Delitos informáticos

Tomasi, Susana Noemí

1-Introducción

Hace a la problemática de la seguridad informática todo lo inherente al robo de identidad y la privacidad, y como afectan estas temáticas a nuestras empresas, instituciones y organismos, y al Estado.

La informática y el derecho se relacionan a raíz de acciones concretas en el ámbito informático que tienen relevancia en el ámbito del derecho.

Qué responsabilidad tienen las organizaciones por los delitos informáticos cometidos por sus dependientes o como agentes directos ellas y que responsabilidad patrimonial le acarrean estos ilícitos, aun cuando dicha organización o sus dependientes no tengan intención de causar daño.

Qué responsabilidad tienen por la información contenida en sus Bases de Datos, de clientes, proveedores y personal, y en el caso de las organizaciones, de sus usuarios.

También debe tenerse en cuenta, el desarrollo de los delitos informáticos, y tratar de efectuar políticas de prevención por parte de las organizaciones, para no verse afectados por los mismos.

Las políticas de prevención sirven para mitigar el riesgo, buscando las vulnerabilidades de las empresas en sus sistemas informáticos y a través del diagnóstico correspondiente minimizar las fallas que puedan contener sus sistemas, se detectan las debilidades en las configuraciones de la seguridad, ya que los ataques de los intrusos son cada vez más sofisticados.

Tomar en consideración que el delito informático atraviesa las fronteras y es difícil, actuar contra los delincuentes, su identificación, los procedimientos a seguir en distintos países, y la protección de la prueba, para que finalmente puedan los ladrones informáticos ser debidamente juzgados y procesados.

En Segu Info.com.ar, Legislación y delitos informáticos, se expresa: "...El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La cuantía de los perjuicios así ocasionados es a menudo muy superior a la usual en la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no lleguen a descubrirse o castigarse... El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho. Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún..."

2-Desarrollo:

Los delitos informáticos por el momento no se encuentran actualmente contemplados en la legislación vigente, ya que no existe una categoría especial respecto a ellos, y se utiliza la legislación común para su castigo, siendo a veces difícil la identificación del mismo y la acumulación de la prueba necesaria para su condena.

Sergio Mola (perteneciente a la Unidad Fiscal de Investigación contra la droga y el crimen organizado), en el Congreso Legal & Privacy - Contingencias Legales en el uso de la Tecnología, dentro de Infosecurity, 2007, realizado el 7 de junio en el Hotel Sheraton de Buenos Aires, expresó, que el derecho penal (cuyo Código es de 1921), que no se encuentra actualizado, corre detrás de los hechos, y que en derecho penal todo lo que no está prohibido está permitido, aún hechos dañosos.

Los desarrollos en técnicas de investigación respecto a delitos informáticos, siempre están un paso atrás del delito en sí, pero las fuerzas de seguridad tratan de aggiornarse para este tipo de delitos, y se deben hacer políticas de prevención, antes que pensar que la Justicia pueda dar soluciones adecuadas para este tipo de hechos.

Pero teniendo en cuenta que este tipo de delincuentes son muy sofisticados, y que son delitos difíciles de investigar, ya que las personas que cometen estos delitos, son profesionales insertos socialmente y mezclados en el funcionamiento del engranaje comercial, es complicado la prueba para condenar a los responsables de los mismos.

Además agregó que a veces es difícil perseguir todos los delitos, y las cuestiones más complejas, como son los delitos informáticos van quedando de lado lo que implica impunidad.

Actualmente se están creando unidades especializadas en el Ministerio Público para que sirvan a tal fin.

Las características especiales que tienen los delitos informáticos es que son transnacionales por lo cual escapan a la soberanía del país, que es muy difícil la recolección, guarda y preservación de las pruebas, y que las mismas deben ser colectadas en debida forma, para no ser nulas.

Se está tratando en el Congreso de la Nación un proyecto de ley de los delitos informáticos, que por ser tan nuevos, no se encuentran regulados por ninguna legislación, aunque los jueces utilizan actualmente el Código Civil y el Penal adaptándolo a las circunstancias.

Se propuso un cambio al Código Penal a través del cual se incorporen figuras específicas del tratamiento de sistemas de la información, de informática y comunicaciones, ya que el vacío legal existente imposibilita muchas veces penalizar los delitos, y tenemos una situación desventajosa a nivel internacional.

En Infobaeprofesional.com, Los delitos informáticos siguen sin tener castigo penal, Patricio Eleisegui expresa: "... En diálogo con Infobaeprofesional.com, Martín Carranza Torres, abogado especializado en propiedad intelectual y derecho de alta tecnología, remarcó los problemas que ocasiona la demora en la aprobación de leyes concretas para el ámbito tecnológico y señaló las imprecisiones de la iniciativa aprobada en Diputados...Carranza Torres señaló en los inconvenientes que se derivan de no establecer jurisdicciones claras y definidas a uno de los principales problemas que enfrenta el derecho para regular el desempeño en Internet.

"La tecnología ha creado problemas nuevos, entre ellos la dificultad de reunir pruebas para penar un delito. Hoy, por ejemplo, es posible perpetrar un ataque desde servidores ubicados en distintos países o a través de computadoras 'robots' y eso hace difícil rastrear desde donde se originó la agresión y a quien castigar por ella", explicó...Con relación al modo en que se castigan hoy algunos delitos cometidos con herramientas informáticas en la Argentina, el especialista afirmó que "en los pocos casos que se denuncian se aplican normas generales porque no hay disposiciones específicas. Sostuvo que los casos más complicados están relacionados con el monitoreo indebido del correo electrónico, una práctica que genera debate dada la ausencia de reglas claras que ostentan algunas empresas para con sus empleados...

Otro de los temas más complejos en materia de legislación vinculada a cuestiones informáticas está relacionado, directamente, con el monitoreo del correo electrónico en espacios laborales...

"Suele suceder que las empresas no tienen reglamentado el uso de herramientas informáticas que, vale decirlo, son de su propiedad. Si la empresa no aclara cómo debe ser la utilización del e-mail corporativo, está bien que la privacidad del mismo se haga respetar", dijo Carranza Torres.

"Igualmente, la solución a este problema pasa por la expectativa de privacidad del correo que tenga el empleado. Es necesario romper esa expectativa, y por eso en caso de monitoreo siempre debe hacerse con previo aviso. Otra opción es permitir carpetas de correo personal que no sean monitoreadas, como las que ya permiten algunas empresas", agregó.

El proyecto en tratamiento establece tipos de delitos contra la privacidad pero, según argumentó Carranza Torres, "no aborda de manera específica la cuestión del correo electrónico laboral" por lo cual, de ser aprobado el pliego, lejos estará éste de clausurar un punto que en el último tiempo ha generado más de una polémica...

..."A no ser por las empresas del sector tecnológico, la mayoría de las compañías no toman conciencia de los perjuicios que pueden ser provocados o sufridos con una PC; el riesgo que puede implicar, por ejemplo, la circulación sin control de información confidencial o las posibilidades de robo que esto permite", concluyó..."

El Dr. Pablo Moreda, funcionario de la Justicia Civil, en el Congreso Legal & Privacy - Contingencias Legales en el uso de la Tecnología, dentro de Infosecurity, 2007, realizado el 7 de junio en el Hotel

Sheraton de Buenos Aires, explicó qué responsabilidad les competen a las organizaciones por los hechos realizados por sus dependientes, y los aspectos patrimoniales que estos hechos tienen, ya que la responsabilidad de una persona en un ilícito informático, como agente directo o como dependiente de una organización, queriendo efectuar el ilícito o no siendo consciente de que el hecho afectaba a otras personas o instituciones, implica responder por el mismo, por ese daño y afecta el aspecto patrimonial de las organizaciones.

Entonces existen a través del uso de las nuevas tecnologías, por el uso de una página WEB, se debe responder si se determina un daño a otros, por ejemplo si utilizó en la página una imagen que es exclusiva de una empresa, el mail es una actividad riesgosa?, a pesar de que no está previsto en el Código Civil, si existe el riesgo de la cosa, por ejemplo es riesgoso el correo spam (no deseado), y a pesar de que existe un vacío legal, se complementa con el art. 1067 del Código Civil, que es el concepto genérico de la cosa.

Ahora bien, no hay responsabilidad sin culpa, pero se puede obrar sin intención (sin dolo), pero dañoso, cuando uno envía un mail, no tiene intención de causar un daño, pero si fui imprudente o negligente en mi envío de correo spam, debería haber tomado más precauciones, ya que sino soy culpable, ya que no actué como las normas me lo pedían.

La responsabilidad del empleador por su dependiente está determinada en el art. 1113 del Código Civil, como ejemplo podemos decir que si un empleado envía un correo afectando la intimidad y privacidad de un tercero, baja un software ilegal, implementa en una página WEB de la empresa una imagen que se encuentra registrada por una organización etc., el responsable es el dueño de la casilla de correo, o sea el empleador de ese dependiente.

Qué requisitos se deben cumplir, según Pablo Moreda, debe ser:

— dependiente de la organización,

— debe actuar dentro del marco de su incumbencia,

— el hecho se encuentra prohibido por ley, y

— debe haber causado un daño, en este caso procede la responsabilidad de la organización producida, por el hecho, con la cosa, de la cosa y por la cosa.

El riesgo de la cosa informática, puede estar dado por mails, software, hardware, etc., que pueda causar, injurias, afectar la privacidad de la persona, etc.

Además por el art. 907 del Código Civil, existen hechos involuntarios, que lo comete la propia cosa porque es en sí misma riesgosa y responde el dueño o guardián de la cosa, (objeto material susceptible de tener un valor según el art. 2311 del Código Civil).

Pero por la ley 17.711 existen cosas que no son cosas, y las disposiciones referentes a las cosas las aplicaremos a la energía y a las fuerzas naturales susceptibles de tener valor, y el mail entra dentro de éste concepto de cosa.

Los hechos cometidos por incapaces, como ser nuestros hijos menores, también pasan a ser nuestra responsabilidad.

3- Normativa nacional

— Con respecto al Estado se creó el ARCERT, en 1999, que es una unidad de respuesta ante incidentes en redes que centraliza y coordina los esfuerzos para el manejo de los incidentes de seguridad que afecten los recursos informáticos de la Administración Pública Nacional, es decir ante cualquier ataque o intento de penetración a través de sus redes de información el organismo actúa coordinadamente.

Desde abril del 2004 pasó a ser miembro de FIRST, que es un órgano coordinador de CERT a nivel internacional, que tiene 41 países miembros y 188 equipos de trabajo, y forma parte del subgrupo 13 del MERCOSUR, y es el punto de contacto para la OEA.

Los distintos CERT, internacionales comunican y difunden información con el fin de neutralizar dichos incidentes, y ataques, en forma preventiva o correctiva, y notifican también tanto al sector público como al privado, ya que los ataques informáticos no vienen discriminados por sector y nos notifican si detentan que Argentina se encuentra bajo ataque informático.

Además se encargan de capacitar al personal técnico afectado a las redes de los organismos del Sector Público Nacional, en eventos que organiza el FIRST y actúan como repositorio de toda la información sobre incidentes de seguridad, herramientas y técnicas de defensa.

Se estableció a través de la ley 25.326 - dec. 995/2000 - dec. 1558/2001, Res. 325/2002 - Disposiciones 1 y 2/2003 - dec. 1187/2003 - Res. 40/2004 - Disposiciones 1 y 4/2004 - Res. 415/2004 - Disposiciones 2, 3, 6 y 7/2005 - Res. 1133/2005 - Res. 15/2005 - Disposiciones 2, 5, 8, 9 10 y 11/2006 y Res. 1022/2006, la protección de datos personales, las medidas de seguridad para el tratamiento y la conservación de los mismos.

La ley 25.326 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 art. 43, párrafo tercero de la Constitución Nacional, y que las disposiciones de la ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

Se determina que tratamiento de datos son las 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.

Que el responsable de archivo, registro, base o banco de datos es la persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.

Que respecto de las medidas de protección se especifica de conformidad con lo prescripto por el art. 9° de la ley 25.326, que el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales, a fin de evitar su adulteración, pérdida, consulta o tratamiento no autorizado y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Que a tal fin, se establece un **Documento de Seguridad de Datos Personales,** como instrumento para la especificación de la normativa de seguridad, el que deberá adecuarse en todo momento a las disposiciones vigentes en la materia dictadas por la Dirección Nacional de Protección de Datos Personales.

Que asimismo, se establecen 3 niveles de seguridad: Básico, Medio y Crítico, conforme la naturaleza de la información tratada, pautas aplicables también a los archivos no informatizados (registros manuales).

— Las medidas de seguridad de nivel básico que deberán adoptar los archivos, registros, bases y bancos de datos que contengan datos de carácter personal son las que a continuación se detallan:

Disponer del Documento de Seguridad de Datos Personales en el que se especifiquen, entre otros, los procedimientos y las medidas de seguridad a observar sobre los archivos, registros, bases y bancos que contengan datos de carácter personal.

Deberá mantenerse en todo momento actualizado y ser revisado cuando se produzcan cambios en el sistema de información.

Deberá contener:

1. Funciones y obligaciones del personal.

2. Descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan.

3. Descripción de las rutinas de control de datos de los programas de ingreso de datos y las acciones a seguir ante los errores detectados a efectos de su corrección. Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento (batch, interactivo, etc.), deben incluir en su diseño, rutinas de control, que minimicen la posibilidad de incorporar al sistema de información, datos ilógicos, incorrectos o faltantes.

4. Registros de incidentes de seguridad.

4.1. Notificación, gestión y respuesta ante los incidentes de seguridad.

5. Procedimientos para efectuar las copias de respaldo y de recuperación de datos.

6. Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su

uso.

7. Procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información. La relación entre el usuario autorizado y el/los sistemas de información a los que puede acceder debe mantenerse actualizada. En el caso en que el mecanismo de autenticación utilice contraseña, la misma será asignada por el responsable de seguridad de acuerdo a un procedimiento que garantice su confidencialidad. Este procedimiento deberá prever el cambio periódico de la contraseña (lapso máximo de vigencia) las que deberán estar almacenadas en forma ininteligible.

8. Control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados.

9. Adoptar medidas de prevención a efectos de impedir amenazas de software malicioso (virus, troyanos, etc.) que puedan afectar archivos con datos de carácter personal. Entre otras: 1) Instalar y actualizar, con la periodicidad pertinente, software de detección y reparación de virus, ejecutándolo rutinariamente; 2) Verificar, antes de su uso, la inexistencia de virus en archivos recibidos a través de la web, correo electrónico y otros cuyos orígenes sean inciertos.

10. Procedimiento que garantice una adecuada Gestión de los Soportes que contengan datos de carácter personal (identificación del tipo de información que contienen, almacenamiento en lugares de acceso restringidos, inventarios, autorización para su salida fuera del local en que están ubicados, destrucción de la información en desuso, etc.).

Nota: Cuando los archivos, registros, bases y bancos contengan una serie de datos personales con los cuales, a través de un determinado tratamiento, se permita establecer el perfil de personalidad o determinadas conductas de la persona, se deberán garantizar las medidas de seguridad del presente nivel más las establecidas en los puntos 2, 3, 4 y 5 del siguiente.

— Las medidas de seguridad de nivel medio que deberán adoptar los archivos, registros, bases y bancos de datos que contengan datos de carácter personal de las empresas privadas que desarrollen actividades de prestación de servicios públicos, así como los archivos, registros, bases y bancos de datos pertenecientes a entidades que cumplan una función pública y/o privada que, más allá de lo dispuesto por el art. 10 de la ley 25.326, deban guardar secreto de la información personal por expresa disposición legal (v.g.: secreto bancario), además de las medidas de seguridad de nivel Básico, deberán adoptar las que a continuación se detallan:

1. El Instructivo de seguridad deberá identificar al Responsable (u órgano específico) de Seguridad.

2. Realización de auditorías (internas o externas) que verifiquen el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad para datos personales.

Los informes de auditoría pertinentes, serán presentados al Responsable del Archivo a efectos de que se adopten las medidas correctivas que correspondan. La Dirección Nacional de Protección de Datos Personales, en las inspecciones que realice, deberá considerar obligatoriamente, con carácter no vinculante, los resultados de las auditorias referidas precedentemente, siempre que las mismas hayan sido realizadas dentro de un período máximo de un año.

3. Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

4. Se establecerá un control de acceso físico a los locales donde se encuentren situados los sistemas de información con datos de carácter personal.

5. Gestión de Soportes e información contenida en ellos,

5.1. Se dispondrá de un registro de entradas y salidas de los soportes informáticos de manera de identificar, día y hora de entrada y salida del soporte, receptor, emisor, forma de envío, etc.

5.2. Se adoptarán las medidas necesarias para impedir cualquier recuperación de la información con posterioridad a que un soporte vaya a ser desechado o reutilizado, o que la información deba ser destruida, por la causa que correspondiere. Asimismo se deberán adoptar similares medidas cuando los soportes, o la información (ej.: cuando se hacen copias de respaldo a través de una red de transmisión de datos, la información sale de un soporte local y viaja hasta otro remoto vía dicha red.), vaya a salir fuera de los locales en que se encuentren ubicados,

5.3. Deberá disponerse de un procedimiento de recuperación de la información de respaldo y de

tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales.

6. Los registros de incidentes de seguridad, en el caso de tener que recuperar datos, deberán identificar la persona que recuperó y/o modificó dichos datos. Será necesaria la autorización en forma fehaciente del responsable del archivo informatizado.

7. Las pruebas de funcionamiento de los sistemas de información, realizadas con anterioridad a su puesta operativa no se realizarán con datos/archivos reales, a menos que se aseguren los niveles de seguridad correspondientes al tipo de datos informatizados tratados.

— Las medidas de seguridad de nivel crítico (quedan exceptuados de aplicar las medidas de seguridad de nivel crítico, los archivos, registros, bases y bancos de datos que deban efectuar el tratamiento de datos sensibles para fines administrativos o por obligación legal. No obstante, ello no excluye que igualmente deban contar con aquellas medidas de resguardo que sean necesarias y adecuadas al tipo de dato), que deberán adoptar los archivos, registros, bases y bancos de datos que contengan datos personales, definidos como "datos sensibles", con la excepción que se señalará más abajo, además de las medidas de seguridad de nivel Básico y Medio, deberán adoptar las que a continuación se detallan:

1. Distribución de soportes: cuando se distribuyan soportes que contengan archivos con datos de carácter personal —incluidas las copias de respaldo—, se deberán cifrar dichos datos (o utilizar cualquier otro mecanismo) a fin de garantizar que no puedan ser leídos o manipulados durante su transporte.

2. Registro de accesos: se deberá disponer de un registro de accesos con información que identifique al usuario que accedió, cuando lo hizo (fecha y hora), tipo de acceso y si ha sido autorizado o denegado. En el caso que el acceso haya sido autorizado se deberá identificar el dato accedido y el tratamiento que se le dio al mismo (baja, rectificación, etc.). Este registro de accesos deberá ser analizado periódicamente por el responsable de seguridad y deberá ser conservado como minino por el término de 3 años.

3. Copias de respaldo: además de las que se mantengan en la localización donde residan los datos deberán implementarse copias de resguardo externas, situadas fuera de la localización, en caja ignífuga y a prueba de gases o bien en una caja de seguridad bancaria, cualquiera de ellas situadas a prudencial distancia de la aludida localización. Deberá disponerse de un procedimiento de recuperación de esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales.

4. Transmisión de datos: los datos de carácter personal que se transmitan a través de redes de comunicación (se trata de comunicaciones que salgan fuera de la red de la organización) deberán serlo cifrados o utilizando cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas.

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. Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.

Además los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido, y la recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley, los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención, los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario, los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el art. 16 de la presente ley, los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular, y los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

La Dirección Nacional de Protección de Datos Personales ha lanzado la Red Argentina de Protección de Datos Personales (RAPDP) invitando a participar a todas las provincias argentinas, a fin de garantizar la protección integral de los datos personales.

La Red Argentina de Protección de Datos Personales consiste en proponer un sistema de estructuras administrativas provinciales ideado para asegurar de la protección de los datos personales en todo el territorio nacional.

Cada estructura se desempeñará como nodo de Red independiente y serán creadas según el criterio de cada provincia, trabajando en conjunto con la Dirección Nacional de Protección de Datos Personales.

El principal objetivo de la Red Argentina de Protección de Datos Personales es el de **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, conforme lo establecido por la Red Argentina de Protección de Datos Personales, entre otros que se propongan, tendrá los siguientes objetivos:

— Hacer cumplir la legislación sobre protección de datos personales y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso y rectificación de los datos personales.

— Informar a los ciudadanos de todo el país acerca de los derechos en materia de protección de datos personales, y también de los procedimientos de reclamo que existan para su protección y defensa.

— Vincular a las unidades provinciales (llamados nodos) con la Dirección Nacional de Protección de Datos Personales, desarrollando acciones conjuntas en materia de registración de bases de datos, capacitación de recursos humanos, inspecciones y relevamientos a nivel provincial y nacional

4- Ejemplos

Primero

En Noticiasdot.com, José María Luque Guerrero de la Comisión de seguridad en la red expresa: "...Aparece el "PhishingCar": Nueva forma de estafar por Internet. ... captación de compradores de coches a un costo muy bajo, la venta nunca se efectúa, esta persona realiza un pago como señal, se queda sin dinero y sin coche. La pesca de incautos de compradores de coches. Nos intentan "pescar" (phishing) con cualquier tipo de engaño (ingeniería social) para que facilitemos nuestras claves, datos, todos nuestros datos. ¿Quién no ha recibido un ataque de phishing bancario, de Ebay de Paypal, Scam (trabajos falsos)?. Los ciber-delincuentes encontraron una nueva forma más directa para robarle su dinero, el reclamo de un artículo a bajo costo y además es usted el que les entrega el dinero. Es más rápido que el phishing tradicional y más económico para el estafador. Las personas dedicadas a la seguridad informática tienen dos puntos de referencia, la seguridad basada en el tráfico (control de conexiones) y seguridad basada en el usuario (control de admisión de usuarios), pero todo esto se queda corto, ahora nos hace falta dar un paso más: "enseñar seguridad al usuario final".

Parece un poco absurdo pero recuerdan cuando eran pequeños y en su colegio llego un policía y durante una semana les enseñó seguridad vial, "enseñarnos a cruzar por un paso de peatones", en internet también tenemos que enseñar y concienciar de "los nuevos peligros". Negar el crecimiento de fraude sería cerrar los ojos a la realidad, la Asociación de Internautas lleva varias campañas de seguridad en la red, enseñando al usuario luchar contra virus, troyanos, intrusiones, spyware, etc. pero el avance de las tecnologías nos hace ahora dar un paso más y realizar campañas contra el fraude, el peligro ya no son los virus, códigos malware, el peligro ahora se llama phishing.a de ejecución más fácil, cómoda, rápida y económica de obtener dinero. El nuevo formato le hemos llamado "Phishing-Car" para diferenciarlo del ataque tradicional bancario, pescando incautos con ganas de comprar un coche muy barato. La víctima es la ideal, los reclamos se producen por medio de llamativas ofertas en vehículos lujosos, incluso tienen web trampas con nombre de dominios muy similares a empresas con mucho prestigio que se dedican a la venta de vehículos de ocasión, pero todos los fraudes tienen algo en común:

— El pago se realiza por medio de empresas de envió de dinero a otros países (Tipo Western Unión, Money Gram).

— El vendedor le oferta la entrega a domicilio.

— En un 90% el vehículo que venden está fuera de su país, de esta manera usted sólo puede verlo en fotos.

— Le piden primero el 30% ó el 40% del precio ofertado como primera seña.

— Captan a las víctimas por medio de anuncios en web de venta de coches o de segunda mano y por supuesto la recepción de correos electrónicos.

— Muchas veces el vendedor dice que es un español que vive en Gran Bretaña y por motivos laborales

de estancia en el país inglés, tiene que cambiar de forma urgente de coche porque se conduce por la izquierda y su coche al estar matriculado en España el volante está al lado contrario y no se adapta, por este motivo vende el coche de forma muy económica, te enseñan un coche matriculado en España.

— La mayoría de los estafados enviaron el dinero a Reino Unido, esto no quiere decir que cambien.

La Asociación de Internautas cuenta con un servicio operativo desde hace meses para todos aquellos internautas que quieran reportar información sobre este tipo de fraudes realizados por medio de Phishing, con sólo mandar un correo y adjuntar la información a; phishing@internautas.org

Se estudia el caso y se comunica a las Fuerzas de Seguridad del Estado para cursar la denuncia junto a un comunicado de aviso a la entidad suplantada..."

Segundo

Se da el caso de una Editorial, la cual, se dedica a la edición de folletos, catálogos y guías de productos para terceras empresas que solicitan dicha impresión.

La empresa editora, tiene como empleado, a un profesional especializado, quien efectúa las tareas de programar, armar, compaginar y diseñar las páginas de los catálogos que se editan.

Este profesional, utiliza para efectuar dichas tareas, programas informáticos especializados, como ser Ilustrador, Corel Draw y Photoshop, entre otros y tiene acceso a la Base de Datos de dicha empresa editorial, en forma completa, pues en este caso, siendo una empresa mediana, no cuenta con medidas de seguridad, que protejan los datos muy sensibles que se encuentran almacenados en dicha base de datos y a la que tiene acceso además, todo el personal de la empresa.

En determinado momento, el profesional gracias al acceso que tiene respecto a esa Base de Datos, la copia completa, e inicia acciones legales respecto a su empleadora, por estimar que esta última se encontraba incumpliendo la legislación vigente, (no voy a analizar si era real o no este hecho, pues para lo que se está examinando no tiene importancia).

Pero le puede pasar a más de una empresa, si no tiene las mínimas medidas de seguridad con respecto a los usuarios que tienen acceso a los Sistemas y Bases de datos de las mismas, y que por ley son obligatorias contar.

En el caso que estoy tratando, el profesional había agregado a la causa judicial, copia en CD de la siguiente información de la Editorial, que había sido su empleadora:

— Todos los datos correspondientes a la clientela de todo el país, con sus domicilios, teléfonos, personal responsable de compra, productos que compraban, precios, forma de pago, etc.

— Cartas con cotizaciones, folletería y documentación inherente a la comercialización completa de la editorial.

— Fotos de los productos editados.

— Mails de intercambio de todo el personal, sus directores, con proveedores, clientes, y otros profesionales.

— Facturación y saldos de pagos de todos los clientes.

— Currículum Vitae de los directivos de la Empresa Editora.

— Saldos bancarios

— Datos respecto a los cheques emitidos para proveedores.

— Listado de fabricantes e importadores de productos de librería.

— Listado de proveedores.

— Contratos de trabajo de la Empresa Editora con clientes.

— Agendas completas de proveedores y clientes.

— Listados de catálogos con precios.

— Ofertas

— Logotipos de clientes

— Etc.

Esta documentación se presentó en una causa judicial, pero ninguna de las partes, ni el Tribunal, interpretó que la documentación agregada al expediente era un delito informático (por robo de los datos sensibles correspondientes a una Base de Datos de una empresa).

La realidad es que sin la legislación correspondiente va a ser muy difícil la penalización de los delitos informáticos.

Así como en este caso, el personal de una organización que tiene acceso a una Base de Datos que abarca por ejemplo todos los contribuyentes de un distrito, si no se cuenta con restricciones a su acceso y copiado, puede copiar dichos datos y venderlos al mejor postor, con las implicancias que estos hechos conllevan para todos los ciudadanos.

Siendo obligación por la legislación vigente la protección de los datos que se encuentran informados en las Bases de Datos de Empresas, Organizaciones, Instituciones Públicas y Privadas en general, deberíamos tomar conciencia de las implicancias que el acceso libre a usuarios y personal significa para dichas organizaciones y la responsabilidad que las mismas tienen en estos hechos.

5- Jurisprudencia

Han existido fallos contra bancos por su responsabilidad en su propia página WEB, o a empresas por el envío de correos no deseados (SPAM), o por el uso de imágenes que son propiedad intelectual de una empresa, o por bajarse de Internet (suelen hacerlo los empleados, nuestros propios hijos), videos, películas o música sin pagar los derechos correspondientes.

1. Hubo un caso en la Justicia Civil, el del Lloyds Bank, que perdió un juicio de daños y perjuicios efectuado por un cliente que entendió se veía afectado su honor y privacidad, ya que en Internet, por un error de un empleado del banco, se lo incluyó con datos falsos de una deuda inexistente.

El banco reconoció el error, pero respondió patrimonialmente por el hecho, ya que la persona que se encontró involucrada en éste hecho, estuvo afectada moral, psíquica y espiritualmente y en su honra personal.

2. También en la Justicia Comercial se ha hecho lugar al daño y perjuicio y daño moral en el reclamo de empresas y particulares contra varias entidades bancarias que hicieron aparecer a un titular de una cuenta bancaria a quien se le habían sustraído ciertos cheques y al ser presentados al cobro los rechazó por **emisión de cheques sin fondos disponibles,** en lugar de **orden de no pagar,** o que se vieron involucrados como titulares de multas impagas, siendo este hecho incorrecto, y los inhabilitaron para operar en cuenta corriente en una o varias cuentas de una sociedad o particulares, que además como consecuencia de la información errónea en sus bases de datos, quedaron inhabilitados para operar en el circuito bancario en general, ya que la información fue enviada al Banco Central de la República Argentina.

No importa que no se haya tenido intención de efectuar un daño, el hecho concreto es que el personal del Banco cometió un error y esto posibilitó, que afectaran los intereses patrimoniales de la sociedad, o de la persona involucrada en tal hecho, y que el sentimiento de vergüenza e impotencia por afectación del propio prestigio generado por la inexacta circunstancia de aparecer en las bases de datos de carácter público como inhabilitado involucrado en una situación de insuficiencia crediticia, que en realidad se originó en informes erróneos de los bancos, en cuestión, implicó una compensación por el daño y perjuicio, y daño moral ocasionado.

3. También, corresponde la compensación por daños y perjuicios y daño moral, según la Justicia Comercial, cuando la inclusión indebida en los informes comerciales que emiten las empresas de riesgo crediticio, provocan un sustancial perjuicio al nombre comercial de cualquier sujeto allí incluido, pues afecta su giro ordinario, lo que causa padecimientos lógicos a quien es así calificado, máxime, considerando que la publicidad generalizada que hoy brindan las bases de datos informatizadas, provocan una exposición pública sorprendente cuyos límites son difíciles de mensurar; de manera que, encontrarse calificado de un modo erróneo en tales bases, como deudor contumaz, produce una lógica afectación a la tranquilidad y el ánimo de cualquier comerciante que conoce que su permanencia en tales condiciones lo hará pasible de ser descartado aún en negocios que ignora de allí que el nerviosismo que tal hecho genera y las urgentes gestiones para aclarar el punto y luego obtener su cese, encuadran en el daño moral susceptible de reparación por parte del banco que emitió la información errónea.

4. Además la Cámara Comercial entendió procedente la demanda deducida por la propietaria de un negocio comidas rápidas y delivery contra dos empresas dedicadas a la comercialización de Bases de Datos de teléfonos por los daños y perjuicios derivados de la errónea publicación del teléfono de la accionante en el rubro boutiques, y fijar un monto en concepto de indemnización por pérdida de chance, o

sea en razón de haber quedado acreditada la frustración de una posibilidad de obtener ingresos.

6- Conclusión

Las empresas, organismos e instituciones deberían contar con una política de prevención para el caso de contingencias que afecten sus organizaciones, tal como existen políticas institucionales para casos extremos en edificios, por incendios, etc, tendría que tomarse conciencia de la necesidad de instalar y actualizar en forma permanente (ya que los delitos informáticos se actualizan a una velocidad mayor que las soluciones para los mismos) de forma tal que ante una contingencia en sus equipos informáticos no se vea afectada la actividad empresarial o de la organización, lo que podría implicar pérdidas millonarias.

Se podría implementar una política para bloquear a los empleados el uso de Internet y salvo los autorizados expresamente que no se pueda tener acceso de cualquier lugar de la empresa a las Bases de Datos sensibles de los organismos, y si los dependientes deben comunicarse con clientes, contratistas, proveedores, etc., por su trabajo, que tengan bloqueados los sitios claves a través de donde pueden bajarse películas, música, etc, que son ilegales sin el pago de los derechos correspondientes, y así no verse afectados los intereses patrimoniales de las empresas.

Actualmente, la Justicia Europea tiene un mecanismo de interconexión de delitos penales, que permite intercambiar información sobre condenas impuestas en los estados miembros, como mecanismo de respuesta a la creciente transnacionalización de la delincuencia, especialmente del terrorismo, el delitos informáticos y el tráfico de drogas.

Es que para el sistema jurídico Europeo, el conocimiento de que un encausado tiene antecedentes penales en otros países es necesario, para aplicar la agravante de reincidencia internacional y permite tener constancia de indicios sobre la peligrosidad del encausado.

A nivel Latinoamericano, muchos países de la región cuentan con leyes específicas para sancionar los delitos informáticos, y nuestro país no puede seguir sin solucionar dicho problema.

Debemos tomar conciencia que la seguridad de la información es clave para todas las empresas, organizaciones y organismos, y actuar en cada lugar en consecuencia.

Bibliografía

Segu Info.com.ar, Legislación y delitos informáticos.

Infobaeprofesional.com, Los delitos informáticos siguen sin tener castigo penal, Patricio Eleisegui.

Noticiasdot.com, José María Luque Guerrero de la Comisión de seguridad en la red.

Delitos informaticos.com.