PROTECCION DE DATOS
Y DELITOS INFORMATICOS[(*)]

Dra. Esc. María José Viega[(**)]

CONTENIDO

1. Introducción. 2. Concepto y principios en materia de protección de datos. 2.1 Principios en materia de protección de datos. 2.2 Derechos del titular de los datos. 2.3 Habeas data. **3. Privacidad en Internet**. 3.1 Aspectos técnicos. 3.2 Situación de la Unión Europea y EEUU. 3.3 Situación en el MERCOSUR. **4. Los delitos informáticos**. 4.1 Características de los sujetos activos y pasivos. 4.2 Acceso no autorizado a sistemas informáticos: "tarea" de Hackers. 4.3 Violación a la intimidad. 4.4. Delitos informáticos en el Derecho Uruguayo. 4.5 Aplicabilidad de los artículos del Código Penal Uruguayo. **5. Conclusiones**.

(*) Ponencia presentada al III Congreso Internacional de Derecho. Bolivia, 10 al 13 de setiembre de 2003 y publicada en el Libro de Memorias de dicho Congreso.

(**) Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UR). Aspirante a Profesor Adscripto de Informática Jurídica en la misma Universidad. Profesora adjunta en el curso de Derecho Telemático y Profesora en el curso en línea Derecho del Ciberespacio en la UR. Cursos del Posgrado de Derechos Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Miembro de la Comisión de Derecho Informático y Tecnológico de la Asociación de Escribanos del Uruguay. Miembro del Instituto de Derecho Informático (UR). Autora de múltiples trabajos de su especialidad. E-mail: mjviega@viegasociados.com

1. Introducción

Cuando pensamos en la problemática y en los desafíos que el ciberespacio plantea, nos encontramos con algunos elementos que podemos calificar como nuevos. Pero en realidad Internet, a redimensionado problemas tradicionales, que si bien estaban regulados jurídicamente, dicha regulación deberá ser actualizada, si es que ya no lo ha sido, para incluir esas nuevas facetas que las tecnologías nos plantean.

Analizaremos en esta oportunidad, en primer lugar, la cuestión del derecho a la intimidad, teniendo en cuenta los riesgos personales que plantean los grandes bancos de datos personales, y la posibilidad del entrecruzamiento de la información que contienen.

En estas circunstancias, surge la libertad informática como un nuevo derecho de autotutela de la propia identidad informática. Este derecho otorga a las personas la posibilidad de controlar sus propios datos. El derecho a la intimidad a evolucionado hacia un nuevo concepto: la privacidad, la cual se ve seriamente violentada por las nuevas tecnologías, al punto tal que se ha llegado hablar de la existencia de un hombre de cristal.

"Las posibilidades tecnológicas de conseguir un "ciudadano de cristal" son cada vez más grandes, no sólo en el ámbito del manejo de datos sensibles de carácter tradicional (como la filiación política, la pertenencia sindical, la confesión religiosa, el grupo humano al que se pertenece, las costumbres sexuales, las apetencias personales y sociales, el historial clínico y penal, las cuentas bancarias, la situación económica, los viajes, etc.) sino también mediante la digitalización de información genética, lo que permitirá crear un cuadro completo de los aspectos más íntimos de la constitución física, hereditaria y hasta psicológica de alguien. Además, su personalidad puede hacerse transparente para fines de mercado (como para establecer pautas de consumo, etc.) u otras pudiendo llegar a generar una auténtica "estigmatización electrónica"[1].

Otro aspecto negativo del desarrollo tecnológico está dado por la existencia de los delitos informáticos. Ellos son la consecuencia de las nuevas posibilidades que la informática plantea, ya que las computadoras nos ofrecen otras formas de infringir la ley, y por lo tanto hoy se pueden cometer delitos tradicionales de una manera muy sofisticada. Por esta razón es importante dilucidar si existen o deben existir delitos informáticos específicos, lo que implica tener en cuenta si las figuras tipificadas en nuestros Códigos Penales tradicionales se adecuan a estos, o si por el contrario necesitaremos tipificar nuevos delitos.

---

[1] DELPIAZZO Carlos. "Dignidad Humana y Derecho".Universidad de Montevideo. Facultad de Derecho. Montevideo, 2001. Página 124.

2. Concepto y principios en materia de protección de datos.

La Protección de Datos es un derecho fundamental de los ciudadanos, que se concreta, al decir de María del Carmen Almada en "el amparo debido a los mismos frente a la utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esa forma, confeccionar una información que identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad"[2].

Es interesante aclarar que cuando nos referimos a la protección de datos personales, en realidad nos estamos refiriendo no a lo protección del dato en sí mismo, sino del sujeto que es titular de dicho dato.

"El legítimo interés constitucional de protección de las personas, se limita en la medida en que la sociedad en general requiere del individuo ciertas informaciones. El conflicto se agrava en la medida que crece el valor económico que poseen los datos sobre las personas. Compañías de seguro, bancos nacionales e internacionales, la empresa privada o la prensa solicitan continuamente datos sobre futuros o actuales clientes. Por parte de la doctrina se ha propuesto, incluso, el reconocimiento de un nuevo derecho de propiedad sobre los datos de carácter personal, que se han convertido en una mercancía vital y de gran valor en la era del *direct-marketing*. Lo que resulta claro es el carácter invasor de las tecnologías de la información, que se apoderan de la vida privada, la traducen en datos de fácil circulación y en una mercancía muy valiosa[3].

Atendiendo su confidencialidad, podemos decir que los datos personales pueden ser:

- públicos y
- privados
    - íntimos y
    - secretos

reservados

[2] ALMADA, María del Carmen. "Encuentro Iberoamericano de Protección de Datos (El Escorial, 20 y 21 de Mayo de 2002). Derecho Informático. Tomo III. Correspondiente al año 2002. Fundación de Cultura Universitaria. Montevideo, agosto, 2003. Página 542.

[3] ARAGÓN REYES, Manuel y FERNÁNDEZ ESTEBAN María Luisa. "Incidencia de Internet en los Derechos Fundamentales". Edita Banco Santander Central Hispano – Asesoría Jurídica del Negocio – C/ Alcalá 49 – 28014 Madrid.

Públicos: “aquellos datos personales que son conocidos por un número cuantioso de personas, sin que el titular pueda saber, en todos los casos, la fuente o la forma de difusión del dato, ni, por la calidad del datos, pueda impedir que, una vez conocido, sea libremente difundido dentro de unos límites respecto de respeto y convivencia cívicos”[4].

Privados: estos datos son los que en determinadas circunstancias la persona se ve obligada a proporcionarlos, no realizándose difusión de los mismos y respetando la voluntad de secreto entre su titular y la entidad a quien se entregan.

Intimos: son los datos que el individuo puede proteger de su difusión frente a cualquiera, pero que, esté obligado por ley a brindarlos cumpliendo sus obligaciones cívicas.

Secretos: los datos que el ciudadano no estará obligado a dar a nadie, salvo casos excepcionales, expresamente regulados en las leyes. La doctrina los ha denominado como “datos sensibles”.

Reservados: aquellos datos que bajo ningún concepto está obligado el titular a darlos a conocer a terceros, si no es su voluntad. Y no admiten excepciones de ningún tipo.

Los datos personales se protegen mediante el derecho a la intimidad, que analizaremos en el punto siguiente. Es importante encontrar en este tema el justo equilibrio entre la libertad de expresión (libertad de opinión, libertad de recibir o comunicar información) y el derecho a la privacidad.

2.1 Principios en materia de protección de datos

La recolección de datos debe realizarse en base a una serie de principios básicos que, según Correa, son los enumerados a continuación y surgen de un estudio de derechos comparado son los siguientes[5]:

1. Justificación social: la recolección de datos debe tener un propósito general y usos específicos socialmente aceptables.

2. Limitación de la recolección: los datos deben ser recolectados por medios lícitos, con conocimiento y consentimiento de la persona, o con autorización legal, y deberán limitarse al mínimo necesario para alcanzar el fin perseguido por la recolección.

---

[4] DAVARA RODRIGUEZ, Miguel Ángel. “Derecho Informático”. Editorial Aranzadi, Pamplona España, 1993. Página 50.

[5] CORREA Carlos, NAZAR ESPECHE Feliz A., CZAR DE ZALDUENDO Susana y BATTO Hilda N. “Derecho Informático”. Depalma, Buenos Aires, Argentina, 1987. Página 257.

3. Calidad o fidelidad de la información: los datos que se recolectan deberán ser: exactos, completos y actuales. La finalidad es que no se induzca en error a terceros con datos erróneos, y por eso las legislaciones otorgan al titular de los datos el derecho de rectificación, cancelación o actualización de los mismos.

4. Especificación del propósito o finalidad: a la hora de recabar los datos, debe informarse para que se están recabando, y posteriormente no podrán ser utilizados para una finalidad diferente.

5. Confidencialidad: el acceso a los datos por parte de terceros se podrá realizar con consentimiento del titular de los datos o con autorización legal.

6. Salvaguarda de la seguridad: la entidad responsable del registro de datos personales tiene la obligación de adoptar medidas de seguridad adecuadas para proteger los mismos contra pérdidas, destrucciones o accesos no autorizado.

7. Política de apertura: "tiende a garantizar la transparencia de las acciones de la administración pública y privada en relación a los procedimientos, desarrollo y prácticas concernientes al proceso de datos personales. Esta transparencia queda asegurada por el conocimiento por parte del público de la existencia, fines, usos y métodos de operación de los registros de datos personales"[6].

8. Limitación en el tiempo: los datos no deben conservarse más tiempo del necesario para alcanzar los fines para los cuales fueron recolectados.

9. Control: es importante la existencia de un organismo de control responsable de la efectividad de los principios contenidos en la legislación.

10. Participación individual: consagra el derecho de acceso a los datos que se concede al individuo.

2.2 Derechos del titular de los datos

Existen una serie de derechos que poseen las personas en relación a sus datos, que enumeramos a continuación:

a) Derecho de acceso: es el derecho de cada uno de nosotros a conocer que información poseen las instituciones.

---

[6] CORREA Carlos, NAZAR ESPECHE Feliz A., CZAR DE ZALDUENDO Susana y BATTO Hilda N. "Derecho Informático". Ob. Cit.

Para Correa[7] el este derecho comprende:

> Obtener información de la entidad responsable de los datos, acerca de la existencia de datos que le conciernen.
>
> Ser informado dentro de un tiempo razonable y de manera comprensible.
>
> Oponerse a cualquier dato que le concierna y a que esa oposición quede registrada.
>
> Obtener que los datos relativos a su persona sean suspendidos, rectificados o completados,
>
> Ser informado de las razones por las cuales se deniega el acceso o si el mismo no es concedido en tiempo y forma razonable.

b) Derecho de rectificación: "dicho derecho permite solicitar al interesado una modificación en los términos de alteración o ampliación, o una suspensión o cancelación de aquellos datos que, referidos a su persona, considere como inexactos o irrelevantes"[8].

c) Derecho de uso de acuerdo al fin: consiste en que el titular de los datos pueda exigir que los mismos sean utilizados únicamente con el fin para el cual se los solicitaron.

d) Derecho de prohibición de interconexión de bases de datos: uno de los principales problemas que plantea la informática es la facilidad con que los archivos pueden compartirse y cruzarse. De forma tal que esta prohibición es de suma importancia.

Y también es relevante la prohibición de ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal sensibles, son considerados tales los que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

La autodeterminación informativa, reconoce a la persona la facultad de decidir cuando y cómo está dispuesta a permitir que sea difundida su información personal o a difundirla ella misma, esto es, la facultad de la persona de controlar y conocer los datos que sobre ella se encuentran en soportes informáticos o susceptibles de tratamiento automatizado[9].

---

[7] CORREA Carlos, NAZAR ESPECHE Feliz A., CZAR DE ZALDUENDO Susana y BATTO Hilda N. "Derecho Informático". Ob. Cit., página 261.

[8] TÉLLEZ, Julio. "Derecho Informático". Segunda Edición. Mc Graw-Hill, México, 1998. Página 71.

[9] CORREA Carlos, NAZAR ESPECHE Feliz A., CZAR DE ZALDUENDO Susana y BATTO Hilda N. "Derecho Informático". Ob. Cit.

También conocida como libertad informática, se la ha definido como “el derecho de disponer de la información, de preservar la propia identidad informática o, lo que es lo mismo, de consentir, controlar y rectificar los datos informativos concernientes a la propia personalidad; al derecho de informar y de ser informado se ha agregado el derecho de proteger la libertad de la información como u bien personal”[10].

2.3 Habeas data

Si bien no es un punto en el que vamos a profundizar, no podemos dejar de mencionar que, el ejercicio de los derechos enunciados en el punto anterior, podrán llevarse a cabo mediante el procedimiento denominado “habeas data”. Dicho proceso permite a las personas poseer una defensa de los derechos que se pretenden proteger.

3. Privacidad en Internet

Hoy por hoy se entiende que la vida privada no se limita a la intimidad, sino que este concepto ha sido sustituido por uno más general como es el de privacidad[11]. Internet es una amenaza en la difusión de elementos relativos a la persona, por diferentes características que encontramos en ella, las que analizaremos una a una.

Al buscar la regulación adecuada para este tema, entendemos que se deben ponderar dos intereses diferentes, por un lado la protección de la vida privada y por otro el interés de la sociedad de la circulación de la información. Este aspecto tiene estrecha relación con la libertad de expresión y de información, así como también de la seguridad que podemos tener en nuestras comunicaciones y las herramientas que pueden ser útiles para ello[12].

La Red es un medio de comunicación polifacético, debido a la existencia de múltiples medios para distribuir información. Ellos son: el correo electrónico, los boletines, los foros de discusión y también la información presente en la www[13].

3.1 Aspectos técnicos

[10] FROSSINI Vittorio. “Informática y Derecho” . Editorial Temis. Bogotá, 1988. Página 35.
[11] DELPIAZZO, Carlos. “Dignidad Humana y Derecho”. Universidad de Montevideo. Facultad de Derecho. Montevideo, 2001.
[12] VIEGA, María José. “Los Derechos Humanos en Internet”. Ponencia presentada al IX Congreso Iberoamericano de Derecho e Informática. Costa Rica, 2002.
[13] VIEGA, María José. “Privacidad en Internet”. Segundas Jornadas Internaciones del Instituto de Derecho Informático. Montevideo, 2000.

Para enfrentar este desafío debemos tener en cuenta los siguientes elementos[14]:

a) la infraestructura de Internet está basada en datos personales (IP),

b) los instrumentos técnicos utilizados, los software de navegación, por ejemplo, que envían más información de la requerida para realizar una conexión,

c) y la cantidad de datos que nos solicitan para realizar actividades comerciales en línea.

Se nos plantea una dependencia entre la utilización de Internet y el dar datos personales. Y esta relación está signada por la desigualdad entre el proveedor y el usuario. Otro elemento relevante es la desinformación del usuario, que la mayoría de las veces no tienen conocimiento que sus datos se han recopilado.

Existen tres elementos de fundamental importancia con relación al manejo de datos, que son:

1) Las **Cookies:** podemos definirlas como fichas de información automatizada, las cuales se envían desde un servidor web al ordenador del usuario, con el objetivo de identificar en el futuro las visitas al mismo sitio. Las cookies son una potente herramienta para almacenar o recuperar información empleada por los servidores web debido al protocolo de transferencia de ficheros (http). Los riesgos ya los conocemos: recopilación de gustos, preferencias, hábitos, nombre y contraseña y además que algún experto podría manipular estos archivos[15].

2) Los **Navegadores**: que suelen envíar más información que la necesaria para conectarse, como por ejemplo el tipo y lengua del navegador, que otros programas se encuentran instalados, cual es el sistema operativo del usuario, cookies, etc

3) **Contenidos Activos**: ejecución de programas con este tipo de contenidos, como por ejemplo Java y ActiveX.

3.2. Situación de la Unión Europea y EEUU

[14] ARAGÓN REYES Manuel y FERNANDEZ ESTEBAN María Luisa. Incidencia de Internet en los Derechos Fundamentales. Edita Banco Santander Central Hispano – Asesoría Jurídica del Negocio – C/ Alcalá 49 – 28014 Madrid.

[15] MENDOZA LUNA, Amílcar. “Los cookies: ¿amenaza a la privacidad de información en la internet?. www.derecho.org/redi

Se han buscado distintas soluciones para este tema, a nivel de la **Unión Europea** encontramos[16]:

1. En el año 1996 el Libro Verde sobre la Protección de los Menores y de la Dignidad Humana en los Nuevos Servicios Audiovisuales y de Información. Distingue el contenido ilícito, que es aquel constitutivo de delito, que estará legislado en forma interna en cada país, del contenido nocivo o dañino, que es aquel que lo es para algunas personas, pero es legal, por ejemplo la pornografía.

2. Plan de Acción para el uso seguro de Internet, el cual se instrumenta a través del fomento de un uso responsable, esto es a través del etiquetado, clasificación y filtros; el impulso de la autorregulación, con el establecimiento de códigos de conducta por parte de los proveedores de Internet y por último la sensibilización a padres y profesores respecto a estos temas.

3. Directiva 95/46/CE sobre la Protección de personas físicas, tratamiento de datos personales y su libre circulación.

4. Directiva 97/66/CE sobre el Tratamiento de datos personales y protección de la intimidad en el sector telecomunicaciones (envío de datos a terceros países).

En **EEUU** en cambio se ha buscado la protección a través de la autorregulación. Lo que ha ocasionado problemas con los países europeos porque no lo consideran un país seguro para el envío de datos. Esto a llevado a que existan propuestas basadas en los principios de puerto seguro, en el año 1999, que no han prosperado[17].

Por otra parte, el **Grupo de Trabajo sobre protección de las personas** ha dictado una Recomendación 1/1999, en la cual se establece que:

1. el navegador debería informar al usuario que información pretende transferir y con que objeto,

2. cuando existen hipervínculos, el navegador debería indicar el sitio en su totalidad

[16] VIEGA, María José. “Privacidad en Internet” Ob. cit.
[17] ARAGON REYES Manuel y FERNANDEZ ESTEBAN María Luisa. Incidencia de Internet en los Derechos Fundamentales. Ob. cit.

3. las cookies deberían informar cuando se está enviando una cookie, que información pretende almacenar, con que objetivo y el período de validez.

Los acontecimientos del 11 de setiembre en EEUU ha llevado a que este país pretenda un estricto control sobre Internet. El gobierno de Estados Unidos no sólo se propone controlar Internet, incluyendo por supuesto los correos electrónicos, sino que también a solicitado a la Unión Europea, en la carta que se enviara el 16 de octubre de ese año, para que se reconsidere la legislación existente en materia de protección de datos. Además, se aprobó en el Senado la ley "Combating Terrorism Act of 2001, el 13 de setiembre de 2001, que multiplica las posibilidades de monitorización de las comunicaciones.

Pero este no es un propósito a largo plazo, sino que podemos leer con sorpresa en el Diario El Mundo español como a un joven de Valencia, que había enviado unos correos electrónicos haciendo bromas sobre Bin Laden, recibió un correo de la NSA (Agencia Nacional de Seguridad de Estados Unidos) diciendo que su cuenta de correo había sido bloqueada. Su cuenta pertenece a una empresa norteamericana en la que había trabajado, lo que facilitó que sus mensajes fueran detectados[18].

Tengamos presente que la comisión de la Unión Europea encargada de determinar la existencia de una red de espionaje de comunicaciones de EEUU llamada ECHELON, entregó un informe afirmativo al respecto[19].

3.3 Situación en el MERCOSUR

En el ámbito del Mercosur, la cuestión no sólo ha recibido acogimiento constitucional en Argentina, Brasil y Paraguay sino que los dos países citados en primer término han dictado leyes en la materia, siendo Argentina el único país del continente al cual la Comisión de la Unión Europea, por reciente decisión de 20 de junio de 2003, ha reconocido que "garantiza un nivel adecuado de protección por lo que respecta a los datos personales transferidos desde la Comunidad" (art. 1º)[20].

En **Argentina** se dictó la Ley de Habeas Data N° 25.326 de 20 de octubre del 2000. "Tanto los registros manuales como los automatizados

---

[18] http://www.elmundo.es/navegante/2001/09/24/esociedad/1001317628.html Privacidad. EEUU interviene un correo por bromear sobre Laden. J.M. Vilar.

[19] El Parlamento Europeo demuestra la existencia de Echelon. http://www.larazon.es/lared/laredesoias.htm y El Parlamento europeo reconoce la existencia de la red de espionaje Echelon.http://idg.es/pcworld/noticia.asp?id=18239

[20] Informe del Instituto de Derecho Informático acerca del proyecto de ley sobre protección de datos personales y derecho de habeas data a estudio de la Comisión de Constitución y Legislación de la Cámara de Senadores (carpeta 1050/2003 – Distribuido 2112/2003), presentado al Consejo de la Facultad de fecha 6 de agosto de 2003.

quedan incluidos en la norma. Esto último incluye bases de datos usadas “on line” para recopilar datos personales que incluyan cookies (por la referencia a datos “determinables”), números de identificadores, formularios web, correos electrónicos, bancos de datos que proveen informes a través de Internet, y cualquier otra forma de recopilación de datos en forma automatizada”[21].

Con relación a la problemática mirada desde Internet podemos destacar que:

a) La ley exige el consentimiento expreso y escrito motivo por el cual los sitios web que registren usuarios deberán tener la posibilidad de que el usuario otorgue su consentimiento en forma previa a realizar su registración, aceptando las condiciones de la misma. Los sitios que no realizan registro pero que captan datos deberán dejar claro cuales son las condiciones de uso del sitio a través de algún vínculo, para que el usuario esté informado de los datos que se recabarán.

b) Existen excepciones previstas en la ley para la exigencia del consentimiento, y una de ellas establece el fin estadístico, en estos casos cuando las cookies recopilen datos relacionados a las visitas a un sitio, si estos datos no se cruzan con otra información personal suministrada por el titular de los datos, no requeriría el consentimiento.

c) La dirección de correo electrónico no está incluida como dato básico del individuo (dentro de las excepciones) por lo cual la distribución de bases de datos de correos electrónicos (para realizar spam) requerirán el consentimiento del titular.

En **Brasil**[22], en virtud de la ley Nº 9.507 de 12 de noviembre de 1997, que consta de 23 artículos, se regula el derecho de acceso a informaciones de carácter personal y se disciplina el proceso de habeas data:

a) por el artículo 1 se considera de carácter público todo registro o banco de datos que contenga informaciones que sean o puedan ser trasmitidas a terceros o que no sean de uso privativo del órgano o entidad productora o depositaria de informaciones, regulándose con plazos la obligación de brindar información a los requirentes (artículo 2 y siguientes.; y

b) a partir del artículo 7 se regula la acción de habeas data en sus aspectos sustantivos y procesales.

---

[21] PALAZZI, Pablo “La nueva Ley de Habeas Data y protección de datos personales en Argentina”. Memorias del VIII Congreso Iberoamericano de Derecho e Informática. México, Noviembre del 2000.

[22] Informe del Instituto de Derecho Informático. Ob. Cit.

En **Uruguay** el Derecho a la intimidad, no está específicamente regulado, pero podemos entender que se encuentra reconocido a través del artículo 72 de la Constitución que establece: “La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno”.

En la medida que la intimidad consiste en que no se produzca ningún tipo de intromisiones en el ámbito reservado a la vida privada de los individuos, cabe hacer caudal también del artículo 10, cuyo inciso 1° dispone que “Las acciones privadas de las personas que de ningún modo atacan al orden público ni perjudican a un tercero, están exentas de la autoridad de los magistrados[23].

a) Decreto - Ley 15.672 - Ley de prensa. Consagra: libertad de expresión y comunicación de pensamientos y difusión de informaciones mediante la palabra, el escrito o la imagen, por cualquier medio de comunicación.

b) Pacto de San José de Costa Rica, ratificado Ley 15.837 de 1985. Convención Americana sobre Derechos Humanos firmada el 22 de noviembre de 1969 artículo 14, artículo 25 “toda persona afectada por informaciones inexactas o agraviantes emitidas en su perjuicio .... y que se dirijan al público en general” tiene derecho a efectuar su rectificación o respuesta.

c) Ley 16.011 - 19/12/1988 Acción de Amparo: “podrá constituirse en un instrumento eficaz de protección genérica de la libertad informática a fin de poder concretar formas de acceso, tales como la de saber que bases de datos existen, obtener respuesta afirmativa o negativa del responsable de una base de datos acerca de si existen datos personales del accionante, y obtener la versión exacta de tales datos en términos claros y accesibles a cualquier ciudadano”[24].

d) Ley 16.099[25] – 3/11/1989 Díctanse normas referentes a expresión, opinión y difusión, en comunicaciones e informaciones, consagradas por la Constitución. Esta ley se refiere a las libertades de prensa y de imprenta, al derecho de respuesta, a los delitos e infracciones cometidos por la prensa u otros medios de comunicación y al procedimiento a llevarse a cabo en esos casos.

---

[23] DELPIAZZO, Carlos. “Los derechos humanos ante las nuevas tecnologías. Ponencia presentada al I Congreso Mundial de Derecho e Informática (Universidad San Francisco de Quito, 15 al 18 de octubre de 2001).

[24] DELPIAZZO Carlos E. “Información, informática y Derecho”. Ediciones Jurídicas Amalio M. Fernández. Montevideo, 1989.

[25] http://www.parlamento.gub.uy/Leyes/Ley16099.htm

e) Ley 16.616[26] - 20 de octubre de 1994. Sistema Estadístico Nacional. El capítulo IV de esta ley se refiere a los principios de la recolección de datos, al secreto estadístico y a la difusión de la información.

4. Delitos Informáticos

Como mencionábamos al inicio los delitos informáticos constituyen un aspecto negativo de las tecnologías, que como hemos podido apreciar las herramientas informáticas, se constituyen en una herramienta poderosa a los efectos de violar la privacidad, pero también de causar otro tipo de daños.

Jijena Leiva los define como: "... *toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma*"[27].

La Organización para la Cooperación Económica y el Desarrollo (OECD) da una definición que es considerada como "abarcante" y lo define como: "*cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos*"[28].

Se ha dicho que los llamados delitos informáticos no constituyen una nueva categoría delictiva, sino que son los mismos delitos que ya se vienen castigando: delitos contra las personas, contra el honor, la libertad, la seguridad pública o la Nación. Se ha tratado de encuadrar los delitos informáticos dentro de los delitos como son: robo, hurto, fraudes, falsificaciones, estafa, sabotaje, etc, pero debemos analizar si las categorías tradicionales son adecuadas o no respecto a estas modalidades delictivas[29].

En mi opinión los delitos informáticos se pueden definir como toda conducta ilícita, sancionada por el derecho penal, para la realización de la cual se utilizan los medios informáticos, frutos de las nuevas tecnologías, ya sea como herramienta para la comisión del delito o como fin en sí mismo, afectando los datos contenidos en un sistema o la transmisión de los mismos.

---

[26] http://www.parlamento.gub.uy/Leyes/Ley16616.htm

[27] JIJENA LEIVA, Renato Javier: "La Criminalidad Informática": Situación de Lege Data y Lege Ferenda en Chile". Actas de III Congreso Iberoamericano de Informática y Derecho". Mérida, España.

[28] CORREA Carlos, NAZAR ESPECHE Feliz A., CZAR DE ZALDUENDO Susana y BATTO Hilda N. "Derecho Informático". Ob. Cit.

[29] VIEGA, María José. "Un nuevo desafío jurídico: los delitos informáticos". Ponencia presentada a ECOMDER 2000. Primer Congreso Internacional sobre Aspectos Jurídicos del Comercio Electrónico organizado por la Universidad de Buenos Aires. Mayo de 2000.

Ahora bien, ¿cual fue el primer delito informático que se cometió?. En 1964 Michael DERTOUZOS era estudiante en el MIT y realizaba cálculos para su tesis sobre uno de los primeros ordenadores de tiempo compartido del mundo, un cerebro central conectado a una pequeña cantidad de terminales sin cerebro que permiten a los individuos compartir el poder y la memoria de procesamiento del ordenador principal. Los responsables de los establecimientos universitarios decidieron que los profesores y los individuos privilegiados tuvieran la posibilidad de utilizar a otros que estaban utilizando el sistema cuando este estaba operando en su capacidad máxima. A los estudiantes se les aparecía de golpe un mensaje que decía "Ha sido usted desplazado por un usuario privilegiado" y el teclado quedaba muerto[30].

"En este contexto infofeudal de ricos y pobre fue donde una noche el irritado joven de dieciocho años al que llamaremos Ben Bitdiddle irrumpió silenciosamente en el sagrado corazón del ordenador, donde se almacenaban los nombres y los privilegios de los usuarios. Una vez que se apoderó del archivo que servía de contraseña, Ben moderno Robin Hood, procedió simplemente a invertir los privilegios, de modo que la gente común tuviera el poder de desplazar a las figuras importantes. A la mañana siguiente noté este hecho con incredulidad y alegría, pues mis compañeros y yo nos conectábamos y desalojábamos a todo el personal docente, incluido el director del laboratorio de informática. Tras divertirse un poco, reír, admirarse y sopesar qué podía significar este nuevo tipo de perversidad, la admiración del laboratorio convocó las inevitables reuniones para decidir la suerte del joven. Después de todo, había que imponerle un buen escarmiento. Finalmente, Ben recibió un a tibia reprimenda: había nacido el delito informático"[31].

Estos delitos han sido objeto de variadísimas clasificaciones, pero a nuestro criterio existen dos aspectos que se deben tener en cuenta: por un lado si la informática fue el instrumento o medio para cometer el delito; o si los sistemas informáticos fueron el fin u objetivo de los mismos.

4.1 Características de los sujetos activos y pasivos

Es importante destacar que no estamos frente a delincuentes comunes, por tal motivo resulta interesante determinar cuales son sus principales características.

Respecto a los sujetos activos podemos decir que son personas que poseen importantes conocimientos de informática. Hasta hace un tiempo se

[30] DERTOUZOS Michael L. "Que será. Como cambiará nuestras vidas el nuevo mundo de la informática".Planeta. Espala, 1997. Páginas 35 a 37.

[31] DERTOUZOS Michael L. "Que será. Como cambiará nuestras vidas el nuevo mundo de la informática". Ob. Cit., página 37.

decían que eran jóvenes, pero en la actualidad entendemos que este no es un aspecto determinante, si bien muchas veces los jóvenes violan sistemas informáticos con motivados por el desafío que implica, y no con fines dañinos, son los denominados harcker, a quien debemos distinguir de los crackers que su objetivo s{i consiste en causar daño. Dentro de este tipo de intrusos, vamos a encontrar a los preackers, que son quienes violan el sistema telefónico.

Otro aspecto en el que se ha hecho hincapié es en el trabajo que los mismos realizan, determinando que normalmente ocupan puestos estratégicos, en los cuales tienen acceso a información de carácter sensible (se los ha denominado *delitos ocupacionales* ya que se cometen por la ocupación que se tiene y el acceso al sistema.

Respecto al nivel educacional de lo mismos las opiniones se encuentran divididas, mientras algunos piensan que el nivel educacional no es indicativo, otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico. Y cuando de violar sistemas se trata, no dudo en que efectivamente tienen estas características.

Estos delitos se han calificado de "cuello blanco", porque el sujeto que comete el delito es una persona de cierto status socioeconómico.

Un aspecto interesante a destacar es que la opinión pública no considera delincuentes a estos sujetos, no los segrega, no los desprecia, ni los desvaloriza. Incluso el propio autor de estos delitos pretende distinguir entre el daño a las personas (que lo considera inmoral) del daño a las organizaciones, porque en este último caso sienten que “hacen justicia”, por lo cual se ha designado a este punto de vista como el *síndrome de Robin Hood*.

Respecto a los **Sujetos Pasivos** vamos a definirlo como el sujeto sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. Normalmente son grandes empresas, públicas o privadas, siendo los bancos de los más atractivos. La mayor parte de los delitos informáticos no son descubiertos o denunciados a las autoridades responsables, ya que los mismos tienen miedo de dejar al descubierto la falta de seguridad que poseen.

"Si hace unos años sólo las grandes empresas y las instituciones u organismos públicos eran objeto de incidentes de acceso no autorizado por terceros (hackers), ahora puede ser potencialmente víctima de los mismos cualquier familia o pequeña empresa que tenga una conexión más o menos permanente a Internet"[32].

[32] CREMADES Javier. FERNÁNDEZ-ORDOÑEZ Miguel Angel e ILLESCAS Rafael. “Régimen Jurídico de Internet”. RODRIGUEZ MOURULLO Gonzalo, ALONSO GALLO Jaime y LASCURAIN SANCHEZ Juan Antonio. Derecho Penal e Internet". Capítulo II. Ob. Cit., página 258.

4.2 Acceso no autorizado a sistemas informáticos: “tarea” de Hackers

El espionaje es la obtención de información a través de medios informáticos para ser utilizada posteriormente normalmente para la obtención de beneficios económicos de enorme magnitud.

El acceso puede darse en forma directa, por ejemplo cuando un empleado accede en forma no autorizada, estamos frente a un riesgo interno. Pero se puede acceder en forma indirecta, o sea a través de una terminal remota.

El delincuente puede aprovechar la falta de medidas de seguridad para obtener acceso o puede descubrirle las deficiencias a las medidas existentes de seguridad. A menudo, los hackers se hacen pasar por usuarios legítimos del sistema, esto suele suceder debido a la frecuencia en que los usuarios utilizan contraseñas comunes.

La fuga de datos consiste en la versión informática de las tradicionales prácticas de “espionaje industrial”

El acceso no autorizado a sistemas informáticos reviste diversas modalidades, que son:

Puertas falsas. Se trata de intromisión indebida a los sistemas informáticos aprovechando los accesos o “puertas” de entrada, que no están previstas en las instrucciones de la aplicación, pero que facilitan la revisión o permiten recuperar información en casos de errores de sistemas. También llamadas “puertas trampa” porque permiten a los programadores producir rupturas en el código y posibilitar accesos futuros.

Llave maestra (Superzapping). Consiste en el uso no autorizado de programas para modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en un sistema informático. El nombre proviene de un programa de utilidad que se llama superzap, que permite abrir cualquier archivo de una computadora aunque se halle protegido por medidas de seguridad.

Pinchado de líneas. Se realiza a través de la interferencia de las líneas telefónicas o telemáticas a través de las cuales se transmiten las informaciones procesadas en las bases de datos informáticas.

"Los hackers son individuos, frecuentemente jóvenes, que, aprovechando los defectos de seguridad y la vulnerabilidad de las redes informáticas, fundamentalmente de Internet, acceden sin autorización y de forma ilícita a un sistema informático desde un ordenador remoto, bien con el

solo objetivo de conseguir el acceso, bien con el fin ulterior de obtener infromación protegida (passwords o contraseñas, informaciones sobre tarjetas de crédito, secretos empresariales, etc.), o atacar un sistema o red provocando su paralización (como en los incidentes de denegación de servicio que más adelante trataremos), o dañando los datos almacenados"[33].

Para hablar de los hacker y las actividades que estos realizan, nos interesa realizar una clasificación del denominado "pirata informático"[34]:

Hacker**:** persona que disfruta explorando detalles de los sistemas programables y aprendiendo a usarlos al máximo, al contrario del operador común, que en general, se conforma con aprender lo básico.

Cracker: aquel que rompe con la seguridad de un sistema. El término fue acuñado por Hacker en 1985, oponiéndose al mal uso de la palabra Hacker por parte de la prensa.

Preaker: arte y ciencia de crackear la red telefónica para obtener beneficios personales (por ejemplo llamadas gratis de larga distancia).

Es de interés destacar que Internet es un caldo de cultivo para la actividad de estos sujetos, ya que la inseguridad de los software en cuanto a la existencia de puertas traseras, la cantidad de información que circula en la Red, la cual casi nunca está encriptada, e incluso los problemas del protocolo TCP/IP permiten que los internautas sean afectados cada vez con mayor frecuencia por este tipo de acciones.

Es así que dentro de estas conductas relacionadas con el acceso no autorizado a sistemas informáticos podemos distinguir diferentes tipos, de los cuales enumeraremos los siguientes:

a) Snooping: consiste en obtener información sin modificarla, por curiosidad, con fines de espionaje o robo. Downling: "bajar" esa información de la red.

b) Tampering o Data Diddling: estamos acá ante casos de modificación desautorizada de datos o del software del sistema.

c) Spoofing: es la técnica para conseguir el password de un usuario legítimo, para poder realizar actos irregulares en nombre de ese usuario.

---

[33] CREMADES Javier. FERNÁNDEZ-ORDOÑEZ Miguel Angel e ILLESCAS Rafael. "Régimen Jurídico de Internet". RODRIGUEZ MOURULLO Gonzalo, ALONSO GALLO Jaime y LASCURAIN SANCHEZ Juan Antonio. Derecho Penal e Internet". Capítulo II. Ob. Cit., página 266.

[34] LEVENE Ricardo y CHIARAVALLOTI, Alicia . "Delitos informáticos". Libro de Ponencias del VI Congreso Iberoamericano de Derecho e Informática.

d) Looping: en este caso el intruso utiliza el sistema para obtener información e ingresar a otro sistema. La técnica es que evapora la identidad del atacante y su ubicación.

e) Jaaming o Flooding: son ataques que pueden activar o saturar los recursos de un sistema.

f) Phreaking: es el acceso no autorizado a sistemas telefónicos para obtener gratuidad en el uso de las líneas, esta conducta a su vez tiene variantes, que son:

- Shoulder operations: consiste en la obtención del código de la víctima mientras esta lo utiliza, para aprovecharlo posteriormente.

- Call-sell operations: el sujeto presenta un código identificador de usuario que no le pertenece y carga el costo de la llamada a la víctima.

- Diverting: penetración ilícita a centrales telefónicas privadas para realizar llamadas de larga distancia que se cargan al dueño de la central.

- Acceso no autorizado a sistemas de correos de voz***:*** atacan a las máquinas destinadas a realizar el almacenamiento de mensajes telefónicos

g) Trashing: obtención de información secreta o privada que se logra por revisión de la basura (material o inmaterial).

4.3 Violaciones a la Intimidad

Juan José BLOSSIERS y Sylvia CALDERON[35] analizan dos tipos de violaciones a la privacidad:

1. Divulgación o autorizada de datos o "Data Leakcage": Consiste en sustraer información confidencial almacenada en un computador central desde un punto remoto, accediendo a ella, recuperándola y finalmente enviándola a una unidad de computador personal, copiándola simultáneamente. La sustracción de información confidencial es quizás uno de los cánceres que con mayor peligro acechan a los grandes sistema informáticos.

[35] BLOSSIERS MAZZINI Juan José. CALDERON GARCIA Sylvia B. "Los Delitos inform@ticos". Editora RAO SRL Lima, 2000. páginas 53 y 54.

2. Suplantación de la personalidad o "Impersonation": Puede ser entendida como la suplantación de personalidad fingiendo ser una persona que no es imitándola e inclusive remedándola. El caso más común es el robo de tarjetas de crédito y de cajeros automáticos. Los autores del delitos se hacen pasar por empleados de la central de tarjetas de crédito, llamando telefónicamente al titular para solicitarle que con el objeto de anular la posibilidad de utilización fraudulenta de la tarjeta robada le revele su clave secreta o personal.

4.4 Delitos informáticos en el Derecho Uruguayo

La primera norma uruguaya que tipifica un delito informático es la Ley 16.002 del 25 de noviembre de l988, la cual en el artículo 130 establece: "*El que voluntariamente trasmitiere a distancias entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda*". Los artículos 129 y 130 de dicha norma regulan la autenticidad y prueba de los documentos trasmitidos a distancia por medios electrónicos entre dependencias oficiales. Y los delitos a que alude son los que penalizan la falsificación documentaria.

Art. 129. "*La documentación emergente de la transmisión a distancia, por medios electrónicos, entre dependencias oficiales, constituirá, de por sí, documentación auténtica y hará plena fe a todos sus efectos en cuanto a la existencia del original trasmitido*".

Art. 130. "El que voluntariamente trasmitiere a distancias entre dependencias oficiales un texto del que resulte un documento infiel, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda".

La Ley 16736 de 5/1/1996 amplía el artículo 129 de la ley 16.002 en dos aspectos: sustituye el término "medios electrónicos" por "medios informáticos y telemáticos" y elimina la frase "entre dependencias oficiales", lo que convierte a la norma en aplicable para la generalidad[36].

El inciso segundo establece: "*El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento almacenado en soporte magnético, o su respaldo, incurrirá en los delitos previstos por los artículos 236 a 239 del Código Penal, según corresponda*".

Comparando con el art. 130 de la ley 16.002 podemos observar que en primer lugar hay una ampliación de los comportamientos reprimibles, en segundo lugar se elimina también aquí la expresión "*entre dependencias*

[36] VIEGA María José. "La influencia de la informática en la actividad probatoria y su regulación en Uruguay". Ponencia presentada al VII Congreso Iberoamericano de Derecho e Informática. Lima, 2000.

oficiales" y se tiene en cuenta para quien adultere o destruya el "*documento almacenado en soporte magnético o su respaldo*".

El 13 de enero de 2003 se promulgó la Ley de Protección del Derecho de Autor y Derechos Conexos Nº 17.616, la cual modifica el texto de la ley 9.739, incluyendo en forma expresa al software como una de las obras objeto de su protección, regulando de esta forma la reproducción ilícita de software.

La información no es un bien que se encuentre protegido en nuestro derecho, salvo excepciones muy concretas como el caso del secreto profesional y el secreto de Estado. Otro elemento a tener en cuenta es que esta clase de delitos se concretan en la mayoría de los casos como delitos a distancia, una forma jurídica que hasta hoy era casi inaplicable. Y la distancia va a estar dada desde dos puntos de vistas: geográfico y temporal[37].

Pero hay que tener muy en cuenta que "la confidencialidad y corrección de los datos transmitidos a través de Internet, y la confianza de los ciudadanos y de las empresas en que los datos que transmitan permanezcan secretos y no sean objeto de alteración, son esenciales para el comercio electrónico y, con ello, cada vez más para el tráfico jurídico mismo"[38].

4.5 Aplicabilidad de los artículos del Código Penal Uruguayo

Debemos preguntarnos acerca de la posibilidad de aplicar los delitos tipificados en nuestro Código Penal a las diversas posibilidades que analizamos anteriormente.

Hurto

Artículo 340. "*El que se apoderare de cosa ajena mueble, sustrayéndosela a su tenedor, para aprovecharse o hacer que otro se aproveche de ella, será castigado con tres meses de prisión a seis años de penitenciaría*."

El problema está planteado con el objeto, o sea la cosa ajena mueble. En nuestro derecho fue necesario agregar por el artículo 316 de la ley 13.737 el Hurto de Energía y Agua Potable (art. 343 del Código Penal).

Teniendo presente el principio de legalidad, este artículo no es aplicable a los casos de hurto de información, por ejemplo, donde la misma no se sustrae a su tenedor, sino que este sigue teniéndola. Tampoco se puede

---

[37] VIEGA María José. "Un nuevo desafío jurídico: los delitos informáticos". Ponencia presentada al Congreso Virtual Ecomder 2000.

[38] CREMADES Javier. FERNÁNDEZ-ORDOÑEZ Miguel Angel e ILLESCAS Rafael. "Régimen Jurídico de Internet". RODRIGUEZ MOURULLO Gonzalo, ALONSO GALLO Jaime y LASCURAIN SANCHEZ Juan Antonio. "Derecho Penal e Internet". Capítulo II. Ob. Cit., página 262.

aplicar al dinero contable que contiene una transferencia electrónica de fondos, porque tampoco estamos en presencia de una cosa mueble.

Estafa

Artículo 347. "*El que con estratagemas o engaños artificiosos, indujere en error a alguna persona, para procurarse a sí mismo o a un tercero, un provecho injusto, será castigado con seis meses de prisión a cuatro años de penitenciaría*".

Se ha discutido acerca de si se puede engañar a una máquina, o si por el contrario la víctima de la estafa debe ser una persona. Se ha dicho que no puede engañarse a una máquina, sin embargo hoy existe una nueva interpretación que establece que detrás de la máquina hay una persona que la diseñó y es el programador.

Daño

Artículo 358. "*El que destruyere, deteriorare o de cualquier manera inutilizare, en todo o en parte, alguna cosa mueble o inmueble ajena, será castigado, a denuncia de parte, cuando el hecho no constituya delito más grave con multa de .....*"

El objeto del daño debe ser una cosa mueble o inmueble, los delitos informáticos dañan los datos, la información, los programas, pero no a la computadora en sí. En virtud de esto sería imposible aplicar este artículo al daño informático. Además se habla de dañar cosa ajena, y aquí en realidad el propietario del soporte físico (la computadora) es en la mayoría de los casos el usuario.

5. Conclusiones

De lo antedicho surge que Uruguay no tiene una norma específica en materia de protección de datos, existe un proyecto de ley a estudio del Parlamento referente a protección de datos con finalidad comercial, que regula también la acción de habeas data. Sin perjuicio de lo cual, podemos proteger a través de la normativa citada las posibles violaciones a la privacidad.

Debemos tomar conciencia que somos propietarios de nuestros datos personales, de la misma forma que podemos poseer cualquier propiedad física. Por lo tanto debemos ser cuidadoso de a quien se los entregamos y con que motivo. Somos los primeros que debemos protegernos actuando con cautela.

Como juristas es importante tomar cartas en el asunto a los efectos de que dichos bienes estén protegidos adecuadamente en cada uno de nuestros países.

Respecto a los delitos informáticos los mismos deben estar expresamente tipificados en la ley penal, de forma tal que es necesario legislar en esta materia. Pero es imprescindible contar con las herramientas tecnológicas adecuadas, y con técnicos preparados para que los delitos no queden en la letra de la ley por falta de medios para detectarlos.

Montevideo, 3 de setiembre de 2003.