JORNADA RIOPLATENSE DE DERECHO INFORMATICO
Buenos Aires, 18 de agosto 2011

Los Delitos Informáticos: una mirada desde la seguridad y la protección de datos

Dra. Esc. Prof. María José Viega(*)

CONTENIDO

(*)Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UDELAR). Experta Universitaria en Protección de Datos, UNED (ESPAÑA). Directora del Instituto de Derecho Informático de la Facultad de Derecho de la Universidad de la República. Directora de la Dirección de Derechos Ciudadanos de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (AGESIC) – Presidencia de la República. Profesora de Informática Jurídica, de Derecho Informático y de Derecho Telemático en la UDELAR. Coordinadora del Grupo del Jurisprudencia del Instituto de Derecho Informático de la UDELAR. Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Ex - Profesora del curso en línea Derecho del Ciberespacio en la UDELAR. Ex - Profesora de Derecho de las Telecomunicaciones en la Universidad de la Empresa. Ex - Profesora en la Oficina Nacional de Servicio Civil (Presidencia de la República) del Curso Derecho de Internet. Ex - Profesora de los cursos de e-learning “Introducción al Derecho de las TICs”, “Documento y firma electrónica”, “Protección de datos” y “Contratos Informáticos” en Viega & Asociados. Directora del Estudio Jurídico Viega & Asociados. Miembro Honorario de la Asociación Paraguaya de Derecho Informático y Tecnológico (APADIT). Miembro Fundador del Instituto de Derecho Informático (UDELAR) y de FIADI Capítulo Uruguay. Miembro de la International Technology Law Association. Miembro de la International Association of Privacy Professionals. Autora del libro “Contratos sobre bienes y servicios informáticos”. Amalio Fernández, junio 2008. Co-autora de los Libros: con el Dr. Carlos Delpiazzo: Lecciones de Derecho Telemático Tomo I y II (FCU, abril 2004 y mayo 2009) y con la Dra. Esc. Beatriz Rodríguez deL e-book “Documento Electrónico y Firma Digital. Cuestiones de Seguridad en las Nuevas Formas Documentales (junio 2005) y con la Dra. Esc. Beatriz Rodríguez y Flavia Baladán de “Marco normativo del Derecho Informático” (julio 2011). Es autora de múltiples trabajos de su especialidad y conferencista a nivel nacional e internacional.

1. Introducción

Los beneficios de las tecnologías de la información y las comunicaciones son indiscutibles. Sin embargo, también sirven como herramienta para causar daño y en este sentido la criminalidad en Internet es la parte negativa del desarrollo tecnológico.

La presentación de hoy tiene como objetivo analizar las amenazas existentes en el ciberespacio, tanto en la esfera pública como privada. En la esfera pública analizaremos la creación y cometidos del CERTuy en nuestro país, centro responsable de las respuestas a incidentes en temas de seguridad de la información y quien trabaja con los organismos públicos a los efectos de prevenir amenazas en este sentido.

Por otra parte, en la esfera privada, la importancia económica de la información de todos nosotros nos enfrenta a invasiones permanentes a nuestra intimidad. En tal sentido Uruguay aprobó la Ley de protección de datos personales. Analizaremos las diferentes figuras delictivas vinculadas a la privacidad y el marco jurídico existente en Uruguay.

2. La seguridad de la información en la esfera pública: CERTuy

El centro de la coordinación de CERT® (CERT/CC) es un Centro de Maestría de la seguridad de Internet, que fue creado en 1988 en Estados Unidos y forma parte del Software Engineering Institute de la Universidad de Carnegie Mellon. Su información pretende proteger nuestros sistemas contra problemas potenciales y reaccionar a los problemas actuales y a problemas futuros. Su trabajo implica estudiar los sistemas de seguridad de la computadora y las vulnerabilidades, alarmas de seguridad, investigar cambios a largo plazo en sistemas networked, y proporcionar la información y entrenamiento para ayudarle a mejorar la seguridad en su sitio[1].

La sigla CERT deviene de “Computer Emergency Response Team”, esto es, un equipo de trabajo responsable del desarrollo de medidas preventivas y reactivas relacionadas con los incidentes de seguridad en los sistemas de información[2].

Los problemas relativos a la seguridad de la información guardan una estrecha relación con los activos de información, los que en términos generales pueden estar determinados por el tipo de datos manejados, la calidad de los servicios prestados, el mercado donde se desempeñan, las actividades y vínculos establecidos. Es por ello, que no solo es importante definir y establecer cuáles son los activos de información que el Estado posee, sino gestionar su reutilización y dotar de un marco de seguridad adecuado orientado a la confidencialidad, integridad y disponibilidad de la información. Viega María José y Carnikian Federico. ”Respuesta a los delitos informáticos: su visión desde la privacidad y la

[1] VIEGA, María José y DELPIAZZO Carlos. Lecciones de Derecho Telemático. Tomo I. Lección 13. Página 177.
[2] http://cert.inteco.es/Acerca_de/. Página visitada 29 de junio de 2010.

seguridad de la información". Ponencia presentada al Seminario Nuevas Tecnologías: Privacidad y Seguridad. Cartagena de Indias, 21 al 23 de julio de 2010.

Para lograr un marco adecuado de seguridad, es necesaria la aplicación de un conjunto de medidas técnicas y organizativas a efectos de lograr un entorno seguro para los datos, la información, y los sistemas que los sustentan[3].

Hay que tener presente a norma ISO/IEC 27001 define a la seguridad de la información como la preservación de la confidencialidad, la integridad, y la disponibilidad, pudiendo además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio. A estos efectos, una buena gestión de seguridad puede ser obtenida a través de la concreción de un conjunto de controles, tales como políticas, prácticas, procedimientos, estructuras organizativas y software adecuados.

En este sentido, es necesario que el Estado -como uno de los principales sujetos que almacena y transmite información- adopte medidas de seguridad adecuadas a fin de proteger aquella información sustancial para el desarrollo de sus actividades y cometidos, y que en definitiva es fundamental a efectos de la protección de sus intereses como Estado y la salvaguarda de los derechos de los ciudadanos. El Estado, al igual que los particulares, pueden ser víctimas de ataques de estos "delincuentes informáticos", los que muchas veces atentan contra un sistema de información por el simple hecho de divertirse, o como forma de realizar publicidad de ellos mismos. Conforme a esto, existe la necesidad de contar con políticas, prácticas, medidas de seguridad adecuadas, entre otras, y la existencia de un equipo de trabajo que, a nivel estatal, centralice las competencias al respecto y dé respuestas inmediatas a las amenazas que la propia red pueda ocasionar. Viega María José y Carnikian Federico. "Respuesta a los delitos informáticos: su visión desde la privacidad y la seguridad de la información". CADE

Por Ley N° 18.172 de 7 de septiembre de 2007, artículo 119, se creó el Consejo Asesor Honorario de Seguridad de Informática del Estado en el ámbito de la Agesic, integrado por ……...

El artículo 55 de la Ley 18.046 de …….. en la redacción dada por el artículo 118 de la Ley Nº 18.172 otorgó a la Agesic potestades legales para la concepción y el desarrollo de políticas en materia de seguridad de la información, a los efectos de la prevención, detección y respuesta frente a los incidentes que pudieran afectar los activos críticos del país.

Por Ley Nº 18.362 de 15 de octubre de 2008, artículo 73, se creó el CERTuy dentro del ámbito de la Agesic, con los cometidos de regular la protección de los activos críticos de información del Estado, difundir las mejores prácticas, centralizar y coordinar la respuesta a incidentes informáticos y realizar las tareas preventivas que correspondan.

[3] Curso CEDDET. Módulo 3: Seguridad, confidencialidad, transferencias internacionales y autorregulación. Página 43.

Este artículo fue reglamentado por el Decreto Nº 451/009 de 28 de septiembre de 2009 en el cual se definen los incidentes informáticos como una violación o amenaza inminente de violación a una política de seguridad de la información implícita o explícita, que comprometa la seguridad de un sistema (confidencialidad, integridad o disponibilidad).

El Decreto Nº 452/2009 de 28 de septiembre de 2009 aprobó las "Políticas en la Seguridad en la Información para los Organismos del Estado", de aplicación obligatoria para los organismos públicos integrantes de la Administración Central, exhortándose su cumplimiento a los restantes órganos del Estado.

Podemos diferenciar los cometidos otorgados al CERTuy, en dos grupos: a) los relativos al trabajo en conjunto con los restantes organismos del Estado; y b) los relacionados con los incidentes de seguridad y las medidas atinentes a su control y prevención. Viega María José y Carnikian Federico. "Respuesta a los delitos informáticos: su visión desde la privacidad y la seguridad de la información". Ob. Cit.

a) Se trata de tareas de asistencia, coordinación, colaboración entre los organismos públicos con la finalidad de proporcionar una asistencia eficaz en los casos de incidentes de seguridad informática, proponer normas destinadas a incrementar los niveles de seguridad en los recursos y sistemas relacionados con las TIC.

Además de los verbos nucleares utilizados por la norma reglamentaria descrita, se desprende que se trata de un proceso donde los distintos niveles de seguridad que los Organismos posean se van a ir acompasando con la normativa vigente gracias a la colaboración, asistencia, coordinación y asesoramiento que el CERTuy les provea.

En este sentido, la norma se encuentra en armonía con el Decreto Nº 450/009 que aprueba un documento de políticas de seguridad de la información para los organismos públicos.

b) El CERTuy posee cometidos relacionados con la alerta ante amenazas y vulnerabilidades informáticas dando respuesta a los incidentes ocurridos. Estos servicios son denominados como reactivos, esto es, servicios diseñados para dar respuestas a solicitudes de asistencia, como por ejemplo a los incidentes de seguridad, investigación forense tendiente a determinar las huellas informáticas que los ataques informáticos generan.

El CERTuy documenta y registra los reportes de los incidentes ocurridos.

El artículo 1º del Decreto dispone que el CERTuy protegerá tanto los sistemas informáticos como los sistemas circundantes a éstos.

La respuesta a incidentes puede significar la realización de análisis forense sobre el sistema o sistemas informáticos circundantes al analizado, tales como la descripción de aquellas "huellas informáticas" que el atacante, dejó en el sistema.

Las tareas preventivas implementadas por el CERTuy, son ejercidas a través de un procedimiento establecido y regulado en los artículos 9 a 13 de la reseñada norma.

Asimismo, se informa que el CERTuy viene trabajando en base a tres columnas de trabajo:

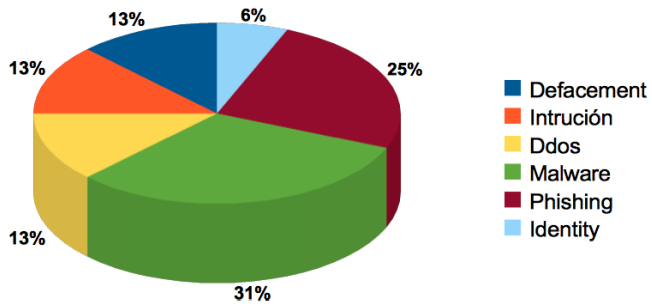
1) Actividades Reactivas: tales como la respuesta a incidentes de seguridad informática e investigación forense;

2) Actividades Proactivas: por ejemplo el asesoramiento en seguridad y alerta de incidentes;

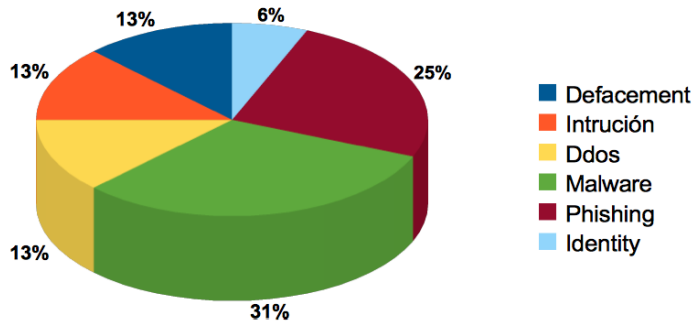
3) Actividades en materia de Seguridad e Infraestructura, es decir, la seguridad en la red y sobre la plataforma de gobierno electrónico.

En cuanto a datos estadísticos, el CERTuy en la actualidad gestiona un promedio de dos incidentes mensuales.

A nivel de ataques encontramos[4]:



A nivel de ataques tenemos[5]:



Se han registrados casos de correos electrónicos enviados a nombre de otro, consumándose robos de identidad.

[4] PAZ Santiago. Presentación del CERTuy junio del 2010.
[5] PAZ Santiago. Presentación del CERTuy

3. La inseguridad de la información en la esfera privada

Abordaremos la conceptualización de la criminalidad en la red vinculada a la seguridad de los datos personales analizando las principales amenazas relacionados con los niños, con la privacidad, con aspectos económicos destacando las siguientes:

3.1 Ciberbullying

El Ciberbullying es una variante del Bullying o acoso escolar tradcional, por denominarlos de alguna forma. Lo que queremos destacar es que esta no es una figura nueva, sino que, se potencializan sus efectos realizados por medios electrónicos, planteándose una situación de anonimato para los acosadores en la red.

Pero, la tecnología también permite detectar el lugar exacto y el equipo informático desde el que se llevó a cabo el presunto delito, a través de la detección de la dirección IP. El desafío se presenta en cuanto a la tipificación penal de esta conducta.

Podemos definirlo como la conducta protagonizada por uno o varios acosadores hacia uno o varios de sus compañeros. Consiste en utilizar medios electrónicos como la computadora, internet o el celular para acosar, intimidar y agredir psicológicamente a las víctimas.

Esta conducta se define como acoso entre iguales en el entorno TIC e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños. En una definición más exhaustiva, se puede decir que el *ciberbullying* supone el uso y difusión de información lesiva o difamatoria en formato electrónico a través de medios de comunicación como el correo electrónico, la mensajería instantánea, las redes sociales, la mensajería de texto a través de teléfonos o dispositivos móviles o la publicación de videos y fotografías en plataformas electrónicas de difusión de contenidos[6].

3.2 Grooming

El grooming es un nuevo tipo de problema relativo a la seguridad de los menores en Internet, consistente en acciones deliberadas por parte de un adulto de cara a establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual, posiblemente por medio de abusos.

El grooming habitualmente es un proceso que puede durar semanas o incluso meses, y que suele pasar por las siguientes fases, de manera más o menos rápida según diversas circunstancias:

---

[6] INTECO, Instituto Nacional de Tecnologías de la Comunicación. “Guía legal sobre Ciberbullying y gooming”.

1. El adulto procede a elaborar lazos de amistad con el menor simulando ser otro niño o niña.

2. El adulto va obteniendo datos personales y de contacto del menor.

3. Utilizando tácticas como la seducción, la provocación, el envío de imágenes de contenido pornográfico, consigue finalmente que el menor se desnude o realice actos de naturaleza sexual frente a la webcam o envíe fotografías de igual tipo.

De esta forma se inicia un proceso de cyberacoso, en el cual se chantajea a la víctima para obtener cada vez más material pornográfico o tener un encuentro físico con el menor para abusar sexualmente de él.

3.3 Suplantación de identidad

"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 delito 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"[7].

Hoy por hoy, con el desarrollo de las redes sociales en Internet, una nueva modalidad es la creación de páginas o usuarios suplantando a otra persona.

3.4 Phishing

Los ataques de estafa a través de Internet por el método "phishing", que significa "pesca" en el argot informático, se han ido incrementando. El sistema más utilizado por los cyber-estafadores es el envío de correos electrónicos con falsos remitentes, como por ejemplo de entidades financieras, de forma tal que las víctimas cliquearan en un link y de esa forma podían obtener información personal[8].

Pero ya se habla de una nueva generación de phishing. Hispasec[9] demuestra cómo es posible realizar ataques phishing en servidores seguros de entidades bancarias, aun cuando el usuario visualice que la URL comienza por https:// seguido del nombre de la entidad y que el icono del candado que aparece en la parte inferior del navegador certifique que se encuentra en el servidor seguro del banco, lo que constituían hasta el momento las recomendaciones que se

---

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

[8] VIEGA, María José. "El problema de los datos personales y el espionaje en Internet", presentada al Cuarto Congreso Internacional de Derecho (CIDER 2005) en las Sedes de Cochabamba, Santa Cruz y La Paz. Bolivia, 23 al 25 de noviembre de 2005. Publicada en el Libro de Ponencias.

[9] http://www.hispasec.com/unaaldia/2406 Página visitada 13 de junio 2005.

hacían para acceder de forma segura a la banca electrónica[10]. Como podemos ver esto se ha vuelto inseguro y el Pharming es la confirmación de esta afirmación.

3.5 Derivados del Phishing

3.5.1 Scam

A este tipo de fraude también se lo conoce como phishing laboral, porque tiene como objetivo obtener datos confidenciales de usuarios, para acceder a sus cuentas bancarias.

Las modalidades utilizadas consisten en envíos masivos de correos electrónicos o la publicación de anuncios en webs, en los que se ofrecen empleos muy bien remunerados. Cuando el usuario acepta la oferta de trabajo, se le solicita que facilite datos de sus cuentas bancarias, a través de un e-mail o accediendo a una web, para ingresarle los supuestos beneficios.

3.5.2 Smishing

Esta es otra variante del phishing, pero el ataque se realiza a través de los mensajes a teléfonos móviles. El resto del procedimiento es igual al del phishing, el estafador suplanta la identidad de una entidad de confianza para solicitar al usuario que facilite sus datos, a través de otro SMS o accediendo a una página web falsa, idéntica a la de la entidad en cuestión.

3.5.3 Spear Phishing

También estamos, en este caso, ante un sub tipo de phishing en el que, en lugar de realizar un envío masivo de correos electrónicos, se envían correos con mayor grado de personalización, a destinatarios concretos, consiguiendo que los mensajes resulten más creíbles que los del phishing tradicional.

3.5.4 Vishing

Esta clase de fraude también persigue la obtención de datos confidenciales de los usuarios, pero a través de la telefonía IP. Los ataques de vishing se suelen producir siguiendo dos esquemas[11]:

- Envío de correos electrónicos, en los que se alerta a los usuarios sobre algún tema relacionado con sus cuentas bancarias, con el fin de que éstos llamen al número de teléfono gratuito que se les facilita.

- Utilización de un programa que realice llamadas automáticas a números de teléfono de una zona determinada.

---

[10] VIEGA, María José. "Privacidad Vs. Espionaje en Internet". Anuario de "Derecho Informático". Tomo VI Jurisprudencia correspondiente al año 2005 y en el Boletín de Derecho y Tecnologías Nº 16 Enero 2005 http://viegasociados.com/moodle//mod/forum/discuss.php?d=440

[11] http://www.delitosinformaticos.info/delitos_informaticos/glosario.html Página visitada 21 de junio de 2010.

En ambos casos, cuando se logra contactar telefónicamente con el usuario, un mensaje automático le solicita el número de cuenta, contraseña, código de seguridad, etc.

3.6 Pharming

El pharming deriva del término *farm,* granja en inglés, expresión que es utilizada cuando el atacante ha conseguido acceso a un servidor DNS o varios servidores, en este último caso granja de servidores o DNS.

Esta modalidad de fraude online ataca la vulnerabilidad del software de los servidores DNS o de los equipos de los propios usuarios, redireccionando el nombre de dominio a un sitio web falso, diseñado por el atacante.

Es utilizada para realizar ataques de *phishing*, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos personales del usuario, generalmente datos bancarios.

Si el phishing engaña a los usuarios uno por uno, conduciéndolos a visitar un sitio apócrifo de su banco o comercio preferido, el pharming interviene las comunicaciones entre el usuario y su proveedor de Internet (ya sea un proveedor de comunicaciones, o un servidor corporativo) para lograr que cuando un usuario teclea en su navegador una dirección legítima, éste sea conducido a una falsificación de la página Web que quiere visitar y sea ahí donde introduzca los datos de su cuenta[12].

Por tanto, el riesgo para el usuario en los casos de pharming es diferente, mientras que en el phishing requiere una actitud activa, hacer click en el link del correo electrónico, en el pharming el fraude se produce sin participación directa del usuario. La utilización de medidas técnicas de seguridad en un sistema, como por ejemplo un firewall, herramientas de protección contra adware y spyware, contrarrestan este tipo de amenazas. Viega María José y Carnikian Federico. ”Respuesta a los delitos informáticos: su visión desde la privacidad y la seguridad de la información”. Ob. Cit.

El pharming se realiza modificando el software, lo cual puede realizarse en forma remota o introduciendo un programa que lo realice en forma automática. Para ello es necesario introducir un troyano en el disco duro de la víctima, el cual puede autoeliminarse, borrando del disco duro las huellas del ataque.

“La respuesta es muy delicada para el banco, si hace responsable al cliente y el "pharming" se generaliza, los usuarios abandonaremos en masa la banca online por insegura y peligrosa, pero si el banco carga con los gastos. ¿A cuánto tendrá que subir las comisiones por operación el banco online para cubrir este riesgo? ¿Seguirá siendo competitivo? Si no se atajan estos riesgos,

---

[12] http://www.mx.terra.com/tecnologia/interna/0,,OI889426-EI4906,00.html Página visitada 21 de junio de 2010. El Pharming: amenaza de fraude a negocios. Trend Micro. 21 de febrero de 2006.

quizá el porvenir de la e-banca no sea después de todo tan brillante como se auguraba"[13].

3.7 Scavenging

Es la apropiación de informaciones residuales, la que consiste en la obtención de información a partir de lo que desechan los usuarios legítimos de un sistema informático.

4. Marco jurídico uruguayo

La primer norma uruguaya que tipifica un delito informático es la Ley Nº 16.002 del 25 de noviembre de 1988, la cual en el artículo 130 establece: "*El que voluntariamente trasmitiere a distancia 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 Nº 18.600 de 21 de setiembre de 2009 de documento electrónico y firma electrónica establece en el artículo 4 inciso 2º establece: "*El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento electrónico, incurrirá en los delitos previstos por los artículos 236 a 245 del Código Penal, según corresponda*".

Además de los delitos tradicionales tipificados en nuestro Código Penal, como el hurto en el artículo 340, la estafa en el artículo 347, el daño en el artículo 358, existen una serie de normas, que enunciamos a continuación:
Viega María José, Rodríguez Beatriz y Baladán Flavia. "Marco normativo del Derecho Informático". Libro editado en Montevideo en Junio 2011.

Ley N° 17.520 de 19 de julio de 2002. Se penaliza el uso indebido de señales destinadas exclusivamente a ser recibidas en régimen de abonados.

Ley Nº 17.559 de 27 de setiembre de 2002. Se aprueba el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en pornografía.

Ley Nº 17.616 de 10 de enero de 2003, artículos 15 a 17. Se modifican y sustituyen artículos de la Ley Nº 9.739 de 17 de diciembre de 1937, especialmente los artículos 46 a 48.

Ley Nº 17.815 de 06 de setiembre de 2004. Se regula la violencia sexual, comercial o no comercial cometida contra niños, adolescentes e incapaces que contenga la imagen o cualquier otra forma de representación.

Ley Nº 18.383 de 17 de octubre de 2008. Se penaliza el atentado contra la regularidad de las telecomunicaciones, modificándose el artículo 217 de Código Penal.

---

[13] http://www.laflecha.net/canales/seguridad/articulos/pharming/ El Pharming, un peligro para la e-banca. Página visitada 21 de junio de 2010.

Ley Nº 18.494 de 05 de junio de 2009, artículo 5º. Se modifica el régimen sobre prevención y control de lavados de activos y del financiamiento del terrorismo regulándose las vigilancias electrónicas.

Ley Nº 18.515 de 26 de junio de 2009, artículos 7º a 10. Se modifican artículos del Código Penal y de la Ley Nº 16.099 de 03 de noviembre de 1989, que tipifican delitos relativos a los medios de comunicación.

Ley Nº 18.719 de 27 de diciembre de 2010 de Presupuesto Nacional, artículo 149. Se crea la Dirección de Seguridad de la Información.

Uruguay está trabajando en un proyecto de reforma del Código Penal, a cuyos efectos, el artículo 22 de la Ley N° 17.897 de 14 de setiembre de 2005 creó una Comisión, la que se integrará por representantes de distintos organismos y organizaciones, tomando en consideración para su elaboración principios modernos de política criminal, introduciendo modificaciones y agregando conductas no tipificadas en el código penal vigente.

El proyecto citado, más precisamente en el capítulo de delitos contra la inviolabilidad del secreto contempla algunas hipótesis de espionaje informático.

En el delito de violación de correspondencia escrita -art. 296 del Código vigente- se incluyó la modalidad de mensajes de correo electrónico o cualquier otro documento cerrado[14].

Los delitos de interceptación de noticia telegráfica o telefónica -art. 297 código penal vigente- incluyen la noticia electrónica y por su parte el delito de revelación de secreto de la correspondencia y de la comunicación epistolar, telegráfica o telefónica -art.298- también se le agregó la modalidad electrónica.

El proyecto añade dentro de los delitos contra la propiedad, un tipo penal denominado “Menoscabo al derecho a disposición de datos” el que se relaciona directamente con la protección de datos personales.

El texto del proyecto dispone que: “…*al que por medio de copia, supresión, inutilización o cambio, menoscabare el derecho de disposición de otro, sobre datos, cuando éstos sean protegidos contra acceso no autorizado y que sean almacenados o se transmitan electrónicamente o en otra forma no inmediatamente visible*”.

En este sentido, la circunstancia de verse privado de disponer de la información personal y por tanto perder el control en el procesamiento y comunicación de los datos personales, afecta indudablemente los derechos de los titulares. De esta manera, se busca la protección de un derecho humano reconocido por la Ley N° 18.331, de Protección de Datos Personales y Acción de Habeas Data, como un derecho inherente a la persona humana.

[14] RODRIGUEZ, María José. “Comentarios al Proyecto de Reforma del Código Penal”. Trabajo Inédito de junio de 2010.

Se considera que el delito incluido, debería hacer alusión a sistema informático, a efectos de ser omnicomprensivo de situaciones que no afectan solamente la disposición de los datos, sino a un sistema, comprendiendo de esta manera la integridad, confidencialidad y disponibilidad de la información contenida en éste. (…) En estos casos se podría abarcar ataques de hacking o cracking -como intrusión o interferencia en un sistema-, incluyendo también la introducción de un virus en el sistema informático[15].

Concomitantemente, hace pocos días, se publicó una nota de prensa bajo el título: Proponen duros castigos a la "ciberdelincuencia", en la cual se anuncia un proyecto de ley del senador Tabaré Viera, que plantea penas de prisión escalonadas para las falsificaciones informáticas, accesos ilícitos, interceptación de datos, pornografía infantil y fraude.

El texto del proyecto propone castigar de forma escalonada una decena de delitos relacionadas con el manejo informático (muchos ya previstos en la ley), con multas que van de las 50 a 500 Unidades Reajustables ($231.500), o penas de prisión de entre tres meses y siete años. Luego de definir lo que entiende por sistema informático, datos y proveedores de servicios, entre otras cosas, el proyecto detalla los casi diez delitos que componen la "ciberdelincuencia"[16].

En cuanto a los criterios para establecer las medidas de seguridad, se considera que ésta debe atender a: la naturaleza de los datos, siendo las más exigentes las relativas a los datos especialmente protegidos; la finalidad del tratamiento, el tipo de soporte donde se almacene y registre dicha información[17].

La normativa uruguaya contiene los principios básicos en materia de seguridad de la información.

Las medidas de seguridad para la protección de los datos personales dependerá del tipo de organización, del volumen de los datos tratados, de los sistemas que utilicen, del responsable o encargado de tratamiento y de las personas que participen en cualquier fase del procesamiento de los datos personales.

El principio de seguridad se encuentra inmerso dentro del conjunto de los principios establecidos en la LPDP, por lo que la aplicación e interpretación del mismo debe guardar estrecha relación con ellos.

---

[15] RODRIGUEZ, María José. "Comentarios al Proyecto de Reforma del Código Penal". Trabajo Inédito de junio de 2010.

[16] http://www.observa.com.uy/actualidad/nota.aspx?id=99214&ex=25&ar=2&fi=1&sec=8 Información del día 8 de julio de 2010.

[17] Curso CEDDET. Módulo 3: Seguridad, confidencialidad, transferencias internacionales y autorregulación. Página 15.

Policía especializada en Delitos Informáticos

La División de Delitos Informáticos perteneciente al Departamento de Delitos Complejos de la Policía de Montevideo, fue creada por Decreto N° 254/003, y comenzó a funcionar en el año 2005.

El Jefe de Delitos Informáticos, Gabriel Lima, aseguró a El País que hoy en día los delitos informáticos más comunes en Uruguay son las amenazas de muerte por correo electrónico y páginas web. Los delitos informáticos han aumentado, se han perfeccionado y son más difíciles de aclarar ya que las pistas no están "al alcance de la mano", explicó Lima agregando que "en una rapiña los investigadores tienen a la víctima que aporta datos, testigos y posibles pruebas en el lugar; en los delitos informáticos las pruebas que nosotros necesitamos no están físicamente en nuestras manos y el 90% de las veces tenés que ir a servidores extranjeros para ver si hay algún respaldo"[18].

"Delitos informáticos" es una nominación para que se entienda, pues no existe una legislación en Uruguay que los defina. "Lo que hacemos es combatir los ilícitos como estafa, hurto, amenaza, y en que el medio para cometerlos sea Internet", explicó el subjefe de la división, el oficial Roberto Ferreira[19].

Un caso que se destacó en la prensa uruguaya en el mes de mayo fue el siguiente: “Eduardo jamás usó Facebook. Por una cuestión de principios, no forma parte de "redes que carecen de un director responsable o en las que la gente puede escudarse en el anonimato". Sin embargo, un día recibió la noticia de que alguien había creado un perfil suyo en la popular red social, en el que se le atribuían preferencias políticas y sexuales que no compartía. Sin dudarlo, inició un proceso de investigación que finalizó con un resultado poco habitual en estos casos”[20].

El día 7 de julio de 2010 mantuvimos reunión con el Agente Walter Mario Calleros de la Policía de Montevideo, Dirección de Investigaciones Departamento de Delitos Complejos Sección Delitos Informáticos, quien manifestó su preocupación acerca de la falta de normativa existente en delitos informáticos, sobre todo en lo que tiene que ver con la regulación de los cibercafés, responsables de teléfonos celulares, concretamente de los chips, ya que la venta de teléfonos tarjeteros no permite identificar al titular del servicio.

Por otra parte, destacó la importancia de guardar información de telecomunicaciones, tanto de las empresas prestadoras de servicios de telefonía celular, como los ISP, resultando fundamental contar con los log de registro, no siendo necesario los contenidos de los mensajes. Con el dato del log es posible que Antel informe a quien le asignó la IP en ese día y hora.

---

[18] Alerta: crece el peligro de delitos a través de Internet. http://www.elpais.com.uy/09/02/11/lault_398189.asp El País Digital del 2 de febrero de 2009.

[19] Ciberpolicías patrullan la web. http://www.elpais.com.uy/Suple/DS/07/04/22/sds_276418.asp El País Digital del 22 de abril de 2007.

[20] Los peligros en las redes sociales: cuando la impunidad es la norma. http://www.espectador.com/1v4_contenido.php?id=182602&sts=1 El Espectador, entrevista del 21 de mayo de 2010.

También es relevante guardar la información de servicios 3G, entendiendo como un plazo razonable entre 6 meses y un año para todos los casos.

Los casos más comunes son de difamación e injurias a través de Internet o de teléfonos celulares prepagos, en igual porcentaje y la suplantación de identidad a través de la creación de sitios web.

Se entiende relevante legislar delitos concretos como el hurto de información, el fraude electrónico, la suplantación de identidad, así como también ratificar la Convención de Budapest sobre Cybercrime.

A vía de ejemplo se hizo referencia a algunos casos investigados en nuestro país, que se comentan a continuación.

Respecto al grooming, es fundamental tener en cuenta la edad de las niñas, distinguiendo si tienen más de 10 años. Se planteó una denuncia por una madre de una adolescente de 14, que se había fotografiado y filmado y a quien la persona de contacto en la web se había negado a conocer personalmente (18 años) al enterarse de la edad de la menor.

La denominada "Operación Peón" refiere a un uruguayo que se encuentra procesado y al que se le incautaron materiales de pornografía infantil. No se le ha podido probar la producción de pornografía, que es el delito más severamente tipificado. Este caso tiene ramificaciones internacionales.

Hurto de correspondencia. Un funcionario de la Intendencia Municipal de Canelones, personal de confianza del Intendente, intervino los correos electrónicos de personas de los partidos blanco y colorado para enemistarlos.

Caso Velásquez. Es un hacker argentino que realizó un phishing mediante el cual ingresó a correos electrónicos de diputados y senadores enviando mensajes diciendo que necesitaba el usuario y password para el restablecimiento de la casilla. De esta forma lograba tener acceso a los correos electrónicos. Se encontró en su computador un listado de claves, todas las direcciones de correo electrónico que había intervenido. Es interesante desatacar que las casillas no fueron robadas, sino que estaban intervenidas, entraba y salía para leer los correos y obtener la información. Fue procesado por el Juez Letrado de Primera Instancia en lo Penal de 7º turno el 25 de enero de 2009.

"Tal fue el delito cometido por el espía argentino Iván Velásquez, quien robó información secreta sobre 60 policías de la Jefatura de Policía de Montevideo, relativa a su identidad y armamento"[21].

Sobre este caso, destaca el auto de procesamiento que: mediante la utilización de medios fraudulentos el encausado accedió a información reservada ocasionando un perjuicio a la seguridad. El encausado posee habilidades suficientes al efecto en virtud de ocupar cargos de inteligencia en la policía

[21] http://www.ultimasnoticias.com.uy/hemeroteca/040210/prints/act13.html Diario Ultimas Noticias del 4 de febrero del 2010.

Argentina, teniendo información de este tipo en su poder, a la cual accedió de forma no autorizada. El engaño se produce al simular hacer entrega de una computadora en donación a una de las dependencias del Ministerio del Interior argentino. La información contenía datos personales de los policías argentinos y uruguayos, sus armamentos, así como también información de personas vinculadas con la política de Uruguay.

El sentenciante entiende que la conducta encarta plenamente en la figura tipificada en el artículo 300 del Código Penal Uruguayo “Conocimiento fraudulento de documentos secretos”.

Además de las investigaciones policiales relatadas, interesa referir a casos resueltos judicialmente.

Por Sentencia del Juzgado Letrado en lo Penal de 20º Turno Nº 225 de 26 de agosto de 2009, se condenó por delito de violación de correspondencia con un ilícito de falsificación de documento privado por interceptación de correos electrónicos. En este caso, a través de la obtención por medios ilegítimos de la contraseña de la cuenta de correo electrónico de la denunciante, la procesada divulgó noticias falsas de ésta última a sus contactos personales.

Mediante orden judicial dirigida a “Anteldata”, se obtuvo la información con la que se pudo determinar el número IP asignado al contrato de adsl de la procesada, siendo más sencilla su determinación en virtud de que no existían conexiones inalámbricas a Internet.

Se considera que la conducta desplegada encarta plenamente en la figura representada en el artículo 296 del Código Penal Uruguayo, al haberse interceptado la correspondencia escrita electrónica con intención de interrumpir su curso normal.

Por Sentencia del Tribunal de Apelaciones en lo Penal de 2º Turno Nº 63 de 19 de marzo de 2009 se confirma procesamiento por un delito continuado de violencia privada mediante amenazas por mensajes de texto, correos electrónicos y llamadas telefónicas. A través del envío de mensajes de texto y correos electrónicos, la imputada amenazó de forma continuada a un hombre de estado civil casado, con el cual mantuvo una relación amorosa.

A pesar de que la defensa argumentó que la conducta desplegada no constituye una violencia o amenaza, la Sala desestimó los agravios, considerando que existió una transgresión al bien jurídico que la ley protege, es decir, la libre determinación de la voluntad, circunstancia la cual se vio alterada por la recepción de sendos mensajes de textos y correos electrónicos agraviantes.

5. Reflexión final

El Dr. Palazzi analiza el robo de identidad vinculado a ficheros sobre solvencia crediticia, manifestando que: “El robo de identidad es entonces algo muy nuevo, pero las soluciones legales están presentes desde hace mucho tiempo (aunque en mayor parte de los casos son de carácter paliativo y no preventivo), como lo evidencian los fallos que responsabilizan a entidades financieras. Lo que se necesita, entonces, no es una nueva ley sino un cambio de la arquitectura del sistema en materia de manejo de información; lo que se requiere, y lo examinaremos en detalle más adelante, es mejorar las protecciones a la difusión y acceso a la información en poder de entidades financieras por parte de terceros que intentan cometer delitos. (…) Lo que necesitamos es hacer más efectivas las normas de protección de datos, y a la vez mejorar las prácticas relacionadas con la obtención de créditos bancarios para evitar el uso de datos falsos”[22].

Uruguay debe trabajar en la actualización de marcos legales adecuados que den seguridad en los delitos informáticos no tipificados en nuestro derecho penal.

[22] PALAZZI, Pablo. “Robo de identidad, protección de datos personales y ficheros sobre solvencia crediticia”, capítulo del libro Derecho a la intimidad y a la protección de datos personales. Heliasta, Argentina, 2009. Página 132.