización.¹²

No obstante, son pocas las voces que se alzan a favor de la prohibición total. Varios de los proyectos existentes sobre la materia, 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. 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.¹³

4. Estadística. El Spam en números

Según la consultora IDC, en 2002 se enviaron 31.000 millones de mensajes en todo el mundo y se espera que ese número crezca a 61.000 millones en 2006, de los cuales algo menos de la mitad será spam.¹⁴

América Online (AOL), proveedor de servicios a Internet (ISP) más grande del mundo, anunció hace un mes que actualmente bloquea 780 millones de mensajes spam por día.¹⁵

Yahoo!¹⁶ por ejemplo, ofrece una opción para marcar un mensaje como spam y compartir esa evaluación con el resto de los usuarios de ese servicio de correo. Si un número suficiente de usuarios marca determinado mail o remitente como spam, será filtrado por los servidores de correo del ISP, antes de llegar a su casilla. Diversos ISP locales (gratis y comerciales) ofrecen un servicio similar.

Hotmail¹⁷ hace algo parecido, y además anunció que no dejará que sus usuarios envíen mensajes de correo a más de cien destinatarios cada 24 horas, en un intento por evitar que sea usado como fuente de correo indeseado.

El volumen de correo no solicitado se ha disparado en los últimos años, saturando las bandejas de entrada de los usuarios y está costando millones de dólares en ancho de banda malgastado.

Los proveedores de acceso a Internet y compañías rastreadoras estiman que representa entre el 40 y el 80 por ciento de todos los emails.¹⁸

Para Ryan Hamlin, estratega de Microsoft encargado de diseñar sistemas contra el spam, pronosticó que dentro de dos años será posible bloquear totalmente el spam. La situación empeorará considerablemente antes de mejorar, el flujo de correo masivo no solicitado aumentará a niveles críticos durante el año 2003, aumentando del 50% actual al 65%. El experto pronosticó que los costos de combatir el spam aumentarán de 9 a 18 mil millones de dólares entre 2002 y 2003.¹⁹

12. <http://www.isoc.org.ar/prensa/spamming.html> »Spamming, una práctica que afecta a la comunidad de Internet», por Edmundo Valenti, Presidente ISOC. AR, Capítulo Argentino de la Internet Society. Agosto de 2000.

13. <http://www.protecciondedatos.com.ar/doc3.htm>

14. Como defenderse del Spam, La Nación, Mi PC

15. <http://www.sinectis.com.ar/seguridad/spam.html#spam>

16. <http://www.yahoo.com.ar>

17. <http://www.hotmail.com>

18. <http://ar.news.yahoo.com/030611/10/6miz.html> REUTERS ESP MJG/ Miércoles 11 de junio, 4:21 PM. Gobierno EEUU reclama más poder a Congreso para eliminar «spam».

19. Nota del Diario Tecnologías de la Información Año 7- edición 1411. Microsoft: 'El spam acabará en os años más. (04/06/2003 08:36). <http://diarioti.com/gate/n.php?id=3147>

5. El Decreto S. 1618

Muchos correos comerciales no deseados contienen un párrafo que según ellos los exoneraría de toda responsabilidad. El mismo dice así: "Este email no podrá ser considerado spam mientras incluya una forma de ser removido. Texto según decreto 1618".

Según un artículo del diario La Nación, éste decreto fué creado por los Spammers para justificar sus prácticas. El decreto nombrado integraba parte del proyecto de los senadores norteamericanos Murkowski y Torricelli que nunca fué sancionado y no tenía que ver con el spam. Así fué hasta hace un par de años, cuando se supo que era otro embuste de los spammers.²⁰

Otros especialistas en la lucha contra el Spam, si bien coinciden en la falsedad del artículo, dicen que en realidad es una enmienda a la Ley de Comunicaciones de Estados Unidos. Esta enmienda no tendría aplicación fuera del territorio norteamericano. Pero además, en el caso de considerar dicha enmienda, el mensaje seguiría siendo un spam, aún existiendo una forma de ser removido de la base de datos, dado que el remitente cambia intencionalmente la información para confundir al destinatario, tratando de darle legalidad a su practica totalmente ilegal. Tampoco incluye su nombre, dirección física, dirección electrónica, como lo prescribe dicha norma.²¹

6. Necesidad de legislar el Spamming. Bien jurídico tutelado

Es notorio el desarrollo de los servicios telemáticos en la sociedad Argentina, así como también en todo el mundo. El impacto de las nuevas tecnologías en la vida cotidiana de todos los ciudadanos genera la necesidad de proteger cada vez más la intimidad y privacidad frente a una innumerable cantidad de violaciones a dichos derechos que se producen por la falta de una protección clara y precisa.

Existen dos tipos de violaciones de la privacidad en Internet:

- El primero de ellos es la recolección de datos personales con fines comerciales, el objetivo es la creación de bases de datos con perfiles del potencial consumidor y las direcciones de correo para el envío de publicidad (spam), o el desarrollo de políticas editoriales y de marketing de los sitios web. Los principales dilemas éticos están en la validez de la recolección de datos, debido a que es realizada sin el consentimiento de los usuarios, y su venta a terceros.
- El segundo tipo de trasgresión de la privacidad en la red, es la vigilancia de los usuarios por parte de organismos o empleadores, que consiste en un monitoreo del tráfico por la web y la intercepción del correo electrónico.

En las comunicaciones establecidas por medio del correo electrónico se intercambia información personal, comercial o laboral, similar a la intercambiada por medio de la correspondencia epistolar, pero con características especiales en cuanto a la posibilidad de ser interferidas y manipuladas. El acceso a las nuevas tecnologías de las comunicaciones por un número cada vez mayor de ciudadanos y de entidades en Argentina, obliga a establecer un régimen específico para garantizar sus derechos.

Siempre han existido datos (aunque no en la cantidad y calidad que ahora) y también la posibilidad teórica de reunirlos. Pero la informática ha permitido el salto potencial de acceder casi de inmediato a todos esos datos, clasificados y ordenados. Permite también formular programas de interpretación de tales datos. A partir de allí la vida del hombre queda expuesta.

La utilización ilimitada de medios digitales multiplica obviamente la información almacenada y las bases de datos, generando así una nueva masa de información personal expuesta al público. Cuando las bases de datos eran pocas o cuando se generaban deliberadamente, era más fácil controlarlas, pero ahora todo se multiplica y las bases se podrían generar en forma automática. La red agrega elementos que hacen perder la privacidad, bajos índices de seguridad, que pueden tener gran incidencia en la vida de las personas quedando mas expuesta que antes por el hecho de que tales registros y actividades podrán ser revisados por muchos.

La utilización de Internet en general, y del email en particular, tiene particular relevancia en el mundo científico, académico, gubernamental y empresarial. Así como anteriormente las herramientas de trabajo eran, entre otras, la máquina de escribir, de calcular, el teléfono, fax, etc., hoy es común, y por otra parte deseable, que las empresas y entes gubernamentales se abran al mundo a través de Internet, y pongan a disposición de sus colaboradores cuentas de correo electrónico, nueva herramienta, para el desarrollo de tareas laborales.

La pérdida de privacidad en Internet se produce en distintos niveles debido a la variedad de formas que entregan los medios digitales para recolección y procesamiento de los datos personales. En ella intervienen gobiernos, empresas, empleadores, proveedores de Internet y sitios web.

20. <http://www.rompecadenas.com.ar/leyspam.htm> Artículo publicado en el diario La Nación. La ley que no existe, por Eduardo Dahl, 13- 11- 2000.

21. <http://www.antispam-argentina.8m.net/>

El problema puede ser enfocado desde dos puntos de vista:

- El primero desde una perspectiva del sitio web que elabora perfiles para permitir entregar un servicio personalizado.
- El segundo, desde el punto de vista del usuario, que ve vulneradas sus libertades al desconocer el destino de dichos perfiles.

Cualquier sitio web puede recolectar información personal a través de cookies, sin que el usuario se entere. Las cookies son enviadas cada vez que un usuario entra a una página, los navegadores más conocidos como Microsoft Explorer o Netscape están configurados por defecto para aceptar todas las cookies de manera automática. Por ello la mayoría de los usuarios desconocen la existencia de ellas y sus consecuencias.

Por medio de las cookies se puede conocer el comportamiento del usuario, ya que puede ser observado por el proveedor acumulando información personal sobre gustos, preferencias, comportamiento del mismo sin tener su consentimiento. Dichos perfiles pueden ser enajenados sin su consentimiento dado que no ha sido advertido de la captación de su perfil.²² Las cookies no solo identifican las páginas que visitó el navegante, sino también permiten saber cuanto tiempo estuvo en cada una de ellas y cual es el sistema operativo que ocupa. También permiten individualizar el navegador, el monitor, y tipo de ordenador, rastreando y averiguando el IP, que vendría a ser un certificado de residencia en Internet.²³

Existe una necesidad de garantizar la confidencialidad e integridad de la información de las personas y de las empresas; como así también un deber de respetar la intimidad y la inviolabilidad del correo, sea electrónico o epistolar.

Los proveedores de servicios que difundan información de sus usuarios en la red deben ser sancionados, ya que los mismos deben cumplir requisitos mínimos para garantizar la protección de los datos obtenidos.

El bien jurídico tutelado en los delitos informáticos es la información en todos sus aspectos (propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos), entendiéndose que su ataque supone una agresión a todo el complejo de relaciones socio económicas culturales, por ende a las actividades que se producen en el curso de la interacción humana en todos sus ámbitos, y que dependen de los sistemas informáticos.

Para ingresar en nuestra PC y conocer nuestros archivos se necesita una orden judicial, ya que la misma constituye un espacio privado. Los spammers no tienen derecho a introducirse en nuestra privacidad. Nadie entra y por ley nadie puede entrar en nuestro hogar sin nuestro permiso; e incluso así, no debería ultrajar nuestros derechos personalísimos.

El spammer ignora esos derechos, simplemente porque la dirección de mail de los usuarios es pública. Es público el email pero no la PC de los mismos. Los Spammers roban el tiempo de los usuarios, ya que los mismos deben revisar y borrar el correo no solicitado, provocándoles un perjuicio y como consecuencia de ello debe existir el resarcimiento de ese daño causado.

Capítulo II - 7. Legislación

7.1. Constitución Nacional

La Constitución Argentina con la reforma de 1994, incorporó en el artículo 43, el habeas data, que dice: "Toda persona podrá interponer esta acción 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 de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística».

El artículo 43 de la Constitución Nacional significa un cambio fundamental en el tratamiento del tradicional proceso de amparo. Ha dejado de ser una figura procesal para constituirse en un «derecho» o «garantía» específica, cuya principal concreción es instalar el derecho al amparo.

El derecho a la intimidad puede entrar en conflictos con otros derechos:

- Tal es el caso cuando se confronta con el «derecho a la información», derecho a obtener datos de individuos o de entidades en numerosas situaciones y con legítimos motivos, tanto de interés público (la información requerida por diferentes organismos del Estado para poder cumplir satisfactoriamente

22. Según la normativa de privacidad de Yahoo!, las cookies sirven para recordar quien es el navegador y obtener acceso a la información de su cuenta (almacenada en sus equipos), para ofrecer un servicio mejor y más personalizado.

23. Fernández, María Luisa, 1998, Nuevas tecnologías, Internet y derechos fundamentales, Editorial McGraw Hill, Madrid, España, página 143

sus cometidos, y que con frecuencia se transforma en él deber de informarse), como de interés particular (gestionar créditos por compras o préstamos, concretar designaciones o ascensos, o para arrendar bienes, etc.)

- El de intimidad implica resistirse al suministro de datos personales cuando parecen abusivos los requerimientos en tal sentido, y el de información pretende lograrlos so pena de llegar a la parálisis de ciertas actividades.
- El tercer derecho en conflicto podría ser el derecho de propiedad sobre los datos obtenidos.

Cada derecho tiene establecida su área de protección, la reglamentación indicada en el art. 14 de la Constitución Nacional el ámbito propio de cada derecho y los límites que habrán de respetarse al ejercerlo.

El derecho a la información asume un papel de atacante contra al atacado derecho a la intimidad, será éste el que deba contar con mayor protección. El derecho a la intimidad en sí mismo no constituye una amenaza, mientras que el derecho a la información asume una postura activa y potencialmente agresiva frente al primero. Mayor eficacia debe asignarse a la protección del derecho a la intimidad por la vía de caminos judiciales, como lo es - tanto entre nosotros como en otros muchos países - la generalmente denominada acción de hábeas data, establecida por la reforma constitucional de 1994 como una modalidad del amparo (art.43 de la Constitución Nacional), ya adoptada por varias provincias de este país y antes establecida, constitucional o legalmente, en otros Estados.

La Constitución Nacional en su artículo 18 asegura el secreto de la correspondencia y de los papeles privados de cada uno, porque ambos atributos constituyen la esfera inviolable de la vida privada, que da mayor sentido a la libertad personal. En el mismo sentido la correspondencia tiene amparo en la Declaración Universal de Derechos Humanos y la Convención Americana de Derechos Humanos.

La protección constitucional a la "correspondencia epistolar" (art. 18) ha sido ratificada con toda amplitud por la Corte Suprema de Justicia de la Nación en el caso "Dessy, Gustavo Gastón s/ corpus corpus" con motivo de restricciones impuestas al demandante por aplicación del Reglamento dictado por el Servicio Penitenciario Federal sobre correspondencia remitidas por los internos.

Particularmente, el voto de la mayoría integrada por los Ministros Fayt, Petracchi y Boggiano recordó que "el Tribunal ha considerado a la inviolabilidad del domicilio y de la correspondencia en términos sustancialmente entrañables, calificándolos como un derecho «básico» o «fundamental» de la persona humana.²⁴

En otras palabras, no debe analizarse si los derechos y garantías Constitucionales se adecuan a las nuevas tecnologías de la información, sino - por el contrario - verificar si éstas, en su instrumentación, son respetuosas de los derechos de los ciudadanos.

No se advierten motivos para que –aún sin existencia de legislación específica- el denominado "correo electrónico" escape a dicha protección, tanto más si así fue admitido jurisprudencialmente en el ámbito del derecho penal, donde la analogía está prohibida (CNCrim. y Correc., Sala VI, marzo 4-999, "Lanata, Jorge").²⁵

Los derechos, garantías, obligaciones y responsabilidades en la red, aún 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.²⁶

7.2. Habeas Data

El habeas data significa, que cada persona tiene sus datos. El objeto tutelado es la intimidad o privacidad de la persona. Todos los datos a ella referidos que no tienen como destino la publicidad, o la información a terceros, necesitan preservarse.²⁷

El bien jurídico protegido es la información, ya que es un bien intangible que ha sido elevado a la categoría de bien jurídico porque ha pasado a ser un interés jurídicamente protegido, que interesa a toda la sociedad.

24. Fallos: 308:1392, págs. 1428 y 1475. Asimismo: Declaración Universal de Derechos Humanos, art. 12; Pacto Internacional de Derechos Civiles y Políticos, art. 17; Declaración Americana de los Derechos del Hombre, art. X; Convención Americana sobre Derechos Humanos, art. 11.2

25. La Ley, 1999-C-458, con nota de Marcelo Alfredo Riquert

26. Vibes, ob. cit., p. 1018 cfr. Federico Carlos Vibes, "Internet y Privacidad. La difusión en Internet de imágenes lesivas de la intimidad, el honor y otros derechos personalísimos, La Ley, 2000-D, p. 1013

Correo Electrónico Poder Judicial de la Nación Juzgado Comercial N° 18 – Secretaría 36 "G., D.E.c/ C. SA. s/diligencia preliminar" - Expte. 39749

Causa Nro. 33.628 "Vita, Leonardo G. Y González Eggers, Matías s/procesamiento" Juzgado 10 - Secretaría 20

Expte. 8515/98 - «Gornstein Marcelo Hernán y otros s/delito de acción pública» - JUZGADO NACIONAL EN LO CRIMINAL Y CORRECCIONAL FEDERAL N° 12 – SECRETARIA N° 24

27. Manual de la Constitución Reformada, Tomo II, Pág. 388. German J. Bidart Campos

En nuestro país, a partir de 1994, se incorporó en el art. 43 de la Carta Magna el instituto del habeas data, el cual establece que las personas tienen derecho a tomar conocimiento de sus datos y a solicitar, en caso que proceda, la rectificación y/o actualización de los mismos», por lo que toda persona tiene derecho a proteger sus datos.

Seguidamente se promulgó la ley 25.326,²⁸ que garantiza el derecho al honor y a la intimidad de las personas, de conformidad con el art. 43 de la Constitución Nacional.

En su artículo 1, la ley especifica su objeto diciendo:

“ 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 ”.

En el artículo 2,²⁹ la ley se ocupa de definir, entre otros, el concepto de datos personales como toda información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

En lo concerniente a la licitud de los archivos de datos, el artículo 3 dice que 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. De más está decir que: “Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública”.

Con respecto al consentimiento del titular de los datos, el artículo 5 dice que 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. Dicho consentimiento no será requerido cuando los datos se obtengan de fuentes de acceso público irrestricto; se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; o cuando 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.

Así mismo se requiere que el titular de los datos personales sea informado previamente a la recopilación de datos, en forma expresa y clara. El artículo 6 se refiere al deber de información exigiendo al recopilador de datos que haga conocer al titular de la finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; 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; 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; las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; como así también la posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.

La ley también regula el deber que tienen los responsables y las personas que intervengan en el tratamiento de datos personales. En el artículo 10 se refiere al deber de confidencialidad que tienen el responsa-

28. Publicada en el boletín oficial del 02-11-2000. Ley de protección de los datos personales

29. Art. 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.

ble y las personas que intervengan en cualquier fase del tratamiento de datos personales. Los mismos están obligados al secreto profesional respecto de los datos manejados. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos. Solo quedaran eximidos de dicho deber por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

La ley permite la cesión de datos personales, previo consentimiento del titular de los datos, solo cuando los fines se relacionen directamente con el interés legítimo del cedente y del cesionario.³⁰

Según las opiniones del Dr. Bidart Campos y del Dr. Gozáni, el habeas data, tutela en relación con los servicios informáticos, computarizados o no, y con toda clase de utilización, aunque no sea automatizada, si el soporte material de los datos es susceptible de tratamiento automatizado.³¹

En contra de dicha postura, encontramos la del Dr. Padilla que dice: la protección de Habeas Data resulta de fundamental importancia para proteger el derecho de intimidad, pero el gran desafío del desarrollo de las tecnologías impone al derecho una legislación específica al respecto. Con el Habeas Data y la ley 25.326 no queda amparado el derecho a la privacidad en la Red.³² El habeas data se limita solamente a la información de datos personales, en cambio la legislación sobre delitos informáticos³³ tiene mas bienes jurídicos a proteger.

7.3. Tratados

El Habeas Data se encuentra respaldado por tratados internacionales. Art. 75 inc. 22. La reforma constitucional, en su artículo 75, inciso 22, introdujo un elemento nuevo bajo la forma de sus definiciones de derechos, equiparando varios pactos y tratados sobre derechos humanos a las disposiciones constitucionales, siempre que no sean contrarias a ella. Este inciso es un respaldo constitucional a reglamentaciones destinadas a cubrir todos los aspectos del derecho a la intimidad.

Tales tratados son:

➤ **La Declaración Universal de Derechos Humanos de 1948:** reconoce el derecho a la vida privada y rechaza la intromisión en la vida familiar, domicilio o su correspondencia.

Artículo 1.- Todos los seres humanos nacen libres e iguales en dignidad y derechos, y dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros.

Artículo 12.- Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o en correspondencia, ni de ataque a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

En Internet se han alcanzado niveles casi insospechados en la pérdida de la privacidad.

➤ **La Declaración Americana de los Derechos y Deberes del Hombre. (abril de 1948):**

Artículo 5.- Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar.

➤ **El Pacto Internacional de Derechos Civiles y Políticos, Art. 17. (1966):**

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.

➤ **La Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica, 1969):**

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.

30. Art. 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.

31. Manual de la Constitución Reformada, Tomo II, Pág. 388. German J. Bidart Campos

32. La Revolución Digital y la Privacidad, Dr. Miguel Padilla

33. Los delitos informáticos son aquellas acciones típicas, antijurídicas y culpables que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, en cualquiera de las fases que tienen vinculación con su flujo o tratamiento contenida en sistemas informáticos de cualquier índole sobre los que operan las maniobras dolosas. La información, como valor a proteger, ha sido tenida en consideración por el derecho penal desde la óptica de la confidencialidad.³³

7.4. Código Civil

El artículo 1071 bis del Código Civil sanciona comportamientos representativos sobre todo de violaciones a formas hogareñas de la intimidad, mediante el siguiente texto:

«El que arbitrariamente se entrometiere en la vida ajena, publicando retratos, difundiendo correspondencia, mortificando a otros en sus costumbres y 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...»³⁴

Para la aplicación del art. 1071 bis del Código Civil, debe existir entrometimiento arbitrario en la vida ajena, y que, de acuerdo con las circunstancias de personas, tiempo y lugar, la interferencia perturbe la intimidad personal y familiar del perjudicado. El margen de apreciación judicial de tales circunstancias es muy extenso, debiéndose tener en cuenta, en especial, la personalidad del afectado, el ámbito en que se desenvuelve, la naturaleza de la intrusión, la finalidad perseguida, el medio empleado y la incidencia futura que pueda tener sobre la vida familiar, entre otros factores y parámetros.³⁵

7.5. Código Penal

El Código Penal sanciona los agravios al derecho a la intimidad, en el área de los cometidos por la prensa, los delitos de calumnias e injurias³⁶, aunque muchas informaciones de los medios no encuadran siempre en esas figuras y quedan, así, sin sanción.

Capítulo III - 8. Proyectos de Ley con tratamiento en el Congreso de la Nación Argentina.

Existen dos proyectos de ley con trámite parlamentario a la fecha, ellos son:

- El Proyecto de Ley de Protección del Correo Electrónico de los senadores Fontdevila y Ubaldini. 325-D.-2002
- El Proyecto de Ley de Delitos Informáticos. Exp.- Dip.- 64/02 / Exp. 1815-D-2002.

8.1. Proyecto de ley de la Cámara de Diputados. Exp. 325-D-2002. Régimen de protección del correo electrónico de los senadores Fontdevila y Ubaldini.³⁷

El proyecto de Ley sobre Régimen de Protección del Correo electrónico, creado por los Diputados Fontdevila y Ubaldini, ha sido considerado por las Comisiones de Comunicaciones e Informática (SECOM) y de Legislación del Trabajo. Dichas Comisiones el 4 de julio de 2002, aconsejaron su sanción con modificaciones en la orden del día n° 576. El proyecto obtuvo media sanción de Diputados el día 31 de Julio de 2002 y en este momento se encuentra pendiente de tratamiento en el Senado de la Nación.

El proyecto de Fontdevila y Ubaldini, utilizando criterios diferentes pero tutelando el mismo bien jurídico, tuvo como antecedente el trabajo realizado en el año 2001 por la Comisión de Estudio de Correo Electrónico, constituida en el ámbito de la Secretaria de Comunicaciones de la Nación.

Se conceptualiza el correo electrónico, como toda transmisión de información enviada a través de una red de interconexión entre dispositivos electrónicos con capacidad de procesamiento, a una dirección o casilla de correo electrónico.

Confiere al email el mismo estatus de privacidad que al correo postal. El citado proyecto lo equipara con la correspondencia epistolar abarcando su creación, transmisión y almacenamiento. (Art. 2) El email quedaría protegido por la Constitución Nacional.

En el ámbito laboral, la casilla de correo electrónico provista por el empleador es de uso exclusivo del trabajador, alcanzándole a esa casilla la confidencialidad que establece el Art.2.³⁸

Se obliga al empleador a notificar en forma fehaciente al trabajador respecto de su política sobre el acceso y uso del email en el lugar de trabajo. (art. 4)

El art. 5 fué introducido por las Comisiones de Comunicaciones e Informática y de Legislación del Trabajo, el mismo no se encontraba en el texto original del proyecto de Fontdevila y Ubaldini. El mismo sustituye los arts. 153, 154 y 155 del Código Penal, contemplando penas de prisión para quien abra, se

34. texto según art. 1071 bis Código Civil

35. SZEWC, Andrés c/ CARREFOUR ARGENTINA S.A. s/ COBRO DE SUMAS DE DINERO (Sentencia Definitiva - CNCIV - Sala E - Nro. de Recurso: E225405 - Fecha: 9-10-1997 - Vocal Preopinante: MIRAS.)

36. Capítulo 6, Título II Delitos contra el honor Código Penal

37. <http://www.cnc.gov.ar/>

38. Art. 3, texto modificado, el proyecto originario decía: se entenderá que el empleador ha cedido al trabajador el uso exclusivo del email, debiendo respetar la confidencialidad establecida en el art. 2

apodere, suprimiere o desviare de su destino una carta o pliego cerrado que no le esté dirigido. Agravándole la pena en el caso de que el mismo divulgue el email, o sea empleado de correos o telégrafos y también en el caso de que el hecho pudiere o causare perjuicios a terceros.

8.2. Régimen de delitos informáticos. Exp. 1815-D-2002. Penalización de delitos informáticos³⁹

Las Comisiones de Legislación Penal y de Comunicaciones e Informática, el día 11 de julio de 2002, dictaminaron en la orden del día n° 639 aconsejar la sanción del proyecto de delitos informáticos, basándose en el Anteproyecto de Ley de Delitos Informáticos sometido a Consulta Pública por la Secretaria de Comunicaciones (476/2001), considerando los Proyectos de Ley de los diputados: Di Leo y otros (2772-D-2001), Fontdevila y otros (1299-D-2002) y Ferrari de Grand y Chaya sobre Régimen de Delitos Informáticos; y teniendo en vista los Proyectos de Ley de los diputados Cardesa y otros (0299-D-2001), Cafiero (0385-D-2001), Godoy (1185-D-2001), Martínez (5061-D-2001), Corchuelo Blasco (7316-D-2001), Roggero y otros (2585-D-2002), Rubini (2629-D-2002), Herzovich y otros (2871-D-2002) y Molinari Romero (3335-D-2002)

El día 8 de agosto de 2002, la Cámara de Diputados aprobó dicho proyecto unificado pero con modificaciones. El mismo fué remitido al Senado de la Nación para su aprobación.

Por tratarse de un bien jurídico novedoso que puede presentar numerosas modificaciones en el futuro y fundamentalmente para no romper el equilibrio de la sistemática del código penal se lo regula mediante una ley específica.

El proyecto define numerosos conceptos informáticos y protege penalmente el bien jurídico tutelado de la información creando tres tipos de delitos básicos, con sus correspondientes agravantes.

Ellos son:

➤ **Acceso ilegítimo informático o intrusismo informático no autorizado (hacking):** supone vulnerar la confidencialidad de la información en sus aspectos de exclusividad e intimidad. (arts. 1 y 2)

Es la figura básica, por acceso se entiende todo ingreso no consentido, legítimo y a sabiendas a un sistema o dato informático. Su aplicación se restringe a los supuestos que no media intención fraudulenta ni voluntad de dañar. La acción se limita a acceder a un sistema o dato informático que se sabe privado o publico de acceso restringido y del cual no se posee autorización.

Como elemento subjetivo se requiere la intencionalidad de acceder a un sistema de carácter restringido, sin consentimiento expreso o presunto de su titular. Por ello están excluidos los accesos permitidos por el propietario u otro tenedor legítimo del sistema.

En él supuesto que el autor revelare, divulgare o comercializare la información se agrava la pena, ya que la víctima pierde la exclusividad de la información. La pena también se agrava si los sistemas vulnerados pertenecen al área pública, por ser los mismos, servicios vitales para la Nación.

➤ **El daño o sabotaje informático (cracking):** conducta dirigida esencialmente a menoscabar la integridad y disponibilidad de la información. (arts. 3 y 4)

Se incluye a los sistemas y datos informáticos como objeto de delito de daño.

Este artículo llena el vacío presentado por el tipo penal de daño que solo contempla las cosas muebles, penando así el daño sobre los datos o información almacenada en soporte magnético que se materializa en todo ataque, borrado, destrucción o alteración de dichos bienes intangibles.

Protege por ende a los usuarios de los ataques con virus informáticos, caballos de troya, gusanos, etc.

La pena se agrava si los sistemas dañados pertenecen al área pública, al ser de trascendencia pública los datos protegidos.

➤ **El fraude informático:** hipótesis en la cual se utiliza el medio informático como instrumento para atentar contra el patrimonio de un tercero, que se incluye en esta ley por su propia especificidad que impone no romper la sistemática de este proyecto de ley especial, y por la imposibilidad de incorporar a los delitos contra la propiedad contemplados en el código Penal. (arts.5 y 6)

En esta conducta se juntan dos elementos típicos, ausentes en los tipos tradicionales de fraudes previstos en el código penal, estos son el ánimo de lucro y el perjuicio patrimonial. El ánimo de lucro es el elemento subjetivo del tipo que distingue el fraude informático de las figuras de acceso ilegítimo informático y daño informático, en los casos en que la comisión de las conductas descriptas en estos tipos trae aparejado un perjuicio patrimonial. El otro elemento es el medio comisivo del delito de fraude informático consistente en la manipulación o despliegue de cualquier artificio tecnológico semejante sobre un sistema o dato informático. La conducta comprende tanto la acción de supresión, modificación, adulteración o ingreso de información falsa en un sistema o dato informático.

39. <http://infoleg.mecon.gov.ar/basehome/alfaredi.htm>

El fraude informático también se agrava si el hecho recae sobre alguna administración pública.

Todos estos delitos también se agravan si el actor se desempeña en cargos públicos, o tiene a su cargo el deber de custodia u operación del sistema, en razón de las responsabilidades y deberes que le incumben.

Capítulo IV - 9. Legislación Extranjera ⁴⁰

9.1. Comunidad Europea ⁴¹

La Comunidad Europea actualmente incorporó a su legislación comunitaria la Directiva 2002/58/CE del Parlamento Europeo y del Consejo Europeo, del 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.⁴² Ésta Directiva es aplicable a todos los estados miembros. ⁴³

El artículo 13 se refiere al tema de la siguiente manera:

“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 lo establecido en el artículo 6.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de Datos de Carácter Personal, esa misma persona física o jurídica podrá utilizar dicha dirección electrónica 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 en el momento en que se recogieron los datos y, en caso de que el cliente no haya rechazado inicialmente su utilización, cada vez que reciban un mensaje ulterior”.

La Directiva de la Unión Europea propone una regulación general de la prestación de servicios de la Sociedad de la Información, de las comunicaciones comerciales, la validación jurídica de la celebración de contratos por vía electrónica, la protección específica de los consumidores, la promoción del establecimiento de códigos de conducta y de la solución extrajudicial de litigios y de la celeridad en la vía judicial.

9.1.1. España⁴⁴

En España, la regulación del envío de publicidad por correo electrónico se rige por las siguientes normas. La LOPD (Ley Orgánica de Protección de Datos), la LSSI-CE (Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico, comúnmente llamada Ley de Comercio Electrónico o LSSI), y por último, la Directiva Comunitaria sobre la Privacidad y las Comunicaciones Electrónicas (Directiva 2002-58-CE) que entrará en vigor para España el 31 de octubre de 2003 (o antes si el Gobierno español aprueba la correspondiente norma interna basada en dicha Directiva).

El 12 de octubre del 2002 entró en vigencia la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)⁴⁵, la misma exige el consentimiento expreso del receptor como condición previa al envío del email publicitario. El artículo 21º se refiere al tema, de la siguiente manera:

«Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas».

Esta norma exige uno de estos dos requisitos:

- Que la publicidad hubiese sido previamente solicitada por el destinatario
- O expresamente autorizada por el mismo

41. Directiva 1999/93/CE del Parlamento Europeo y del Consejo de la Unión Europea estableciendo un marco comunitario para la firma electrónica_____Convention on Cybercrime - Budapest - 23.11.2001__

42. Directiva sobre la privacidad y las comunicaciones electrónicas, Diario Oficial nº L201 31/07/2002 p.0037-0047

43. <http://www.bufetalmeida.com>

La Directiva de la Unión Europea sobre Comercio Electrónico, elaborada en 1997 por la Comisión Europea y presentada a los organismos comunitarios competentes a través de una comunicación dirigida a promover un sistema europeo de comercio electrónico. Esta directiva se complementa con otra que establece la prohibición de transferencia de datos personales a países que no tengan un nivel adecuado de protección de la privacidad. Esta norma, ha desatado un debate diplomático y comercial con los Estados Unidos, recientemente superado.

44. **Nombres de Dominio** Orden 662/2003 del 18 de Marzo de 2003 que aprueba el Plan Nacional de Nombres de Dominio Internet bajo el Código de País correspondiente a España «es»_ Firma Electrónica Real Decreto 14/1999 - Firma Electrónica en España

Sociedad de la Información y Comercio Electrónico Ley 34 de Servicios de la Sociedad de la Información y Comercio Electrónico del 11.07.2002_

45. <http://www.setsi.mcyt.es/>

La LSSI prevé sanciones tales como la de abrir un expediente administrativo sancionador, que en caso de concluir con que el incumplidor ha infringido la ley, podrá acarrear una multa de hasta los 150.000 euros. Dicho procedimiento habrá de tener en cuenta determinados criterios a la hora de graduar la sanción. Es por ello que la Administración, a la hora de decidir qué sanción impone, habrá de barajar distintos aspectos en el declarado infractor, como son:

- Existencia o no de intencionalidad, y grado de la misma, en su caso...
- Durante cuanto tiempo se ha estado llevando a cabo la infracción.
- Apreciación o no de reincidencia en hechos del mismo tipo.
- En su caso, naturaleza y cuantía de los perjuicios ocasionados.
- Beneficios estimados o comprobados, por la comisión de la infracción.

La promulgación de la LSSI, causó grandes protestas, ya que contradice la directiva 2002/58/CE de la comunidad europea según áreas académicas, políticas y empresariales.

La contradicción legal española es la siguiente:

La LSSI es radical a la hora de regular el llamado spam, porque simple y llanamente, lo prohíbe. Pero, la Directiva 2002/58/CE, que España habrá de incorporar a sus leyes antes del 31 de octubre de 2003 -y si no lo hace antes, será de aplicación directa en el derecho nacional-, indica en su artículo 13 que cuando se obtenga la dirección de correo electrónico de un cliente, en el contexto de una contratación con el mismo de algún producto o servicio, podrá el prestador utilizar su dirección para la promoción de productos o servicios, o de otros similares, siempre y cuando se ofrezca al mismo, al obtener su dirección, de forma gratuita y sencilla, la posibilidad de oponerse a ello, y que si no manifiesta su oposición en ese momento inicial, lo podrá hacer cada vez que con posterioridad a ese momento reciba un nuevo correo con promociones.⁴⁶

En suma, la LSSI prevé cuantiosas multas, y la Directiva es más permisiva.

El Ministerio de Ciencia y Tecnología Español, como una manera de poner fin a tal discusión, optó por reformar el proyecto de ley general de telecomunicaciones, art. 38, enviado al congreso, en vez de modificar la LSSI. El citado artículo establece el derecho de los consumidores y usuarios finales a no recibir llamadas automáticas sin intervención humana, mensajes de fax, mensajes de correo electrónico o mensajes de datos o terminales fijos o móviles, con fines de venta directa sin haber prestado su consentimiento previo e informado para ello.

9.1.2. Inglaterra⁴⁷

Políticos y ejecutivos de la industria de Internet están ansiosos en la promulgación de nuevas leyes para bloquear el flujo de «spam», los mensajes no solicitados que inundan las casillas de los correos electrónicos y amenazan con desestabilizar las redes informáticas del mundo.⁴⁸

Los legisladores británicos están en el proceso de elaborar leyes que convertirían en delito la entrega de mensajes electrónicos no solicitados. Sin embargo, las autoridades advierten que sin la cooperación internacional, los «spammers» seguirán enviando mensajes electrónicos en masa.

Legisladores, defensores de los consumidores y ejecutivos de la industria de la Internet se reunieron, en la más reciente de una serie de muchas discusiones previstas para elaborar leyes internacionales para reducir el «spam». Los legisladores coinciden en la creencia de que las nuevas leyes deben actuar como un factor disuasivo para los «spammers», pero que no deben eliminar los legítimos mensajes de mercadeo por medio del correo electrónico.

El ministro de comercio electrónico de Gran Bretaña, Stephen Timms, dijo en la inauguración de una cumbre sobre el spam que «El spam no es sólo un problema europeo o del Reino Unido», ya que la mayor parte del spam proviene del exterior. Gran parte procede de Estados Unidos.

En la Conferencia sobre seguridad informática se concluyó que lo mejor es lograr acuerdos entre la Comunidad Económica Europea y Estados Unidos. Pero existen desacuerdos fundamentales sobre cómo esto se puede hacer cumplir. La mayor discrepancia existente es sobre si un comerciante debería obtener el permiso del usuario de una computadora de antemano. Por ejemplo, el reglamento de protección de información de la Unión Europea exige que todos los que envían mensajes electrónicos, ya sea si son comerciantes legítimos o «spammers», obtengan el consentimiento previo del usuario. Esto que es denominado ruta «opt-in» definiría las actividades de «spam» como muchos e-mails que llegan sin el permiso del usuario, que, según funcionarios de la UE es una restricción efectiva. Pero las actuales propuestas estadounidenses contienen un mecanismo «opt-out» más amigable con el anunciante. «La ley estadounidense va

46. La publicidad por correo electrónico por [Javier Hernández](#), abogado especialista en Derecho de Internet y de las Nuevas Tecnologías. 17/06/2003 [Opinión Virtual](#) <http://www.baquia.com/com/20030617/art00011.html>

47. [Electronic Communications Act 2000 Chapter c.7 The Electronic Signatures Regulations 2002-Nº 318](#)

48. [México. Viernes 4 de julio de 2003. Terra > Tecnología > Actualidad - Guerra contra Spam. Instan políticos a una guerra mundial contra el spam. 01/07/2003 Por: Bernhard Warner. Reuters.- Londres.](#)

a ser la clave», dijo Steve Linford, fundador de Spamhaus Project, un grupo no lucrativo con sede en Londres que rastrea e identifica a los mayores «spammers» del mundo. Los spammers están aplaudiendo la legislación opt-out. Legaliza el status quo», agregó.

Capital del spam del mundo. Linford llamó a Estados Unidos «la capital del spam en el mundo». Alrededor de 140 individuos, la mayoría de ellos radicados en Estados Unidos, son los responsables de casi el 90 por ciento del «spam» del mundo. Al señalar la reputación de Estados Unidos como el lugar de nacimiento del spam, las autoridades de Internet en todo el mundo han comenzado cuestionar si las leyes de Estados Unidos reducirán el flujo de correo no deseado que se origina dentro de sus fronteras. Mientras el debate sobre la efectividad de las versiones «opt-in» y «opt-out» crece, otros señalan que la ley existente hasta la fecha puede funcionar. «Las nuevas leyes no detendrán el spam. Actuarán como un factor disuasivo», dijo Enrique Salem, presidente ejecutivo de Brightmail, una firma de software para filtrar «spam» con sede en Estados Unidos. «Se requiera una solución técnica mundial», agregó.

9.2. Chile ⁴⁹

Chile posee legislación sobre delitos informáticos, Ley N° 19.223.⁵⁰ La misma castiga con penas de multa y prisión las siguientes conductas:

- El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento.
- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él.
- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.
- El que maliciosamente revele o difunda los datos contenidos en un sistema de información.

La Ley de Chile adopta los requisitos mínimos de forma establecidos por la CNUDMI, otorga amplia validez jurídica a los documentos electrónicos, adopta una definición amplia de firma digital y delega en la reglamentación la fijación de estándares técnicos y de certificación de las firmas electrónicas.

Chile posee una legislación sobre Protección de datos personales,⁵¹ pero hace falta una legislación específica en materia de correo electrónico comercial. En Octubre de 2002 la Cámara de Diputados presentó un proyecto que modificaría la citada ley 19628 sobre protección de datos de carácter personal, el motivo, introducir el concepto de uso indebido o abusivo de datos. Actualmente dicho proyecto se encuentra en la Comisión de Constitución, Legislación y Justicia. (Boletín n° 03095-07).⁵² Numerosos proyectos pasaron por la Cámara de Diputados de Chile, pero solo uno logró seguir con su tramitación.⁵³

El Congreso chileno, archivó una serie de proyectos que prohibían y castigaban el envío de emails no deseados⁵⁴. Ellos eran:

- Proyecto de Ley Sistema de regulación de Internet. (02395-19)
- Proyecto de Ley sobre Comunicaciones Electrónicas: Internet, Dominio, Web. (02512-07)
- Proyecto de Ley de Privacidad de los Datos recolectados a través de Internet. (03003-19)
- Proyecto de Ley sobre comercialización y publicidad por medio de redes de telecomunicaciones. (03094-19)
- Proyecto de Ley que modifica la Ley N° 19.628 de protección de datos de carácter personal. (03185-19)

En el estudio realizado por la Cámara de Comercio de Santiago de Chile se recoge que, cada año, este tipo de mensajes «causan perjuicios económicos al país por más de 36 millones de dólares, derivados de la pérdida de tiempo laboral asociada a la actividad de bajarlos, leerlos y borrarlos».⁵⁵

9.3. México ⁵⁶

Aunque existe un apartado dentro de la Ley Federal de Protección al Consumidor que protege al usuario en su información personal, no hay una ley en México encargada de velar por la intimidad y la privacidad de

49. Ley de Delitos Informáticos de Chile

Decreto de Firma Digital para la Administración del Estado de Chile

Ley 19799 sobre Firma Electrónica de Chile

50. <http://delitosinformaticos.com/legislacion/chile.shtml>

51. <http://www.bcn.cl/index2.html> Ley 19628 (Publicada El 28/8/99)

52. http://websinileg.congreso.cl/websinileg/tpro/rep_tramite_proyecto.asp?reporte=tramitacion_proyecto.rpt

53. <http://www.sofofa.cl/legislativa/senado.htm> <http://www.sofofa.cl/legislativa/diputado.htm>

http://websinileg.congreso.cl/websinileg/tpro/rep_detalle_boletin.asp?reporte=detalle_boletin.rpt&SINBOTONES=1

54. http://websinileg.congreso.cl/websinileg/tpro/tpro_procesa.asp

<http://websinileg.congreso.cl/websinileg/tpro/>

[tpro_procesa.asp?nro_paso=1&flag_comision=si&filtro_comision=1&corr_comision=00053](http://websinileg.congreso.cl/websinileg/tpro/tpro_procesa.asp?nro_paso=1&flag_comision=si&filtro_comision=1&corr_comision=00053)

55. <http://www.delitosinformaticos.com/noticias/%20archivo/arc7-2002.shtml>

las personas; sin embargo, se tienen propuestas en el Congreso de la Unión para crear una ley y evitar el comercio ilícito de bases de datos.

Otro delito del que los usuarios no tienen protección es el «spamming» o correo electrónico no deseado, a pesar de que en el artículo 76 bis de la Ley Federal de Protección al Consumidor se refiere a que el proveedor debe respetar la decisión del consumidor de no recibir avisos comerciales, indicó el presidente de la Academia Mexicana de Derecho Informático. «Cualquiera que lo lea lo interpreta como el spam, sin embargo, hay un grave error porque la ley habla de avisos comerciales, que están regulados por la Ley de Propiedad Industrial, y esta ley lo que nos dice como definición de aviso comercial es prácticamente un slogan». En conclusión, lo que protege es que no te manden slogans, no contra spam, porque no utilizaron la tecnología apropiada u otro término más adecuado.⁵⁷

En Mayo de 1999, México modificó el Código Penal Federal para incluir nuevos tipos de delitos informáticos, como accesos ilícitos a sistemas particulares, de gobierno y del sector financiero. En Mayo de 2000 se reformaron el Código de Comercio, Código Civil Federal, Código Federal de Procedimientos Civiles y Ley Federal de Protección al Consumidor en la parte de Comercio Electrónico.⁵⁸

9.4. Ecuador ⁵⁹

Éste país legisló todo lo referente a correo electrónico mediante la Ley de Comercio Electrónico, Firmas y Mensajes de Datos del Ecuador.⁶⁰ La ley sanciona el envío de Spams. Se requiere la aceptación del usuario para poder enviarle emails comerciales. El consumidor tiene la posibilidad de ser removido de las listas de manera inmediata ante su pedido.

9.5. Venezuela ⁶¹

En Octubre del 2001, el Congreso Venezolano aprobó la Ley Especial contra los Delitos Informáticos.⁶² La citada norma en su capítulo III se refiere a los delitos contra la privacidad de las personas y de las comunicaciones penando con multas y privación de la libertad ciertas conductas violatorias de la intimidad de las personas.

El artículo 20, referido a la violación de la privacidad de la data o información de carácter personal, dice lo siguiente:

- El que por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
- La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Con respecto a la violación de la privacidad de las comunicaciones, el artículo 21 sanciona de este modo:

- El que mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

En lo referente a la revelación indebida de data o información de carácter personal, el artículo 22 prescribe al respecto lo siguiente:

- El que revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
- Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

56. Código Penal Federal de Méjico - Delitos Informáticos

Código Penal Estado Sinaloa - Méjico - Art.217 - Delito Informático

57. James Graham, catedrático de la Facultad Libre de Derecho de Monterrey

58. NOTA: Con información de Joel Gómez, presidente de la Academia Mexicana de Derecho Informático.

<http://biblioteca.dgsca.unam.mx/boletines/msg00030.html> <http://www.senado.gob.mx/buscador.php>

59. Ley de Comercio Electrónico, Firmas y Mensajes de Datos de Ecuador

60. Ley No. 67. RO sup. 557 de 17 de Abril del 2002.

61. Ley sobre Mensajes de Datos y firma Electrónicas de Venezuela

Ley Especial sobre los Delitos Informáticos N° 48 de Venezuela

62. LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS N° 48 DE LA REPUBLICA DE VENEZUELA. Publicada el 30 de Octubre del 2001 en Gaceta Oficial N° 37.313.-

9.6. Estados Unidos⁶³

La Comisión de Comercio del Senado aprobó en Junio de 2003, un proyecto de ley contra el correo electrónico no solicitado, o «spam», también aprobó otorgar mayor autoridad a las fuerzas antifraude para que luchen contra este tipo de táctica comercial y prometió medidas más duras cuando llegue la hora de efectuar la votación decisiva.⁶⁴ Ambas propuestas fueron aprobadas con escaso debate, lo que indica el alto grado de consenso que se ha alcanzado en el Capitolio respecto a la necesidad de nuevas leyes para evitar la difusión en la red de pornografía, engaños para enriquecimiento rápido y curas milagrosas que acaban con la paciencia de internautas y hacen perder a los servidores miles de millones de dólares en ancho de banda desperdiciado.

El senador republicano por Arizona, John McCain, quien preside la comisión dijo: «Hay que hacer algo para proteger a los consumidores y empresarios estadounidenses contra el 'spam', y éste es un buen comienzo».

El proyecto de ley anti-spam obligará a los comerciantes de la red a poner direcciones de retorno en sus mensajes, describir siempre sus productos de forma honesta y atender las solicitudes de los consumidores que deseen ser tachados de las listas de envío. Los infractores podrán sufrir penas de hasta un año de cárcel y multas de hasta un millón de dólares.

El proyecto aprobado por la comisión del Senado fue propuesto por Conrad Burns, senador republicano por Montana, y Ron Wyden, demócrata por Oregon, y ha encontrado apoyo en grupos de mercadeo y los más importantes proveedores de servicios de Internet.

La comisión acordó penas más duras para varias técnicas de «spam», como el secuestro de cuentas de usuarios y «ataques diccionario», que consisten en enviar mensajes a millones de direcciones creadas al azar.

Wyden dijo que junto a Burns y miembros de la Comisión Jurídica trabajarán para redactar un borrador de responsabilidades penales mientras la ley se prepara para ser votada en el Senado. «La ley se hará más fuerte mientras seguimos avanzando», señaló.

Los senadores del grupo también otorgaron a la Comisión Federal del Comercio mayor autoridad para perseguir a los 'spammers', personas que envían correos no deseados, por medio de nuevas leyes de divulgación e instando a la cooperación con otros países para detectar a infractores que operan fuera de las fronteras de Estados Unidos.⁶⁵

En el mes de Abril de 2003, los senadores estadounidenses presentaron un proyecto de Ley Federal para reducir el correo basura que llega a través de Internet, que constituye un 40% del correo electrónico en el mundo. Los legisladores Conrad Burns, republicano de Montana, y Ron Wyden, demócrata de Oregon, señalaron que, por ley, quienes utilizan ese recurso deben proporcionar una dirección en sus mensajes.⁶⁶ Según el senador Wyden, ésta iniciativa ayudará al flujo del tráfico y el comercio electrónico legítimo, y acosará a individuos que utilizan el correo con propósitos turbios y molestos. El proyecto no establece que los consumidores puedan demandar judicialmente a los autores de los mensajes, pero deja esta tarea a las autoridades de la Comisión Federal de Comercio.

La comisión también podría multar a los infractores y las compañías que proporcionan los servicios de Internet podrían bloquear los mensajes molestos de sus redes.

Un proyecto similar fué aprobado el año pasado en el Comité de Comercio del Senado, pero no fué sometido a votación en pleno. Para el senador Burns el proyecto de ley ha sido demorado durante demasiado tiempo, y ha llegado el momento de avanzar

El portal Yahoo, anunció que respalda el proyecto, en tanto que América Online dijo que cooperará con el Senado para poner fin a la saturación del correo electrónico.

Varios proyectos de ley contra el spam se habían introducido en el Congreso y los legisladores de ambas Cámaras estimaban que probablemente aprobarían una de ellas a mediados del año 2003. El congreso de Estados Unidos tenía tres proyectos separados de ley contra el *spam*. De los tres proyectos, el de mayor alcance era el ofrecido por el representante Chris Smith, republicano de Nueva Jersey. Su proyecto simplemente extendería al *spam* la prohibición de *junk* faxes dispuesta en una ley de 1991. Otro proyecto, el del senador Frank Murkowski, republicano de Alaska, obligaría a los remitentes a poner la palabra «Publicidad» en sus mensajes, y requerirles adicionalmente que escriban de manera correcta sus direcciones, direccio-

63. Electronic Signatures in Global and National Commerce Act.
The Digital Millennium Copyright Act of 1998 ([The Library of Congress](#))
Ley del Estado de Utah sobre Firma Digital
Ley de Firma Digital del Estado de Nueva York
USA-PATRIOTIC Act of 2001 - 24.10.2001 (Legal Information Institute-Cornell Law School)

64. [Aprueban duras medidas anti-spam - Será dura lucha contra esta táctica comercial -19/06/2003 - Por: Andy Sullivan Terra > Tecnología > Actualidad-México. Viernes 4 de julio de 2003. Reuters.-Washington.-](#)

65. www.hispamp3.com/http://www.deltosinformaticos.com/protecciondatos/noticias/105637027918734.shtml

nes electrónicas y números telefónicos en los mensajes. Además, los proveedores de servicios solicitaran a sus clientes se desean que el *spam* sea bloqueado de sus direcciones electrónicas. El tercer proyecto, presentado por el senador Robert Torricelli, demócrata de New Jersey, obligara a los remitentes a borrar de sus listas de correspondencia la dirección del usuario que así lo solicite. Este proyecto es considerado en general como el más atractivo para los que realizan mercadeo en Internet..

Para contrarrestar la amenaza de la regulación del gobierno, un grupo de remitentes estableció un código voluntario de conducta. Este prohíbe a las empresas usar falsas direcciones de *e-mail* y hace cumplimiento obligatorio cualquier pedido de remoción de dirección hecha por un usuario. Como en el sistema de clasificación de las películas, ésta estrategia de mercado evita la cuestión de la censura.⁶⁷

En el mes de Junio la Comisión Federal de Comercio de Estados Unidos (FTC) adujo que necesita más poderes para librar la batalla contra el correo electrónico no solicitado, o «spam», que representa actualmente alrededor del 50 por ciento de todo el tráfico de email. En su comparecencia ante la Comisión de Energía y Comercio de la Cámara Baja estadounidense, miembros de la FTC solicitaron poderes para investigar en secreto a quienes envían este tipo de mensajes y más margen para perseguir a los sospechosos en el extranjero. Los miembros de la Comisión dijeron que quienes comercian a través del correo electrónico deberían describir siempre sus productos de forma honesta y atender a las peticiones de quienes soliciten ser retirados de sus listas de contactos. También deberían aplicarse sanciones penales a aquellos que falsifiquen sus direcciones de remitente.

Las propuestas darán herramientas de investigación y coacción más eficaces para seguir desarrollando la labor de la FTC. El volumen de correo no solicitado se ha disparado en los últimos años, saturando las bandejas de entrada de los usuarios y está costando millones de dólares en ancho de banda malgastado.⁶⁸

Aunque ya hay 27 de los 50 estados del país que tienen leyes antispam vigentes, los esfuerzos por aplicar una legislación en todo el país han chocado con la oposición de quienes defienden la libertad de expresión.

El estado de California (USA), en el mes de febrero de 2003, lanzó una cruzada contra la invasión de publicidad no deseada en Internet, con la presentación de una nueva propuesta contra el spam. Según la creadora de la propuesta, la senadora californiana Debra Bowen, no se trata sólo de que sea incómodo, sino que también consume tiempo y dinero de los usuarios al forzarlos a discernir entre millones de mensajes. Esta propuesta convertirá en delito el envío de mensajes publicitarios no deseados, tanto aquellos que se originen en California como los que se envíen a residentes de este estado. Será un delito que se penará con una multa de al menos 500 dólares por cada infracción. Bowen, que en 1998 escribió la primera ley californiana contra el correo basura, es consciente de que su nueva propuesta no pondrá fin al problema, ya que señaló que sería necesario una versión nacional de esta propuesta, en ocasiones discutida en el Congreso estadounidense pero nunca aprobada.⁶⁹

9.7. Australia⁷⁰

La nueva legislación Australiana promulgada en el 2002, prevé sentencias para los cibercriminales. Podrá aplicársele una pena de hasta 10 años de cárcel para toda persona que atenté contra la seguridad e integridad de los datos almacenados en una computadora o las comunicaciones electrónicas.⁷¹

9.8. Japón⁷²

Desde Julio del 2002, en Japón, existe una legislación sobre SPAM. Mediante la misma, se obliga a este tipo de correo electrónicos a ser calificados de anuncios no solicitados. Por ende no podrán ser enviados a ningún destinatario sin su previa aceptación.

66. http://wyden.senate.gov/media/2003/04112003_canspam.html__<http://www.elmundo.es/navegante/2003/04/11/esociedad/1050048044.html>

67. <http://www.x-trainet.com/news1.html> Christopher Hamilton - Economic Strategic Institute - Washington E.U.A. La idea de una legislación en particular sobre el spam pondría a Estados Unidos en la extraña posición de promover la libertad absoluta del flujo de información en Internet y de simultáneamente prohibir un tipo de libertad de expresión comercial.

68. <http://ar.news.yahoo.com/030611/10/6miz.html> REUTERS ESP MJG/ Miércoles 11 de junio, 4:21 PM. Gobierno EEUU reclama más poder a Congreso para eliminar «spam».

69. <http://www.elmundo.es/navegante/2003/02/19/esociedad/1045649390.html>

70. Electronic Transactions Act N° 162 - Ley 28

71. http://www.heraldsun.news.com.au/common/story_page/0,5478,5085309^2862,00.html

<http://www.ds-osac.org/edb/cyber/news/story.cfm?KEY=9008>

72. Ley Japonesa de Firma Digital

10. Conclusión

El mundo sin fronteras creado por Internet impide que intentos de soluciones locales puedan aplicarse a problemas globales. Todos los países deben sincronizar sus legislaciones en materia informática para proteger a todos los ciudadanos del mundo en forma igualitaria. Una legislación en el ámbito comunitario, que reúna a todo el Mercosur, a la Comunidad Económica Europea y a los demás Estados. Si todos los países se unen contra el spam la solución será más fácil.

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 in consentidos perjudica su imagen comercial.⁷³

La legislación buscada debe facilitar el desarrollo del comercio electrónico, sin menoscabar las garantías de los usuarios. La importancia de las nuevas tecnologías debe hacer que su introducción en la sociedad Argentina se lleve a cabo dinamizando el tejido empresarial y, al mismo tiempo, protegiendo suficientemente los derechos de los usuarios, estableciéndose, a tal efecto, las oportunas garantías.

Una legislación idónea en materia informática no puede ser elaborada por diputados y senadores solamente, sino que se debe pedir la colaboración de expertos en el área informática, tales como autoridades universitarias, empresarios, etc., para que sea una visión de conjunto y permita que las acciones que se tomen respecto de cada tema en particular sean coherentes y respondan a un objetivo común.

El objetivo de la Ley sobre Protección de Datos Personales, debe contribuir al correcto funcionamiento del mercado de Argentina garantizando la libre circulación de los servicios de la sociedad de la información entre los habitantes de Argentina y también de estos con el mundo entero, estableciendo garantías claras para permitir el desarrollo del comercio electrónico.

La legislación debe ser específica en la materia, dado el continuo crecimiento tecnológico. Debe incluir no sólo el correo electrónico no deseado por Internet, sino también los mensajes vía Wap, debido al gran crecimiento de la cantidad de usuarios que leen sus mails desde sus teléfonos celulares. No debe prohibir la publicidad por correo electrónico, pero sí regularla.

Para enviar correo electrónico publicitario se debería solicitar el consentimiento expreso del destinatario de los mensajes, salvo que el destinatario ya hubiera consentido anteriormente la recepción de comunicaciones comerciales por correo electrónico. La información contenida en el mensaje debe ser cierta, debiendo indicar claramente que la misma es publicidad, como así también debe tener una forma de desuscripción. Para ello, en el texto del mensaje debe haber una opción donde el destinatario pueda declinar dicha autorización de manera ágil y definitiva.

Otra posibilidad a tener en cuenta, sería la creación de un nuevo dominio genérico o de primer nivel⁷⁴ para el envío de este tipo de mensajes. De hecho, la habilitación por parte de la ICANN, de un dominio nuevo para tales emails, que podría ser “.PUB”, posibilitaría a los usuarios que no deseen seguir recibiendo SPAMS aplicar la restricción en su programa de correo electrónico para todos aquellos emails cuyas direcciones sean “.PUB”. Un ejemplo de ello: soyspammer@esteemiservidor.pub.ar

Con ésta opción, todos los usuarios que no deseen recibir emails publicitarios podrán bloquear directamente y de manera general a todos los remitentes terminados en “.pub”. Así quedarían amparados aquellos usuarios que deseen seguir recibiendo todo tipo de publicidad libremente. Si se optara por ésta vía, la persistencia en el envío de mensajes periódicos no deseados de cualquier tipo, se debería sancionar con

73. Gustavo Daniel Tanús. Artículo publicado en Information Technology, revista editada por Mind Opener S.A. Edición Nº 53 - Abril 2001, pág. 112. Buenos Aires, Argentina.

74. Hay dos tipos de dominios: dominios genéricos y dominios territoriales.

Los dominios genéricos (también denominados internacionales o globales) están organizados conceptualmente y son los dominios básicos en Internet. Cualquier empresa que realice negocios a través de Internet o que tenga intención de hacerlo debe registrarse en uno de estos dominios genéricos, dada la popularidad que han adquirido. Tienen tres letras, y son los dominios .com (inicialmente previsto para empresas comerciales), .org (inicialmente previsto para organizaciones) y .net (inicialmente previsto para empresas relacionadas con la Internet). El dominio más popular es .com, que en la actualidad cuenta ya con más de dos millones de dominios registrados. El organismo que lo gestiona se llama InterNIC.

Los dominios territoriales (también denominados geográficos o ISO3166) son los dominios mantenidos por cada país. Estos dominios territoriales son utilizados por las organizaciones y empresas que desean establecerse en Internet o que quieren proteger la identidad de su marca o su nombre comercial en un país concreto. Los dominios territoriales tienen dos letras; p. ej., .es para España, .ar para Argentina, .uk para el Reino Unido, .au para Australia, etc. Hay aproximadamente 230 dominios territoriales. El organismo que registra dominios territoriales en España se llama EsNIC.

multas, de manera gradual, según la cantidad de incumplimientos de acuerdo a lo regulado por la ley que así lo disponga.

Para ello debe estar protegido por un Ente especializado en la materia que haga cumplir la legislación informática. Ese Ente debe ser un Órgano Fiscalizador, creado a tal fin, integrado por ingenieros en informática y abogados. Para el cumplimiento de la ley, el órgano que se cree debe fomentar la elaboración y aplicación de códigos de conducta e impulsar la participación en los mismos de todas las asociaciones y organizaciones interesadas. Dichos códigos deben ser conocidos por todos los usuarios, por ello se debe crear una política educativa en los colegios, universidades, organismos, empresas y medios.

Las controversias suscitadas por esta ley no deben sobrecargar los tribunales, para ello, sería aconsejable que fueran resueltas por medios alternativos de resolución de conflictos. También sería conveniente la creación de un Tribunal Arbitral que ponga fin al conflicto de manera sencilla, cómoda y económica para las partes. Solo como última vía se debe recurrir a los tribunales judiciales.

Capítulo V - 11. Jurisprudencia

11.1. Argentina

Equiparación del email a la correspondencia postal. Violación de correspondencia.

En Argentina la Cámara de Apelaciones Criminal y Correccional de la Capital Federal equiparó el email a la correspondencia postal, encuadrando dicha conducta como violación de correspondencia o publicación indebida de correspondencia. Con motivo de la apelación interpuesta, la Cámara de Casación confirmó el fallo de la Cámara del crimen, reafirmando así la protección del correo electrónico, dotándolo de las mismas seguridades que el correo convencional. Los camaristas, Carlos González, Carlos Elbert y Luis Ameghino Escobar, consideraron oportunamente que «nada se opone para definir al medio de comunicación electrónico como un verdadero correo en versión actualizada y goza de la misma protección incluida en los arts. 153 y 155 del Código Penal, cuando aún no existía este tipo de avances tecnológicos». Dicha postura fué mantenida por Casación. Sólo falta que el juez convoque a una audiencia de partes, fracasada la conciliación, el caso deberá llegar a juicio oral y público.⁷⁵

«Las comunicaciones que se cursan por vía electrónica constituyen correspondencia epistolar cuya inviolabilidad se encuentra garantizada por la Constitución Nacional, por lo que no puede entenderse que la autorización con que contaba para abrirla y enterarse de su contenido suponía la atribución de disponer de ella o comunicarla a terceros, siendo únicamente el juez quien puede disponer su incautación» (CNPenal Económico, Sala A. 13/09/2002. «Steinhaus, Raquel y otros»).⁷⁶

Email laboral. Deber de Información sobre el del correo electrónico en el ámbito laboral. Pereyra, Leandro Ramiro c/ Servicios de Almacén Fiscal Zona Franca y Mandatos S.A. s/ Despido.⁷⁷

En el caso, la accionada no ha acreditado que haya dictado norma alguna -escrita o verbal- sobre el uso que debían hacer los empleados del correo electrónico de la misma, con el agravante de que procedió a despedir a Pereyra directamente, sin hacerle ninguna advertencia previa sobre el uso particular del correo electrónico. Desde esta óptica, entonces, el despido de autos tampoco se ajusta a derecho. (CNTrabajo, Sala VII, «Pereyra, Leandro Ramiro c/ Servicios de Almacén Fiscal Zona Franca y Mandatos S.A. s/ Despido». 27/03/2003).

«El correo electrónico es hoy una «herramienta» más de trabajo. La cuestión sin duda debe analizarse de acuerdo a los derechos y deberes de las partes (Arts. 62 y sgts. de la LCT -Ley 20744-) y de acuerdo al principio de buena fe (Art. 63) y el Art. 70 de dicha norma, que faculta al empleador a realizar las facultades de controles personales, destinados a la protección de los bienes de la empresa.»⁷⁸

Hay que tener presente que "... las condiciones de confidencialidad de acceso por parte del empleador al "correo-herramienta", otorgado al trabajador como consecuencia de una relación laboral deben ser amplias, y ello encuentra sustento en que no se prive al trabajador de verdaderas herramientas tecnológicas imprescindibles para el desarrollo de cualquier trabajo. Si una empresa no tiene una política clara en el uso de esta

75. <http://www.portaldeabogados.com.ar/derechoinformatico/0607.htm>

76. <http://www.protecciondedatos.com.ar/>

77. <http://www.protecciondedatos.com.ar/>

78. CAUSA 15198/2001 S. 36580 - «Pereyra, Leandro Ramiro c/ Servicios de Almacén Fiscal Zona Franca y Mandatos SA s/ despido» - CNTRAB - SALA VIII - 27/03/2003.

herramienta, no advirtiéndole al empleado que dicho uso debe ser realizado exclusivamente en función de su actividad laboral y haciéndole conocer el derecho de la compañía a controlar el correcto uso del e-mail, podría crear una falsa expectativa de privacidad. (CNTrabajo, Sala VII, «Pereyra, Leandro Ramiro c/ Servicios de Almacén Fiscal Zona Franca y Mandatos S.A. s/ Despido». 27/03/2003).

Email laboral. Uso particular. V.R.I. c/ Vestiditos S.A. s/despido. Uso indebido de Correo electrónico.⁷⁹

Juzgo como suficientemente acreditado que la reclamante utilizó repetida y constantemente su horario y herramienta de trabajo (sistema de correo electrónico de la accionada) pese a las indicaciones que en contrario le fueran reiteradamente impartidas, para recepcionar y reenviar el tan particular y en diversos aspectos objetable material literario y gráfico y perturbando el normal funcionamiento de la accionada y personal de la misma en la medida que este se veía diariamente convertido en pasivo destinatario de las manifestaciones de su estrafalario sentido del humor, para calificar con suma benevolencia al contenido de aquellos mensajes (e-mails) por medio de los cuales la actora canalizaba una personalidad que no dudo en tipificar -en el aspecto que nos ocupa- como diametralmente opuesta a los lineamientos previstos por el ordenamiento legal de aplicación en lo que hace a las conductas que deben observar las partes integrantes de una relación laboral como aquella que mantuvieran los actuales litigantes. Establecida, como se ha destacado, la intervención protagónica de la actora en los sucesos de marras, el proceder disolutorio adoptado en el evento por la principal aparece como ajustado a derecho toda vez que si bien no escapa al suscripto la circunstancia de conllevar quizás la disposición resolutoria un acentuado rigorismo dado que, ante la ausencia de antecedentes sancionatorios de la dependiente podrían haberse utilizado, antes de la cesantía, las penalidades correctoras de menor alcance contempladas por el ordenamiento respectivo, no es menos cierto que las características que revistiera el tan reiterado proceder de la actual reclamante así como el contenido y trascendencia del material por aquella difundido, provee a mi entender de una justa causa al acto rescisorio adoptado por la principal.⁸⁰

Email laboral. Despido con causa. Envío de e-mails pornográficos en horario laboral.⁸¹

Así lo resolvió el juez Jorge Finizzola, quien rechazó una demanda presentada por una mujer que pedía una indemnización a la empresa que decidió prescindir de sus servicios por utilizar la computadora del trabajo para mandar correos electrónicos con esos contenidos. Enviar e-mails de contenido pornográfico utilizando una computadora del trabajo, en horario laboral, constituye «causal de despido», según resolvió el juez laboral Jorge Finizzola. El magistrado rechazó la demanda laboral planteada a raíz del despido de una mujer identificada sólo por sus iniciales, R.I.V, contra una empresa.

En marzo de 2002, la empresa despidió a RIV tras comprobar que la mujer recibía y reenviaba a sus compañeros de trabajo una gran cantidad de mails de contenido que -según el fallo- era «en su gran mayoría, ofensivo a la moral y buenas costumbres». Por esos fundamentos, entendió que «el contenido y trascendencia del material difundido, provee una justa causa» de despido. El tráfico de correos electrónicos provocaba «extrema lentitud» en la navegación por Internet y en la recepción de e-mails propios de la actividad laboral de la empresa, según una auditoría realizada por la empresa donde trabajaba RIV.

«La reclamante utilizó repetida y constantemente su horario y herramienta de trabajo, pese a las indicaciones que en contrario le fueron reiteradamente impartidas», sostuvo el juez.

«No hallo fundamento lógico, ético ni moral para que la autora de tales conductas antisociales y repudiables desde todo punto de vista, pudiera pretender percibir un monto indemnizatorio de parte de quien procedió con fundamento a resolver la desvinculación de dicha dependiente», añadió. Para el magistrado, conceder la indemnización a la empleada despedida «equivaldría a consagrar, dentro del ámbito de las relaciones laborales, un criterio que conllevaría a la indeseable consecuencia de otorgar un aparente premio a la comisión reiterada e ilimitada de conductas por completo ajenas a cualquier tipo de límites sociales, éticos y morales».

11.2. Brasil

El spam puede llegar a ser legal en Brasil

En la primera sentencia que se produjo en Brasil, el 8 de Enero de 2002, una juez de Mato Grosso do Sul consideró un contrasentido «perseguir esta actividad». El spam puede llegar a ser legal en Brasil, tras una sentencia pronunciada por la jueza Rosângela Lieko Kato del Juizado Especial Cível Micro Empresas. La

79. <http://www.protecciondedatos.com.ar/>

80. («V.R.I. c/ Vestiditos S.A. s/despido». Juzgado Nacional de Primera Instancia en lo Laboral Nº 24. 27/05/2003).

81. Fuente: DyN http://www.lanacion.com.ar/03/06/23/dg_506058.asp Nota del 23/06/2003. Diario La Nación, Información General.

juez debía resolver una demanda presentada por João Campos contra las empresas: Inova Tecnología S/C, Site Entretenimentos y el Portal Planeta Serviços e Internet en el que solicitaba una indemnización de 5000 reales por uso indebido de su nombre en listados y por haber sido objeto de una invasión de una invasión de mensajes no solicitados en su buzón de correo electrónico. La jueza comparó el spam con el envío de publicidad directa a través del correo postal, considerando que «sería un contrasentido admitir que alguien precisa una autorización para enviarnos correspondencia.» Concluyendo que «no hay motivo para caracterizar en violación de la intimidad, o de la vida privada, o de la honra», esta actividad.⁸²

11.3. España

Intercepción de correo electrónico - empleado del Deutsche Bank.

En Barcelona, el Juzgado de Instrucción nº 2, auto del día 25 de noviembre de 2001 resolvió que la interceptación de correo electrónico encuadraba en el delito de descubrimiento y revelación de secretos, previsto en el artículo 197 del Código Penal, por ello decidió elevar a juicio la causa denunciada por un empleado del Deutsche Bank.

Desde el 7 de octubre al 19 de noviembre de 1999, el denunciante «remitió, dentro de su horario laboral, 140 mensajes a través del referido correo electrónico con un total de 298 destinatarios, referentes a temas ajenos a su trabajo, así: mensajes de carácter sexista, de carácter obsceno y otros de carácter humorístico. En fecha 1 de diciembre de 2000 la entidad D.B.S.A. entregó carta de despido disciplinario al denunciante por «irregularidades detectadas en el uso del correo electrónico del Banco». El denunciante interpuso demanda por dicho despido, lo que estimó el Juzgado de lo Social nº 17 de Barcelona, acordando la nulidad del mismo. Tal resolución fué recurrida por la entidad ahora denunciada, de la cual conoció la Sala de lo Social de Catalunya (Rollo 4854/00), que estimando el recurso interpuesto revocó en su integridad la sentencia dictada en instancia, declarando la procedencia del despido y extinción del contrato afectado, sin derecho a indemnización ni a salario de trámite.

El empleado inició una causa que motivó la sentencia del Juzgado nº2 en la cual se expidió sobre el tema diciendo lo siguiente «Habida cuenta del resultado de las diligencias practicadas a lo largo de la instrucción, se desprende, prima facie, que los hechos objeto de la misma presentan caracteres del tipo penal previsto en el artículo 197 del Código Penal, por lo que procede dar cumplimiento a lo previsto en el artículo 790.1 de la Ley de Enjuiciamiento Criminal, acordando la continuación del trámite de la causa conforme a lo establecido en el artículo en el capítulo II del Título III del Libro IV de la Ley de Enjuiciamiento Criminal, dando traslado de la causa al Ministerio Fiscal y a la Acusación Particular personada, a fin de que, en el plazo común de cinco días soliciten, o bien la apertura del juicio oral en la forma prescrita por la ley formulando escrito de acusación o bien el sobreseimiento de la causa, sin perjuicio de que puedan solicitar, excepcionalmente, la práctica de diligencias complementarias que consideren indispensables para formular acusación.»⁸³

Uso indebido de instrumentos de la empresa

Contradictoriamente, en Madrid, los tribunales avalan el despido por el abuso del correo electrónico e Internet. Los jueces estiman que abusar de la Red vulnera la buena fe contractual.⁸⁴

Los tribunales han comenzado a fallar sobre conflictos surgidos entre empresa y trabajador por el abuso del correo electrónico e Internet en horario laboral. La mayor parte de las sentencias fallan que los empleados han vulnerado con ello la buena fe contractual del empresario.

Abusar del acceso a Internet y al correo electrónico desde el lugar del trabajo para fines distintos de los estrictamente profesionales puede tener consecuencias graves para los trabajadores. Ésta es la tendencia de las últimas sentencias. El Tribunal de Cataluña ha dictado varias resoluciones en este sentido. Considera procedente el despido de trabajadores que abusaron del uso de la Red. Según este tribunal, es una «clara infracción del deber de lealtad laboral que justifica la decisión empresarial de extinguir el contrato de trabajo». Utilizar el correo electrónico para denigrar a una compañera de trabajo fué considerado por la sala (5-7-2000) un uso indebido de instrumentos de la empresa para fines ajenos a los laborales. También lo consideró así en un fallo de 14 de noviembre de 2000.

Derecho a la intimidad, inviolabilidad y uso de casillas de e-mail laboral.⁸⁵

Dos fallos de tribunales españoles dejaron sin efecto despidos por uso indebido de e-mail laborales. En tanto que un pronunciamiento avaló la privacidad y el derecho a la intimidad, el otro consideró que la potestad del empleador del despido fué extrema ya que al empleado se lo pudo haber sancionado.

82. www.delitosinformaticos.com/noticias/

83. <http://www.bufetalmeida.com/sentencias/deutsche.html>

84. www.aui.es/biblio/bolet/bole022/product.htm 03/08/2001. Arantxa Corella. Madrid.

85. Diario Judicial - Noticia del día Lunes, 14 de Julio de 2003

La justicia española por medio de dos sentencias consideró improcedentes los despidos de dos trabajadores quienes habían sido despedidos de sus respectivos trabajos. Los motivos “justificados” del empleador en un caso, fué el uso del correo electrónico para charlas privadas, en tanto que el otro despido fué por hacer chistes “agravantes” según el empleador, sobre la empresa.

El primero de los fallos, del Tribunal Superior de Justicia catalán, hizo primar “el derecho a las comunicaciones” que figura en el artículo 18 de la Constitución Española para declarar improcedente el despido de la empleada al comprobarse en su casilla de correo electrónico que mantenía charlas de temas privados. El fallo consideró así que el correo electrónico es inviolable, y ratificó el pronunciamiento de la instancia anterior del Juzgado Social Nº 32 de Barcelona que no reconoció como prueba válida los correos electrónicos presentados por la empresa, alguno de los cuales contenían las conversaciones de carácter íntimo entre la trabajadora y otras empleadas. Además el juez, limitó en lo relativo al e-mail las facultades de control del empleador al determinar que no se podrá aplicar para casos similares los puntos del artículo 20.3 del Estatuto de los Trabajadores que permite al empresario “*adoptar las medidas más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana...*”.

En este sentido precisó que sólo se puede acceder a las casillas de correo mediante “necesidad o propósito especificado y explícito y legítimo; que la supervisión sea una respuesta legítima y proporcionada sobre un patrón de riesgo, y que tenga mínimas repercusiones en los derechos a la intimidad de los trabajadores”.

Esta resolución abre una nueva arista para resolver éstas cuestiones ya que se garantizó la inviolabilidad del e-mail laboral, inviolabilidad que no es tenida en cuenta por la corriente doctrinal que considera al e-mail como una herramienta más de trabajo que el empleador pone a disposición del trabajador, y considera legítimo por ello el ejercicio de la potestad de control que posee el empleador sobre el dependiente, en este caso sobre las casillas de e-mails laborales.

Distinta postura

Otro tribunal de Barcelona, el Social Nº 2 de Granollers, también declaró improcedente el despido que sufrió un trabajador de Bimbo por enviar un chiste sobre la empresa por correo electrónico, aunque destacó que el hombre cometió una falta grave al enviar el e-mail.

El hombre trabajaba en la planta de Bimbo de Granollers desde 1995, y fué despedido después de que la dirección de la firma le abriera un expediente disciplinario por remitir desde el ordenador de su casa y fuera del horario de trabajo un chiste desde la casilla de «e-mail» laboral a sus compañeros.

El chiste por el que fué despedido, trata sobre un hombre que es atracado en plena calle por un delincuente que le obliga a darle todo los objetos de valor. La víctima le dá el reloj, un Rolex falso, y una cartera de imitación de marca con una moneda de dos céntimos de euro en el interior. Ante esto, el ladrón le pregunta dónde trabaja, a lo que responde que es un cargo intermedio de Bimbo, momento en el que el delincuente se quita su máscara y le pregunta ¿en qué planta está?

En este pronunciamiento se condenó a la empresa a que indemnice al trabajador con 37.903,01 euros o a que en su defecto lo vuelva a tomar en las mismas condiciones en las que estaba trabajando cuando fué dejado cesante, tal cual lo reclamó la defensa del empleado.

Para el magistrado, si bien «el trabajador se excedió en el ejercicio de su derecho a la libertad de expresión», la decisión de la compañía de despedirlo fué “más allá de una racional interpretación».

El magistrado consideró así que por el contenido de la broma el empleado debía haber sido doblemente sancionado; por haber cometido una infracción grave y también por haber usado el correo de la empresa.

De ese modo, el magistrado remarcó que «la imposición de la sanción de despido» al trabajador fue «desproporcionada» y «excesiva» por lo que hubiera podido ser sancionada por la empresa al cometer dos faltas graves aunque, concluyó, la sentencia «sólo puede declarar la procedencia o improcedencia del despido sin que pueda autorizar una sanción de inferior entidad».

11.4. Estados Unidos

Acuerdo Extrajudicial por estafa vía Spam.⁸⁶

Tres ciudadanos estadounidenses, residentes de Illinois, llegaron a un acuerdo extrajudicial, por el cual tendrán que devolver 200 mil dólares a un grupo de gente que fue estafada por un esquema fraudulento de «trabaje desde su hogar llenando sobres». La maniobra por la cual se denunció la actividad de estas personas, consistía en el envío de un mensaje de correo electrónico en donde se leía “trabaje desde su hogar llenando sobres”. La oferta laboral consistía en que los potenciales trabajadores debían enviar 40 dólares y

86. <http://www.diariojudicial.com/default.asp?Estilo=1&Pagina=nota.asp?ID=14271> miércoles 2 de julio, 12:45 PM
<http://mx.news.yahoo.com/030702/2/1270b.html> «Spammers» solucionan cargos de fraude en Estados Unidos

luego se le mandaría el material y por cada sobre que llenaran estas personas recibirían 2 dólares, pero al parecer rara vez recibieron los elementos para trabajar. La oferta laboral era enviada desde el sitio www.stuffingforcash.com, que fue clausurado por un juez estadounidense a mediados del año 2002 a raíz de las estafas que venían denunciando los usuarios por esas maniobras. Ante la difícil situación por la que atraviesan Nelson Barrero, Eduardo Gonzáles e Ileana M. Morales decidieron llegar al acuerdo extrajudicial para evitar las duras sanciones que podrían tener, aunque uno de ellos enfrenta 5 años de cárcel por otra causa paralela. El más comprometido, Barrero, está en prisión después de haberse declarado culpable de dos cargos de fraude de comunicaciones en una investigación criminal separada. Ahora, los tres acordaron devolver 221.600 dólares a los consumidores y abstenerse en el futuro de organizar operaciones de trabajo desde el hogar.

Robo de información confidencial (Responsabilidad del dueño o guardián sobre el contenido de la base de datos personales)⁸⁷

En el mes de Mayo de 2003, un empleado de Coca-Cola se infiltró hace pocas semanas en los sistemas informáticos de la compañía y consiguió robar los datos privados de 450 empleados, entre los que se incluía información sobre los salarios y números de la seguridad social.⁸⁸ La compañía de refrescos más grande del mundo no ha podido hacer nada contra un atacante interno, con acceso a sus redes informáticas, pero que se supone no tenía permiso para obtener información confidencial de otros colegas. Como medida de seguridad, la empresa ha decidido enviar un correo a todos sus empleados avisándoles del problema y aconsejándoles estar atentos a los movimientos de sus cuentas en busca de algo sospechoso, pero en ningún momento avisó a la policía del problema.

De producirse algún perjuicio por este robo de datos, Coca Cola, estaría obligada a indemnizar a las víctimas ya que tiene la obligación y el deber de proteger las bases de datos de sus empleados y es responsable por los daños que causaren los que están bajo su dependencia, o por las cosas de que se sirve, o que tiene a su cuidado.⁸⁹

Lori Billingsley, portavoz de Coca-Cola en Atlanta, informó de que se había abierto una investigación interna para buscar al culpable. La empresa está segura de que la información confidencial no abandonó el edificio en ningún momento, pero, aun así, previene a sus empleados sobre la posibilidad de movimientos inesperados en sus cuentas. No se ha hecho pública la identidad del atacante, pero el representante de Coca-Cola aseguró que se han tomado las medidas disciplinarias necesarias.

La información no solo puede verse vulnerada desde el exterior. Aunque las cifras varían entre las distintas fuentes, el instituto SANS dedicado a la seguridad, estima que alrededor del 80% de los ataques que sufren las empresas vienen producidos por personal de la propia firma o gente vinculada. Empleados insatisfechos o personas que tienen acceso a determinados datos y que en algún momento deciden que pueden sacarle más partido usándolos de cualquier otra manera. En muchas ocasiones, si esta información es manejada con cautela, puede que el delito nunca llegue a ser descubierto.

Mustaque Ahamad, co-director del Information Security Center en Georgia, advierte, a propósito del incidente, sobre lo difícil de realizar estadísticas fiables en este tipo de casos. Los ataques internos no son reportados a las autoridades con demasiada frecuencia, debido casi siempre al deterioro que causan en la imagen de la empresa, y prefieren ser resueltos internamente. Además, un empleado siempre goza de cierta confianza y conocimiento de la estructura interna de la compañía, lo que lo hace mucho más eficaz a la hora de obtener información confidencial sobre la empresa que lo contrata. Sólo una buena política de seguridad definida, puede mitigar los efectos de esta amenaza.

Daños y Perjuicios contra EarthLink por envío de Spams.

La industria de Internet de Estados Unidos obtuvo una importante victoria al conseguir que un tribunal condenara a un 'spam', una persona dedicada a bloquear cuentas de correo electrónico con mensajes indeseados, a pagar 16,4 millones de dólares en concepto de daños y perjuicios al portal 'EarthLink'. Howard Carmack, alias 'Buffalo Spammer', fué condenado por haber enviado, desde marzo de 2002, unos 825 millones de correos comerciales a cuentas de correo que obtuvo después de adoptar múltiples identidades, indicó en un comunicado 'EarthLink'. La decisión del tribunal federal de Georgia (sur) a favor del tercer sitio de acceso de Estados Unidos, abre el camino a que otras empresas del sector como AOL, Microsoft o Yahoo tengan alternativas judiciales parecidas⁹⁰.

87. <http://www.delitosinformaticos.com/protecciondatos/noticias/> Sergio de los Santos s.delossantos@forzis.com Noticias actuales... Archivo de noticias...

88. Atlantic Journal Constitution

89. Conclusión según la aplicación del art. 1113 del Código Civil Argentino.

90. <http://www.elmundo.es/navegante/2003/05/08/seguridad/1052363536.html> EP/AFP WASHINGTON

America Online demanda por Daños y Perjuicios provocados por Spams.

En el mes de Abril de 2003, América Online presentó cinco demandas en la Corte Federal de Alexandria, en el Estado de Virginia, en contra de más de una decena de empresas de particulares a quienes les imputa la responsabilidad de llenar las casillas de los correos con basura publicitaria. La suma pedida en concepto de indemnización por los daños y perjuicios que le provocan este tipo de correos oscila en los 10 millones de dólares. La empresa aduce que estos spams provocaron ocho millones de reclamos de sus respectivos clientes. Por su parte, la presentación de AOL se suma a las medidas que las firmas EarthLink y Microsoft, lanzaron con el fin de poner freno a la llegada de los correos no deseados⁹¹.

Ataque Diccionario contra Hotmail de Microsoft

El pasado 20 de febrero de 2003, la empresa Microsoft demandó a los presuntos responsables del envío de spam a cuentas de correo Hotmail. Microsoft interpuso la demanda ante una corte federal del distrito norte de California en San José (Estados Unidos). En el proceso no se llamará al demandado, pero se permitirá al querellante la potestad de emitir citaciones como parte de la fase de investigación del mismo. Los demandados están acusados de usar un «ataque de diccionario» (conocido como el ataque en el que un programa de ordenador intenta obtener el password de los usuarios), para descubrir la actividad de las cuentas de correo electrónico de Hotmail. En éste caso concreto, el citado programa informático obtuvo millones de direcciones de e-mail.⁹²

America Online c/ CN Productions por Daños y Perjuicios por envío de spams.

El 19 de Diciembre de 2002, la Corte de Estados Unidos dictaminó a favor de América Online otorgándole una indemnización de siete millones de dólares en concepto de daños y perjuicios ocasionados por la empresa CN Productions, que envió cerca de un billón de correos electrónicos no deseados a usuarios de AOL para captarlos hacia sitios web con contenidos de adultos. La corte dictaminó que, con ésta decisión ya son dos las denuncias que gana el gigante AOL contra la compañía CN Productions y su dueño Jay Nelson.⁹³

En el mes de Septiembre de 2002, el estado de California emprendió acciones legales contra el spam. El objetivo es proteger a los consumidores frente a la invasión de correos electrónicos no solicitados que invaden sus cuentas electrónicas violando la legislación estatal. En la legislación de California se contempla desde 1998 la prohibición de mandar correos comerciales a empresas o a personas que no los han solicitado.⁹⁴

Fiscal General de Nueva York, Eliot Spitzer, demanda a la compañía MonsterHut por Spams.

El 29 de Mayo de 2002, el fiscal general de Nueva York, Eliot Spitzer, presentó una demanda contra la compañía MonsterHut por el envío de más de 500 millones de mensajes electrónicos a consumidores que no habían dado su permiso. El fiscal dijo que el Spam no sólo es una molestia para el usuario, sino también un vehículo para el fraude. La compañía, con base en Niagara Falls, su director ejecutivo, y el director técnico están acusados de publicidad fraudulenta y de asegurar que su servicio de 'marketing' electrónico contaba con el visto bueno de sus destinatarios. En la demanda se alegó que la lista de receptores incluyó numerosos nombres de individuos a los que la compañía nunca preguntó si deseaban recibir sus mensajes y que ésta se benefició con esas prácticas ilegales⁹⁵. Más de 750.000 receptores habían reclamado a la compañía que los borrara de su lista de destinatarios y decenas de miles se habían quejado a la empresa Pae Tec, que proveía el acceso a la firma en Internet. Este proveedor cortó el servicio a MonsterHut a comienzos de este mes, después de que un tribunal de apelaciones ratificara que esta empresa había violado sus compromisos contractuales sobre envíos masivos de publicidad no solicitada. Sin embargo, esto no impidió a MonsterHut continuar con sus prácticas a través de otro proveedor de Internet.

11.5. Japón**NTT DoCoMo por Daños y perjuicios.**

El principal operador de telefonía móvil en Japón, NTT DoCoMo, logró que un tribunal de Tokio dicte una sentencia favorable a compensar los costes por el envío de correo electrónico masivo a través de su servicio

91. <http://www.elmundo.es/navegante/2003/04/15/esociedad/1050395621.html> Reuters-EIMundo.es

92. <http://www.elmundo.es/navegante/2003/04/11/esociedad/1050048044.html>

93. www.elmundo.es/navegante/2002/12/19/empresas/1040288154.html Europa Press

94. www.europapress.es/europa2001/abierto/noticia.asp?cod=20020927164803 29/09/02

95. <http://www.elmundo.es/navegante/2002/05/29/empresas/1022631307.html> Agencia EFE. Desde marzo de 2001, MonsterHut ha inundado los buzones electrónicos con más de 500 millones de anuncios sobre una variedad de bienes y servicios, a la vez que las quejas de los consumidores han sido abrumadoras, indicó el fiscal de Nueva York.

inalámbrico de Internet. La cifra que la compañía denunciada debió pagar en concepto de multa por el envío de SPAM, según el tribunal, asciende a 6,57 millones de yenes. Esta cifra ha sido valorada por las autoridades de DoCoMo, que informaron que dedicaban más de cuatro millones de yenes en devolver «e-mails» enviados a su red dirigidos a números de teléfono que no existen. El resto de la compensación está destinada a cubrir consultorías y honorarios legales relacionados con este caso. El SPAM a teléfonos móviles tiene la peculiaridad que el usuario debe pagar por sus correos electrónicos descargados.⁹⁶

12. Glosario

- **Abuso de Correo Electrónico (ACE):** diversas actividades que trascienden los objetivos habituales del servicio de correo y perjudican directa o indirectamente a los usuarios. También llamado Spamming, Mail bombing, unsolicited bulk email (UBE), unsolicited commercial email (UCE), junk mail, etc. Acrobat Reader, es la aplicación que se usa para leer archivos y Acrobat Exchange es la que se usa para crear los archivos PDF. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico.
- **Banner:** anuncios publicitarios que por lo general aparecen cuando estamos navegando sin que nosotros los llamemos, en la parte superior de las páginas y que al ser tocados, llevan al usuario al sitio del anunciante. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico.
- **BBS (Bulletin Board System):** Ordenador y programas que habitualmente suministran servicios de mensajería electrónica, archivos de ficheros, bases de datos y cualquier otro servicio y actividad. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico.
- **Bounce (rebote):** Devolución de un mensaje de correo electrónico debido a error en la entrega al destinatario. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico.
- **Browser (Navegador):** Un programa que permite al usuario navegar por la web. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico.
- **Bulletin Board electrónico:** comprende todo foro de discusión o conferencia virtual. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico.
- **Buscador:** Sitios en el web que catalogan y organizan el contenido de Internet para ayudar a los usuarios a encontrar la información que están buscando. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico.
- **Campo del Asunto:** es el área que contiene una breve descripción del contenido del mensaje. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico. <http://www.hfernandezdelpech.com.ar/>
- **Chat:** Comunicación simultánea entre dos o más personas a través de Internet. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico. <http://www.hfernandezdelpech.com.ar/>
- **Comercio electrónico:** Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información. Definición según LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS. Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
- **Computador:** dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas. Definición según LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS Nº 48 DE LA REPUBLICA DE VENEZUELA
- **Cookies:** cookies, o galletas, son una tecnología implementada en los «browsers» de Internet que permite que el servidor archive información relacionada a los patrones de comportamiento del usuario en su propia máquina. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico. <http://www.hfernandezdelpech.com.ar/>
- **Correo Electrónico:** significa 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. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico. <http://www.hfernandezdelpech.com.ar/>
- **Correo Electrónico Comercial:** significa todo mensaje, archivo, dato u otra información electrónica enviado con el fin de hacer publicidad, comercializar o tratar de despertar el interés respecto de un producto,

96. Sentencia contra el envío de SPAM en servicio inalámbricos de Japón [25-03-03] www.delitosinformaticos.com/noticias/

- servicio o empresa. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico. <http://www.hfernandezdelpech.com.ar/>
- Correo Electrónico no solicitado: significa todo mensaje, archivo, dato u otra información electrónica dirigido a un receptor con quien el originador del mensaje no tiene una relación comercial o personal existente y enviado sin que medie un pedido expreso del receptor o sin su expreso consentimiento. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico. <http://www.hfernandezdelpech.com.ar/>
 - Crackear: Ingresar a un sistema informático pasando las barreras de seguridad. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico. <http://www.hfernandezdelpech.com.ar/>
 - Cracker (intruso): Un «cracker» es una persona que intenta acceder a un sistema informático sin autorización. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico. <http://www.hfernandezdelpech.com.ar/>
 - Cyberspace (Ciberespacio): Término creado por William Gibson en su novela fantástica «Neuromancer» para describir el «mundo» de los ordenadores y la sociedad creada en torno a ellos. Definición según el Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico. <http://www.hfernandezdelpech.com.ar/>
 - Data: hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar significado. Definición según LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS Nº 48 DE LA REPUBLICA DE VENEZUELA.
 - Dato informático o información: es toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático. Definición según (1299-D-2002).
 - Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley. Definición según LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS. Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
 - Datos personales autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular. Definición según LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS. Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
 - Datos de creación: Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica. Definición según LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS. Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
 - Dirección de correo electrónico: serie de caracteres utilizada para identificar el origen o el destino de un mensaje de correo electrónico. Definición según ANTEPROYECTO DE LEY DE REGULACIÓN DE LAS COMUNICACIONES PUBLICITARIAS POR CORREO ELECTRÓNICO.
 - Dirección IP (IP address): Dirección de 32 bits definida por el Protocolo Internet. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de dirección IP es 193.127.88.345. <http://www.antispam-argentina.8m.net/paginas/Definiciones>
 - Dispositivo electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta. Definición según LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS. Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
 - Dispositivo de emisión: Instrumento físico o lógico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica. Definición según LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS. Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
 - Dominio: Es la parte de una dirección de Internet que indica el domicilio del servidor. <http://www.antispam-argentina.8m.net/paginas/Definiciones>
 - Encriptado: Es el tratamiento de los datos a fin de impedir que nadie excepto el destinatario de los mismos puede leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red. <http://www.antispam-argentina.8m.net/paginas/Definiciones>
 - File Transfer Protocol (FTP) (Protocolo de Transferencia de Archivos): Protocolo que permite a un usuario de un sistema acceder, y transferir a y desde, otro sistema de una red. FTP es también habitualmente el nombre del programa que el usuario invoca para ejecutar el protocolo. <http://www.antispam-argentina.8m.net/paginas/Definiciones>
 - Hacker (pirata): Una persona con un conocimiento profundo sobre el funcionamiento interno de los sistemas informáticos, de un ordenador o de una red de ordenadores. Este término se suele utilizar para

aquellos que intentan obtener información privada, accesos privados o ventajas rompiendo barreras de seguridad. Para muchos, en este último sentido, sería más correcto utilizar el término «cracker». <http://www.antispam-argentina.8m.net/paginas/Definiciones>

- **Hardware:** equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que forman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes. LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS Nº 48 DE LA REPUBLICA DE VENEZUELA.
- **Hipertexto (hypertext):** Documento escrito en HTML que contiene enlaces a otros documentos que pueden ser a su vez documentos hipertexto. Los documentos hipertexto son accedidos normalmente a través de navegadores WWW. <http://www.antispam-argentina.8m.net/paginas/Definiciones>
- **Host (sistema central):** Ordenador que permite a los usuarios comunicarse con otros sistemas centrales de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el correo electrónico, Telnet, WWW y FTP. <http://www.antispam-argentina.8m.net/paginas/Definiciones>
- **HTML (Hyper Text Markup Language):** Es un lenguaje de programación de computadoras que permite al usuario crear documentos de hipertexto para su publicación en el web. <http://www.antispam-argentina.8m.net/paginas/Definiciones>
- **HTTP (Hyper Text Transfer Protocol):** Es un protocolo de comunicación de datos que permite la transmisión de documentos de hipertexto a través de redes. Es el protocolo en el que está basado el web. <http://www.antispam-argentina.8m.net/paginas/Definiciones>
- **Internet:** es la red de computadoras más grande del mundo. Tuvo sus inicios en los Estados Unidos durante la guerra fría bajo la amenaza de un holocausto nuclear, el Departamento de Defensa de los Estados Unidos desarrolló un sistema de telecomunicaciones digitales descentralizado que es extremadamente fluido y flexible. En un principio, la aplicación principal era el correo electrónico, que permite a personas geográficamente distantes comunicarse de maneras muy eficientes. Con la aparición del «World-Wide Web» en 1993, Internet gozó de un resurgimiento de interés, esta vez en parte del público general. http://www.ram.com.mx/srvicios/Manual_INTERNET/documento/Spam.htm
- **Intimidación:** El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS. Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR
- **Intranet:** Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS. Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR
- **IP (Internet Protocol):** Protocolo principal de comunicaciones a través de Internet. La transmisión de información ocurre mediante pequeños paquetes de «bits» que contienen la información que está siendo mandada y la dirección hacia la que se dirigen. <http://www.antispam-argentina.8m.net/paginas/Definiciones>
- **Java:** Es un lenguaje de programación desarrollado para producir aplicaciones que corren a través de redes. http://www.ram.com.mx/srvicios/Manual_INTERNET/documento/Spam.htm
- **JavaScript:** Es un lenguaje de programación interpretado y diseñado para complementar las capacidades del HTML. http://www.ram.com.mx/srvicios/Manual_INTERNET/documento/Spam.htm
- **Mensaje de datos:** Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
- **Netscape Navigator:** Es el browser de Netscape Communications Corp., una compañía fundada por Marc Andreessen, uno de los autores originales del browser Mosaic. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
- **Network (red):** Una red de ordenadores es un sistema de comunicación de datos que conecta entre sí sistemas informáticos situados en diferentes lugares. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
- **Nombre de dominio de Internet:** denominación global única y jerárquica de un sistema anfitrión (host) o de un servicio de Internet, que es asignada por autoridades centralizadas encargadas de otorgar dichas denominaciones y esta formada por una serie de caracteres separados por puntos. ANTEPROYECTO

DE LEY DE REGULACIÓN DE LAS COMUNICACIONES PUBLICITARIAS POR CORREO ELECTRÓNICO.

- Página web: Una página es un documento dentro de un sitio de Internet que contiene información. Por lo general (aunque no necesariamente) están escritas en un lenguaje que se llama HTML. http://www.ram.com.mx/srvicios/Manual_INTERNET/documento/Spam.htm
- Password: Contraseña. http://www.ram.com.mx/srvicios/Manual_INTERNET/documento/Spam.htm
- PDF (Portable Document Format): El formato utilizado por el Acrobat de Adobe para representar documentos de manera independiente al sistema operativo en que fueron creados. http://www.ram.com.mx/srvicios/Manual_INTERNET/documento/Spam.htm
- Plug and play (Enchufar y Utilizar): Se aplica a los accesorios para computadoras, internos o externos, que no necesitan de una configuración técnica sino que con solo enchufarlos estarán listos para ser usados.

http://www.ram.com.mx/srvicios/Manual_INTERNET/documento/Spam.htm

- Procesamiento de data o de información: realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo. LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS N° 48 DE LA REPUBLICA DE VENEZUELA.
- Programa: plan, rutina o secuencia de instrucciones utilizados para realizar un trabajo en particular o resolver un problema dado a través de un computador. LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS N° 48 DE LA REPUBLICA DE VENEZUELA.
- Protocolo: Es una lengua común que se establece en dos computadoras para que éstas puedan comunicarse. Existen muchos protocolos. En el Internet, el protocolo más importante es el «TCP/IP». http://www.ram.com.mx/srvicios/Manual_INTERNET/documento/Spam.htm
- Proveedor de servicio de correo electrónico: comprende a toda persona física o jurídica que provee a los usuarios registrados la capacidad para enviar o recibir correo electrónico y que actúa como intermediario en el envío o la recepción de dicho correo electrónico. ANTEPROYECTO DE LEY DE REGULACIÓN DE LAS COMUNICACIONES PUBLICITARIAS POR CORREO ELECTRÓNICO.
- Receptor: comprende a toda persona que recibe correo electrónico comercial no solicitado. ANTEPROYECTO DE LEY DE REGULACIÓN DE LAS COMUNICACIONES PUBLICITARIAS POR CORREO ELECTRÓNICO.
- Red: Dos o más computadoras conectadas entre sí, permitiendo a sus usuarios compartir archivos y recursos. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
- Red electrónica de información: Es un conjunto de equipos y sistemas de información interconectados electrónicamente. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS. Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
- Red Informática: significa una serie de dispositivos y facilidades de comunicaciones relacionados y conectados en forma remota y todo tipo de facilidades de comunicaciones que incluya a más de una computadora que tenga la capacidad de transmitir datos entre sí a través de las facilidades de comunicaciones. ANTEPROYECTO DE LEY DE REGULACIÓN DE LAS COMUNICACIONES PUBLICITARIAS POR CORREO ELECTRÓNICO.
- Seguridad Informática: Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación. LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS N° 48 DE LA REPUBLICA DE VENEZUELA.
- Servicio electrónico: Es toda actividad realizada a través de redes electrónicas de información. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS. Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
- Servidor: Una computadora en una red cuyo propósito es dar acceso a (servir) archivos. El otro polo en la relación es el cliente, que es la computadora que interpreta y despliega la información siendo servida. ANTEPROYECTO DE LEY DE REGULACIÓN DE LAS COMUNICACIONES PUBLICITARIAS POR CORREO ELECTRÓNICO.
- Sin autorización: significa que una persona utiliza una red informática de un proveedor de servicio de correo electrónico para transmitir correo electrónico comercial no solicitado excediendo el permiso concedido o violando las políticas establecidas por el proveedor del correo electrónico. ANTEPROYECTO DE LEY DE REGULACIÓN DE LAS COMUNICACIONES PUBLICITARIAS POR CORREO ELECTRÓNICO.

- Sistema de información: se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos. LEY MODELO DE LA COMISION DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL (CNUDMI) SOBRE COMERCIO ELECTRÓNICO.
- Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma, mensajes de datos. LEY DE COMERCIO ELECTRÓNICO, FIRMAS Y MENSAJES DE DATOS. Ley No. 67. RO Sup. 557 de 17 de Abril del 2002 ECUADOR.
- Sistema informático: es todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio. (1299-D-2002).
 - Sistema operativo: El software de nivel bajo que se encarga de organizar la operación de la computadora, asignar recursos, manejar la interfaz con los diversos periféricos, y comunicarse con el usuario. (1299-D-2002).
 - Sistema opt-in: mediante éste sistema, quien pretenda enviar mensajes comerciales deberá contar con la autorización expresa del destinatario. www.protecciondedatos.com.ar
 - Sistema opt-out: permite a los usuarios solicitar que sus datos sean excluidos de las bases de datos utilizadas por los spammers. www.protecciondedatos.com.ar
 - Software: información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que éstos realicen funciones específicas. LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS Nº 48 DE LA REPUBLICA DE VENEZUELA.
 - Spam: Un SPAM es cualquier mensaje, destinado a una audiencia en general (o sea, un comunicado de masas) que se envía a la gente por e-mail sin que lo soliciten. <http://www.antispam-argentina.8m.net/paginas/info.htm#Definiciones>
 - Transmitir o ayudar a la transmisión: Significa toda acción efectuada por el remitente original de un mensaje de correo electrónico, no a la acción efectuada por cualquier proveedor de servicio de correo electrónico que pueda manejar o retransmitir el mensaje, salvo que dicho proveedor de servicio ayude en la transmisión sabiendo que se trata de correo electrónico que viola las disposiciones de la presente ley. ANTEPROYECTO DE LEY DE REGULACIÓN DE LAS COMUNICACIONES PUBLICITARIAS POR CORREO ELECTRÓNICO.
 - Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data. LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS Nº 48 DE LA REPUBLICA DE VENEZUELA.
 - Usenet: Una aplicación de Internet que permite a personas con intereses similares compartir información a través de listas de correo electrónico organizadas y archivables. Los grupos de noticias son una herramienta para buscar información sobre diversos temas, ya que reúne el conocimiento colectivo de grandes masas de personas. LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS Nº 48 DE LA REPUBLICA DE VENEZUELA.
 - Virus: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema. LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS Nº 48 DE LA REPUBLICA DE VENEZUELA.
 - WWW (World-Wide Web): La aplicación más importante de Internet es este sistema de hipermedia desarrollado por Tim-Berners Lee en 1993. <http://www.antispam-argentina.8m.net/paginas/info.htm#Definiciones>

13. Bibliografía

- Agencia EFE
- Comercio Electrónico y Firma Digital. La Regulación del Ciberespacio. Horacio M. Lynch.
- Comercio Electrónico y Firma Digital. La Regulación del Ciberespacio y las Estrategias Globales. Mauricio Devoto.
- Como defenderse del Spam, La Nación, Mi PC, notas.
- El proceso de Habeas Data en la nueva ley de datos personales, Dr. Osvaldo Gozaíni.
- El habeas data en la reforma constitucional. Autor: Ekmekdjian.
- La Argentina y la Revolución Digital, La Nación, Editorial, 28 de diciembre de 1999.
- La Revolución Digital y la Privacidad, Dr. Miguel Padilla.
- «INTERNET: Su Problemática Jurídica» por Horacio Fernández Delpech
- El Sueño de una Argentina Digital, La Nación, Editorial, 9 de marzo de 2001.
- Nuevas tecnologías, Internet y derechos fundamentales, Fernández, Maria Luisa, 1998, Editorial McGraw Hill, Madrid, España.
- Manual de la Constitución Reformada. German J. Bidart Campos.
- Resumen de ideas para considerar el desarrollo de INTERNET en la Argentina, Secretaría de Comunicaciones de la Presidencia de la Nación (SECOM) para el día 6 de agosto de 1997, Guillermo Bort, Impsat.
- Revista Plenario.
- Reuters MJG RS/
- EUROPA PRESS
- Diario Tecnologías de la Información. <http://diarioti.com>
- Directiva sobre la privacidad y las comunicaciones electrónicas, Diario Oficial n° L201 31/07/2002 p.0037-0047.
- Directiva de la Unión Europea sobre Comercio Electrónico.
- Directiva 95/46/CE.
- LEY ESPECIAL CONTRA LOS DELITOS INFORMATICOS N° 48 DE LA REPUBLICA DE VENEZUELA.
- Enmienda 1618 de la Ley de Comunicaciones de USA.
- exp. 1299-D-2002. Cámara de Diputados. Proyecto.
- Ley 25.326. Habeas Data.
- LEY 19628 SOBRE PROTECCIÓN DE LA VIDA PRIVADA DE CHILE.
- Ley de Comercio Electrónico, Firmas y Mensajes de Datos del Ecuador.
- Anteproyecto de Ley de Regulación de las comunicaciones publicitarias por correo electrónico.

14. Información Web

- www.argentinajuridica.com
- <http://www.aadt.org.ar/>
- <http://www.aaba.org.ar/>
- ACADEMIA MEXICANA DE DERECHO INFORMÁTICO
- <http://www.antispam-argentina.8m.net/>
- <https://www.agenciaprotecciondatos.org/novedades.htm>
- ABA Comm. E-Commerce
- ARTIGOS SOBRE DIREITO E INFORMÁTICA
- Agencia Española de Protección de Datos
- Albany Law Journal of Science and Technology
- Anti-Defamation League
- Arizona State University, Jurimetrics Journal of Law, Science and Technology
- <http://www.aui.es/>
- Bitlaw: Internet Law
- Boletín Hispanoamericano de Informática y Derecho
- Boston University School of Law - Journal of Science & Technology Law
- Brief Reporter
- BOLETIN HISPANOAMERICANO DE INFORMATICA Y DERECHO
- Bytes in Brief
- <http://www.bufetalmeida.com/>
- <http://www.cnc.gov.ar>
- <http://ciberderechos.8k.com/>
- <http://www.clarin.com/diario/hoy/s-6301.htm>
- [http://www.cauce.org /](http://www.cauce.org/)
- Canadian Internet Law Resource Page (CILRP)
- Cases concerning the Internet
- Chicago-Kent College of Law - Journal of Intellectual Property
- Chilling Effects
- Coalition Against Unsolicited Commercial Email (CAUCE)
- CommerceNet
- Computer Law
- Computer Law Asociation
- Computers and Information Technology laws
- Cyberlaw
- CENTRO DE INFORMÁTICA JURÍDICA - Facultad de Derecho de Chile
- Cyberlaw Encyclopedia
- Cyberlex
- Cyberspace Laws
- CyberSecurities Law Tribune
- www.diariojudicial.com
- <http://www.diputados.gov.ar/>
- <http://www.digigrup.net/faq.htm>
- <http://www.dcc.uchile.cl/>
- Data Protection European Directive
- Data Protection UK
- Dirección Nacional de Protección de Datos Personales
- Dominiuris
- DERECHO INFORMÁTICO - RKT LEGAL CONSULTING (México)
- Electronic Frontier Foundation
- Electronic Privacy Information Center
- <http://www.escrache.com.ar/>
- www.eldial.com
- <http://www.euro.cauce.org/es/>
- http://europa.eu.int/pol/infso/index_es.htm
- http://www.europarl.eu.int/home/default_es.htm - Home Page del Parlamento Europeo

- <http://es.postmastergeneral.com/>
- EPIC - Tools for Protecting Online Privacy
- Findlaw CyberLaw
- Franklin Pierce Law Center - IDEA: The Journal of Law and Technology
- <http://www.fes.de/organisation/america/handbook/esp/index.html>
- Glosario de términos de uso habitual en informática e Internet
- <http://www.geocities.com/SiliconValley/Circuit/4888/principal.htm>
- Harvard University School of Law - The Berkman Center for Internet & Society
- Home Recording Rights Coalition
- http://www.hfernandezdelpech.com.ar__
- <http://home.snafu.de/>__
- www.hotmail.com
- <http://www.imc.org/>__
- <http://infoleg.mecon.gov.ar/basehome/alfaredi.htm>
- <http://www.isoc.org.ar>
- <http://www.it-cenit.org.ar>
- IUSTOPIA - Primer site de información ciberjurídica de Panamá
- IANA
- ICANN
- Infolaw Web - Things
- Intellectual Property on the WWW
- INFORMÁTICA JURÍDICA DOCUMENTAL (Chile)
- Internet Law & Policy Forum
- Internet Legal
- JUS - DIREITO E INFORMATICA (Brasil)
- JURISMATICA (México)
- Internet Society
- <http://infoleg.mecon.gov.ar/normas/68794.htm>
- John Marshall School of Law - Journal of Computer & Information Law
- <http://www.kriptopolis.com/>
- Kuesterlaw
- <http://www.lawnuevo.com>
- LatinoamerlCANN
- INFOJUR - Laboratorio de informática jurídica
- http://www.lared.com.ve__
- <http://laguna.fmedic.unam.mx/>__
- <http://maps.vix.com/tsi/>__
- http://www.mercadeoglobal.com__
- www.mecon.gov-infoleg
- <http://www.maccare.com.ar/espanol.htm>
- Miami University
- Miscellaneous Cyberlaw
- NetEthics
- Netlitigation
- Netwatchers Cyberzine
- North Carolina Central University - School of Law - Cyberlaw
- New York Times CyberLaw
- <http://www.neotrace.com>
- www.news.com
- Organización Mundial de la Propiedad Intelectual (OMPI - WIPO)
- Organización Mundial del Comercio (OMC)
- ORGANIZACIÓN MUNDIAL DE DERECHO E INFORMÁTICA
- Office of Information and Privacy
- <http://www.portaldeabogados.com.ar/derechoinformatico/>
- Privacy International
- http://www.ram.com.mx/srvicios/Manual_INTERNET/documento/Spam.htm
- Richmond Journal of Law and Technology
- <http://www.redetel.gov.ar/>

- <http://www.ram.com.mx/>_
- www.Spam.abuse.net
- SpamCon Foundation
- [_http://www.senado.gov.ar/](http://www.senado.gov.ar/)
- State Bar of Texas - The Computer Law Review and Technology Journal
- <http://www.saulo.net/pub/tcpip/b.htm#dr-2>
- www.secom.gov.ar
- <http://www.sinectis.com.ar/seguridad/spam.html#spam>
- Tech Law Journal
- The Anonymizer
- The Internet Junkbuster
- The Link Controversy Page
- <http://www.ucm.es/BUCM/cee/doc/9909/9909.htm>
- UCLA Online Institute for Cyberspace Law and Policy
- <http://www.ulpiano>
- University of California, Berkeley - Berkeley Center For Law & Technology
- University of Florida College of Law - Journal of Technology Law and Policy
- V-Lex Argentina_
- Virginia Journal of Law and Technology
- <http://vip.interplanet.es/faq2/general.htm>
- Weblaw FAQ
- Weikers and Co.
- William and Mary School of Law - Journal of On-Line Law
- <http://wyden.senate.gov/>
- www.yahoo.com.ar
- <http://www.zur2.com/users/fipa/objetivos/leyextran/cnudmi.htm>

Spam

Concepto

- Es un abuso en el correo electrónico
- Consiste en el envío masivo de mensajes de correo comercial y publicitario
- A través de correo electrónico
- Práctica muy utilizada por empresas que comienzan en Internet

Consecuencias

- Satura los registros de correo
- Destruye servidores de correspondencia
- Demora la entrega de *e-mail* por horas
- Aumenta también los costos de usuarios
- Aumenta también los costos de proveedores de servicios de Internet.

Distintas denominaciones

- Junk mail: correspondencia indeseada que suele llegar por medio del correo regular.
- Spamming: práctica de enviar correos electrónicos en forma masiva.
- Correo basura: es el correo que no nos interesa que satura nuestro servidor.
- UCE: unsolicited commercial email, o correo comercial no solicitado.

Origen de la palabra «spam»

- Se le atribuye el origen de la palabra «spam» a la canción de la comedia británica Monty Python.

¿En qué consiste ?

Spammer ⇒ **Armado de listas masivas de direcciones de correo**

⇒ **Y de software especial**



Envía muchas copias de un mismo mensaje



A multitud de usuarios desconocidos



Estos mensajes sirven para hacer publicidad ⇒ **de productos**

⇒ **de eventos**

⇒ **de una página web**

⇒ **de un servicio**

⇒ **de una idea**

¿Cómo obtienen los Spammers los emails de sus víctimas?

- Compra de direcciones
- Suscripciones a listas de distribución falsas
- Robots que escanean las paginas web
- Robots que escanean los grupos de noticias

Problemas provocados por el spam

- El destinatario asume el costo de la publicidad enviada por email.
- Pérdida de tiempo por parte de la víctima del spam.
- Disminuye la capacidad de almacenamiento en el buzón del usuario.
- Satura el servidor de dicho usuario.
- La víctima debe pagar mas por el tiempo de conexión a Internet en el caso de acceder por vía telefónica.

Distintos Sistemas

- Sistema de Opt-Out: permite a los usuarios solicitar que sus datos sean excluidos de las bases de datos utilizadas por los spammers.
- Sistema Opt-In: quien pretenda enviar mensajes comerciales deberá contar con la autorización expresa del destinatario.

El Spam en números

- Año 2002 se enviaron 31.000 millones
- Año 2006 se enviaron 61.000 millones

15. Documentación complementaria

ANTEPROYECTO DE LEY DE PROTECCIÓN DEL CORREO ELECTRÓNICO ANTEPROYECTO DE LEY EL SENADO Y LA CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA, REUNIDOS EN CONGRESO SANCIONAN CON FUERZA DE LEY LEY DE PROTECCIÓN DEL CORREO ELECTRÓNICO

Artículo 1º: Se entiende por correo electrónico 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.

Artículo 2º: A los efectos legales, el correo electrónico se equipara a la correspondencia epistolar. La protección del correo electrónico abarca su creación, transmisión y almacenamiento.

Artículo 3º: Cuando el correo electrónico sea provisto por el empleador al trabajador en función de una relación laboral, se entenderá que la titularidad del mismo corresponde al empleador, independientemente del nombre y clave de acceso que sean necesarias para su uso.

El empleador se encuentra facultado para acceder y controlar toda la información que circule por dicho correo electrónico laboral, como asimismo a prohibir su uso para fines personales.

El ejercicio de estas facultades por parte del empleador, así como las condiciones de uso y acceso al correo electrónico laboral, deberá ser notificado por medio fehaciente al trabajador, al momento de poner a su disposición el correo electrónico o en cualquier oportunidad posterior, como requisito previo a su ejercicio.

El empleador deberá asimismo, notificar fehacientemente al empleado su política respecto del acceso y uso de correo electrónico personal en el lugar de trabajo.

Artículo 4º: Modificase los artículos Nº 153 y 155 del Código Penal, los que quedan redactados de la siguiente forma:

Artículo 153: Será reprimido con prisión de 15 días a 6 meses, el que abriere indebidamente una carta, un correo electrónico, un pliego cerrado o un despacho telegráfico, telefónico o de otra naturaleza que no le esté dirigido; o se apoderare indebidamente de una carta, de un correo electrónico, de un pliego, de un despacho o de otro papel privado, aunque no esté cerrado; o suprimiere o desviare de su destino una correspondencia que no le esté dirigida.

Se le aplicará prisión de 1 mes a 1 año, si el culpable comunicare a otro o publicare el contenido de la carta, correo electrónico, escrito o despacho.

Artículo 155: El que, hallándose en posesión de una correspondencia, un correo electrónico, un pliego cerrado o un despacho telegráfico, telefónico o de otra naturaleza no destinados a la publicidad, los hiciere publicar indebidamente, aunque hayan sido dirigidos a él, será reprimido con multa de \$ 1.500 a \$ 90.000, si el hecho causare o pudiere causar perjuicios a terceros.

Artículo 5º: Comuníquese al Poder Ejecutivo Nacional.

PROYECTO DE LEY DE DELITOS INFORMÁTICOS - APROBADO POR LA CÁMARA DE DIPUTADOS EL 8 DE AGOSTO DE 2002 Y REMITIDO AL HONORABLE SENADO TEXTO APROBADO Y REMITIDO AL SENADO- ACTUALMENTE A ESTUDIO DESDE EL 3.03.2003 EN LA COMISIÓN DE JUSTICIA Y ASUNTOS PENALES Y EN LA COMISIÓN DE EDUCACIÓN, CULTURA Y CIENCIA Y TECNOLOGÍA

Número de Proyecto 64/02 Tipo de Proyecto: PROYECTO DE LEY

Buenos Aires, 8 de agosto de 2002

Al Señor Presidente del Honorable Senado

Tengo el honor de dirigirme al señor Presidente, comunicándole que esta Honorable Cámara ha sancionado, en sesión de la fecha, el siguiente proyecto de ley que paso en revisión al Honorable Senado. El Senado y Cámara de Diputados,...

Artículo 1º- A los fines de la presente ley se entiende por:

Sistema informático: todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.

Dato informático o información: toda representación de hechos, manifestación de o conceptos en un formato que puede ser tratado por un sistema informático o de banda magnética.

Art. 2°- Acceso no autorizado: Será reprimido con pena de prisión de quince días a seis meses, si el hecho no constituye un delito más severamente penado, el que ilegítimamente ya sabiendas accediera por cualquier medio, a un sistema o dato informático, sin que medie autorización del propietario o excediéndose de los límites de la autorización conferida.

La pena será de un mes a un año de prisión si el autor revelare, divulgare o comercializare la información accedida ilegítimamente.

Art. 3°- Espionaje informático. Será reprimido con prisión de un mes a un año, si el hecho no constituye un delito más severamente penado, el que interceptare, interfiriere o accediere a un sistema informático para obtener datos de forma no autorizada, violando la reserva o secreto de la información de dicho sistema. La pena será de un año a cuatro años de prisión si los datos o la información obtenida constituyere secreto político o militar concerniente a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación.

En los supuestos de los dos párrafos anteriores, la pena se elevará al doble tanto en su mínimo como en su máximo si se revelaren, divulgaren o comercializaren los datos o la información obtenida.

Art. 4°- Daño o sabotaje informático. Será reprimido con prisión de seis meses a cuatro años, si el hecho no constituye un delito más severamente penado, el que maliciosamente, destruyere, inutilizare, modificare, borraré, hiciere inaccesible o de cualquier modo y por cualquier medio, obstaculizare el funcionamiento normal de un sistema o dato informático.

Si el hecho pusiere en peligro la seguridad de una nave, aeronave, tren, o cualquier otro medio de transporte público de personas o de cargas, o el normal funcionamiento de las comunicaciones, de la provisión de agua, del suministro de electricidad, de la prestación del servicio de salud o de cualquier otro servicio público, la pena de prisión será de tres a diez años.

Art. 5°- Piratería informática. Será reprimido con prisión de un mes a seis años el que se apropiare, descargue o usare, indebidamente la información contenida en un sistema informático. Si la información constituyere secreto político o militar concerniente a la seguridad, a los medios de defensa o a las relaciones exteriores de la Nación, la pena será de uno a seis años de prisión.

Art. 6°- Fraude informático: Será reprimido con prisión de uno a seis años, el que con ánimo de lucro y valiéndose de cualquier ardid o engaño, perjudicare patrimonialmente a otro mediante la utilización de un sistema informático, sea modificando datos, sea introduciendo datos falsos o verdaderos o cualquier elemento extraño que sortee los procedimientos de seguridad del sistema.

La pena será de dos a seis años de prisión en los siguientes casos:

1. Si el perjuicio en alguna administración pública.
2. Cuando se obtuviere en provecho propio o de tercero el desvío de fondos provenientes de cuentas corrientes, cajas de ahorro, plazos fijos, valores en custodia o cualquier otro tipo de activo financiero.
3. Cuando para sí o para tercero se simulare la realización de pagos no efectuados en realidad, o la existencia de bienes, créditos o deudas.

Art. 7°- Medios destinados a cometer delitos. Será reprimido con prisión de tres meses a tres años, quien entregare a otro, distribuyere, vendiere o publicitare equipos de cualquier índole o programas de computación destinados a facilitar la comisión de los delitos previstos en la presente Ley.

Art. 8°- Cuando el autor o responsable de los ilícitos antes mencionados 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 de la condena.

Art. 9°- En todos los casos de los artículos anteriores, si el autor de la conducta fuese el responsable de la custodia, operación, mantenimiento o seguridad de un archivo, registro, sistema o dato informático, la pena se elevará a tercio del máximo y la mitad del mínimo.

Art. 10.- Comuníquese al Poder Ejecutivo.

Dios guarde al señor Presidente.

EDUARDO O. CAMAÑO - Juan Estrada

Monty Python's Spam sketch

- Scene: A cafe. One table is occupied by a group of Vikings with horned helmets on. A man and his wife enter.
- Man (Eric Idle): You sit here, dear.
- Wife (Graham Chapman in drag): All right.
- Man (to Waitress): Morning!
- Waitress (Terry Jones, in drag as a bit of a rat-bag): Morning!

- Man: Well, what've you got?
- Waitress: Well, there's egg and bacon; egg sausage and bacon; egg and spam; egg bacon and spam; egg bacon sausage and spam; spam bacon sausage and spam; spam egg spam spam bacon and spam; spam sausage spam spam bacon spam tomato and spam;
- Vikings (starting to chant): Spam spam spam spam...
- Waitress: ...spam spam spam egg and spam; spam spam spam spam spam spam baked beans spam spam spam...
- Vikings (singing): Spam! Lovely spam! Lovely spam!
- Waitress: ...or Lobster Thermidor a Crevette with a mornay sauce served in a Provencale manner with shallots and aubergines garnished with truffle pate, brandy and with a fried egg on top and spam.
- Wife: Have you got anything without spam?
- Waitress: Well, there's spam egg sausage and spam, that's not got much spam in it.
- Wife: I don't want ANY spam>!
- Man: Why can't she have egg bacon spam and sausage?
- Wife: THAT'S got spam in it!
- Man: Hasn't got as much spam in it as spam egg sausage and spam, has it?
- Vikings: Spam spam spam spam (crescendo through next few lines)
- Wife: Could you do the egg bacon spam and sausage without the spam then?
- Waitress: Urgghh!
- Wife: What do you mean 'Urgghh'? I don't like spam!
- Vikings: Lovely spam! Wonderful spam!
- Waitress: Shut up!
- Vikings: Lovely spam! Wonderful spam!
- Waitress: Shut up! (Vikings stop) Bloody Vikings! You can't have egg bacon spam and sausage without the spam.
- Wife (shrieks): I don't like spam!
- Man: Sshh, dear, don't cause a fuss. I'll have your spam. I love it. I'm having spam spam spam spam spam spam spam baked beans spam spam spam and spam!
- Vikings (singing): Spam spam spam spam. Lovely spam! Wonderful spam!
- Waitress: Shut up!! Baked beans are off.
- Man: Well could I have her spam instead of the baked beans then?
- Waitress: You mean spam spam spam spam spam spam... (but it is too late and the Vikings drown her words)
- Vikings (singing elaborately): Spam spam spam spam. Lovely spam! Wonderful spam! Spam spa-a-a-a-a-am spam spa-a-a-a-a-am spam. Lovely spam! Lovely spam! Lovely spam! Lovely spam! Lovely spam! Spam spam spam spam!

6. Legislación Extranjera

➤ Alemania

Ley de Firma Digital de la República Federal Alemana

Ordenanza Reglamentaria de la Ley de Firma Digital de Alemania

➤ Australia

Electronic Transactions Act N° 162

Ley 28

➤ Naciones Unidas

Ley Modelo de las Naciones Unidas sobre Comercio Electrónico

Ley Modelo de las Naciones Unidas sobre Firma Electrónica

➤ Austria

Federal Electronic Signature Law

➤ Canadá

Uniform Electronic Commerce Act

➤ Brasil

Decreto 3587 - Infraestructura de Clave Pública del Poder Ej.Federal de Brasil
Anteproyecto Ley Comercio Electrónico, Docum. y firma digital Brasil

➤ Chile

Ley de Delitos Informáticos de Chile
Decreto de Firma Digital para la Administración del Estado de Chile
Ley 19799 sobre Firma Electrónica de Chile

➤ Colombia

Ley 527/99 de Mensajes de Datos, Comercio Electrónico y Firma Digital de Colombia
Decreto 1747 Reglamentario de la ley 527 de Colombia
Resolución 26930 de Entidades de Certificación de Colombia
Ley 679 - Abuso y Pornografía de Menores en Internet

➤ Costa Rica

Ley 8131 de Costa Rica - Contempla los Delitos Informáticos
Ley 8148 de Costa Rica - Incorpora normas al Código Penal en materia de Delitos Informáticos_

➤ Republica Checa

Act 227 of June 29, 2000 - Electronic Sinature And Amendements to certain other legislation

➤ Ecuador

Ley de Comercio Electrónico, Firmas y Mensajes de Datos de Ecuador

➤ EE.UU.

Electronic Signatures in Global and National Commerce Act.
The Digital Millennium Copyright Act of 1998 ([The Library of Congress](#))
Ley del Estado de Utah sobre Firma Digital
Ley de Firma Digital del Estado de Nueva York
USA-PATRIOTIC Act of 2001 - 24.10.2001 (Legal Information Institute-Cornell Law School)_

➤ El Salvador

Ley de simplificación Aduanera

➤ España

Nombres de Dominio. Orden 662/2003 del 18 de Marzo de 2003 que aprueba el Plan Nacional de Nombres de Dominio Internet bajo el Código de País correspondiente a España "es"
Firma Electrónica. Real Decreto 14/1999 - Firma Electrónica en España
Sociedad de la Información y Comercio Electrónico. Ley 34 de Servicios de la Sociedad de la Información y Comercio Electrónico del 11.07.2002

➤ Francia

Ley Francesa de Firma Electrónica
Loi N° 88 relative a la fraude informatique

➤ Guatemala

Proyecto de Ley de Comercio Electrónico y Firma Digital de Guatemala

➤ Inglaterra

Electronic Communicatios Act 2000 Chapter c.7
The Electronic Signatures Regulations 2002-N° 318

➤ Italia

Ley Italiana de Documento Informático

➤ Japón

Ley Japonesa de Firma Digital

➤ **Malasia**

Digital Signature Bill

➤ **Méjico**

Código Penal Federal de Méjico - Delitos Informáticos

Código Penal Estado Sinaloa - Méjico - Art.217 - Delito Informático

➤ **Panamá**

Ley 43 de Firma Digital de Panamá

➤ **Perú**

Ley 27269 del Perú de Firma y Certificado Digital

Ley 27310 - Modifica art.11 ley 27269

Decreto Reglamentario ley de Firma y Certificado Digital

Ley 27291 del Peru que modifica el Código Civil - Medios Electr.y Firma Digital

Ley 27309 de Delitos Informáticos del Perú

Ley 27419 sobre Notificación por Correo Electrónico del Perú

Ley 27444 Notificación por Correo Electrónico en los Procedim. Administrativos

➤ **Portugal**

Ley Portuguesa de Firma Digital

➤ **República Dominicana**

Ley 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales de República Dominicana – Versión en Español

➤ **Singapur**

Ley de Comercio Electrónico (texto en Ingles)

Ley de Comercio Electrónico (traducción libre en español)

➤ **Uruguay**

Ley 16736 - Expediente Electrónico

➤ **Venezuela**

Ley sobre Mensajes de Datos y firma Electrónicas de Venezuela

Ley Especial sobre los Delitos Informáticos N° 48 de Venezuela_

