El problema de los datos personales y el espionaje en Internet

Dra. Esc. María José Viega

1. Introducción

Como miembro del Instituto me ha correspondido hablar en el día de hoy sobre la privacidad en Internet. Y como ya he hablado en otras oportunidades -sobre este tema- en las Jornadas del Instituto, sobre las huellas digitales que vamos dejando a través de esta superautopista de la información, me pareció oportuno en esta oportunidad, ver no solo este aspecto, sino también las "actividades" externas, las intromisiones no autorizadas (aunque no siempre) en nuestros sistemas y por ende en nuestra vida íntima o privada.

Y es que hoy por hoy se entiende que la vida privada no se limita exclusivamente a la intimidad, sino que este concepto ha sido sustituido por uno más general como es el de privacidad[1].

La privacidad es un tema que puede ser enfocado desde múltiples ópticas, desde el cruzamiento de ficheros en soporte papel, el de ficheros electrónicos, la privacidad desde la óptica del consumidor y de las telecomunicaciones (sean por cable o inalámbricas) y nuestro tema de hoy, son las connotaciones en el ámbito de Internet.

Se ha calificado a Internet como una amenaza en la difusión de elementos relativos a la persona, por ser un medio masivo y polifacético de comunicación. Tal es así, que hemos analizado en otra oportunidad[2] las diferentes clases de comunicaciones a través de la Red y las hemos comparado con las comunicaciones "tradicionales", estudiando similitudes y diferencias con la correspondencia privada, la prensa escrita y la radiodifusión.

Para comenzar a reflexionar sobre este tema me gustaría que cada uno pensara sobre las siguientes preguntas:

¿Hay alguien escuchando nuestras llamadas telefónicas?

¿Qué tan seguro es enviar un fax?

¿Alguien lee nuestros mail? ¿Y nuestros chat? ¿Es posible que alguien recupere a través del proveedor lo que escribimos hace unos meses?

---

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

[2] VIEGA, María José. "Derechos Humanos en el Ciberespacio". Trabajo publicado en la Revista electrónica de Derecho Informático (REDI), Junio de 2002.

¿Es realmente importante la privacidad para cada uno de nosotros?

En los hechos la mayor parte de las personas ceden sus datos a cambio de puntos, millas, etc. sin tener conciencia que nos estamos identificando, que estamos dando información sobre nuestros hábitos, consumo, y no conocemos la utilización posterior que se realizará con los mismos.

Ahora bien, ¿"alguien" nos espía?

Según el diccionario espía es una persona que con disimulo y secreto observa o escucha lo que pasa, para comunicarlo al que tiene interés en saberlo.

¿Quien nos espía a través de Internet?

El Gobierno, las empresas, los ciberdelincuentes.

¿Para que nos espían?

Depende de la respuesta que demos a la pregunta anterior serán los motivos. Los gobiernos en aras de la seguridad nacional, las empresas buscan crear perfiles de usuarios a los efectos de ofrecernos productos que sean de nuestro interés, lo que tendrá como resultado el spam, también existe el espionaje entre empresas el cual implica competencia desleal y los ciberdelincuentes obviamente desean obtener nuestros datos para obtener un beneficio con la utilización de los mismos.

¿Cómo nos espían?

"En el pasado, si el Gobierno quería violar la privacidad de los ciudadanos tenía que dedicar una cierta cantidad de esfuerzo para interceptar, abrir al vapor y leer el correo de papel. Esto es similar a pescar con una caña, un pez cada vez. Afortunadamente para la libertad, esta vigilancia que requiere tanto esfuerzo no es práctica a gran escala. Hoy en día, el e-mail está reemplazando al correo convencional y, a diferencia de éste, los mensajes electrónicos son facilísimos de interceptar y escudriñar buscando palabras clave. Esto se puede llevar a cabo de manera rutinaria, automática, indetectable y a gran escala. Es similar a la pesca con red de arrastre, lo que constituye una diferencia orweliana para la salud de la democracia"[3].

George Orwell escribió una novela en el año 1948 de ciencia ficción titulada "1984" en la cual nos presenta el mundo del futuro dividido en tres estados totalitarios. El protagonista es el símbolo de la rebelión contra el poder de un estado policíaco (bajo el control del Gran Hermano) que ha llegado a apoderarse de la vida y la conciencia de todos sus súbditos, interviniendo en las esferas más íntimas de los sentimientos humanos[4].

[3] ZIMMERMANN, autor del paquete criptográfico PGP, citado por García Mostazo Nacho en "Libertad Vigilada. El espionaje de las comunicaciones". Ediciones B. Barcelona, 2003.
[4] ORWN George. 1984. Ediciones Destino. Barcelona. Séptima edición, junio 1984.

Si quien nos espía es el Estado, la pregunta relevante es: ¿estamos dispuestos a "perder" nuestra intimidad, nuestra privacidad debido a la Seguridad Nacional, de nuestro o de un tercero país. ¿Cuáles son los límites? ¿Somos concientes de los alcances?

2. Las primeras amenazas a la privacidad en Internet

A los efectos de buscar una protección en torno a este tema, tenemos que ponderar dos intereses diferentes, por un lado la protección de la vida privada y por otro el interés de la sociedad toda en que circule cierta información.

Internet entonces, nos replantea el desafío a los efectos de la protección de los datos personales, desafío que se originara a raíz del proceso de informatización de las bases de datos, convirtiendo los ficheros manuales en electrónicos, haciendo posible el relacionamiento de los mismos, así como el cruzamiento de bases de datos, a los efectos de lograr un perfil lo más acabado posible acerca de un individuo.

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[5].

Para enfrentar este desafío debemos tener en cuenta los siguientes elementos[6]: el hecho que la infraestructura de Internet esté basada en datos personales, nuevas formas de distribuir información, también los instrumentos técnicos utilizados son nuevos, y la información utilizada para las actividades en líneas.

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

Una discusión muy interesante que se ha planteado es si un numero IP es un dato personal (o dicho número en un instante, porque hay IP variables o rotativos), y si se puede acceder a dicha información sin el consentimiento del usuario.

La Agencia de Protección de Datos Española[7] ha interpretado de esta manera y ha declarado a la dirección IP como dato personal.

¿Es un dato personal o es como dicen los técnicos simplemente un número referenciador?, ¿este número IP puede llegar a considerarse un bien?

El Dr. José Luis Barzallo entiende[8] que la dirección IP es un identificador y una dirección de correo electrónico y que no cumple con los elementos necesarios para considerase como un dato personal. Sin embargo algunas legislaciones, que han avanzado con el tratamiento del tema, ya lo han considerado como tal y lo protegen. Podría considerarse como un dato personal, pero no de aquellos sometidos a

[5] VIEGA, María José. "Privacidad en Internet". Derecho Informático. Tomo II. Fundación de Cultura Universitaria. Montevideo, 2001.
[6] ARAGON 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)
[7] https://www.agpd.es/index.php?idSeccion=390
[8] BARZALLO José Luis. Comunidad alfa-redi www.alfa-redi.org

protección por ser privados, confidenciales o sensibles. Tampoco debemos dejar de lado que el dato personal fue desarrollado por la doctrina de defensa de los derechos humanos para el individuo, entonces las personas jurídicas tienen otras figuras protegidas por otras ramas del derecho como la propiedad intelectual. Podría ser considerado como un bien cuando es fijo y cumpliendo requisitos como una titularidad que alguien tenga sobre ese bien.

Pero debemos ser más precisos y preguntarnos ¿qué sucede si es un numero IP fijo?, porque en este caso identifica a un usuario en el sistema. Tengamos presente que en realidad lo que identificamos es una maquina, ahora bien, si la misma es usada por un único individuo, ¿no estaríamos ante un dato de ese "individuo" y por tanto un dato personal?

El Dr. Felipe Fontes[9] entiende que el numero IP, es equiparado a la dirección de una persona, por tanto no deja de ser un dato personal, pues la dirección, en su opinión lo es y sólo puede ser divulgado con la autorización del propietario o, por supuesto, por decisión judicial y a veces por cuestión de interés público.

Andrés Guadamuz González[10] nos explica que en el Reino Unido, las direcciones de IP son ahora consideradas datos personales de acuerdo con la legislación de datos personales y la legislación de datos electrónicos. Esto es con respecto a la interpretación que se le esta dando a la sección 14 con respecto a "location data". Se interpreta ahora que las direcciones de IP pueden cumplir este requisito. Con respecto a las direcciones IP en general, el Comisionado de Información (el ente regulador en Reino Unido), ahora interpreta que como la dirección de IP puede usarse para identificar usuarios y es lo que hacen en el Internet, se debe considerar como datos personales. De hecho, en Europa en general se piensa que las direcciones de IP deben ser considerados datos personales (http://www.informationcommissioner.gov.uk/cms/DocumentUploads/what%20are%20personal%20data%20research.pdf)

Según Roberto L. Ferrer Serrano[11], al menos desde el punto de vista de la normativa española, es evidente que puede ser considerado un dato personal, igual da que sea IP fija o no, porque en este último caso, siempre hay medios para asociarla a un usuario concreto. En su opinión, no significa que siempre vaya a ser un dato personal porque su naturaleza de dato personal deriva de su posibilidad de asociarlo a una persona identificada o identificable ex art 3 LOPD. *Artículo 3. Definiciones. A los efectos de la presente Ley orgánica se entenderá por a) Datos de carácter personal: Cualquier información concerniente a personas físicas identificadas o identificables.* Por eso entiende que solamente dejará de ser un dato de carácter personal cuando por cualquier circunstancia no sea posible vincularlo a una persona.

b) un **segundo elemento se refiere a los instrumentos técnicos utilizados**, los software de navegación, por ejemplo, que envían más información de la requerida

[9] FONTES Felipe. Comunidad alfa-redi www.alfa-redi.org
[10] GUADAMUZ GONZALEZ, Andrés. Comunidad alfa-redi www.alfa-redi.org
[11] FERRER SERRANO, Roberto. Comunidad alfa-redi www.alfa-redi.org

para realizar una conexión, como por ejemplo el tipo y lengua del navegador, que otros programas se encuentran instalados, cual es el sistema operativo del usuario, cookies, etc

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

d) **múltiples medios para distribuir información**, ya que a través de la Red podemos enviar mail, comunicarnos a través de chat, de foros, de listas de distribución y por supuesto la información contenida en los sitios web.

Si queremos efectivamente realizar e-commerce vamos a tener indefectiblemente que estar brindado una serie de datos personales, que no necesariamente están acorde con los principios generales que rigen en materia de recolección.

3. Situación en Unión Europea

A nivel de la Unión Europea encontramos:

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

2. 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.

3. **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.

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).

5. El **Grupo de Trabajo sobre protección de las personas** ha dictado una Recomendación 1/1999, en la cual se establece que:

a) el navegador debería informar al usuario que información pretende transferir y con que objeto,

b) cuando existen hipervínculos, el navegador debería indicar el sitio en su totalidad,

c) las cookies deberían informar cuando se está enviando una cookie, que información pretende almacenar, con que objetivo y el período de validez. 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 (Mendoza Luna, Amílcar. "Los cookies: ¿amenaza a la privacidad de información en la internet?. www.derecho.org/redi)

Una noticia dice que[12]: "El inmortal cookie de Google. Este buscador fue el primer motor de búsqueda que usó cookies que expiraban en el 2038. Esto ocurría al mismo tiempo que a las webs federales (USA) se les prohibía usar coockies persistentes. Después de más de dos años, los cookies campan a sus anchas en los motores de búsqueda. Podríamos decir que Google es el que marca el estándar, así que nadie les va a desafiar en este asunto. El cookie de Google, coloca sobre tu disco duro, un número identificativo único (ID). Si es la primera vez que entras, Google te coloca el cookie, si no, te lee y registran tu identificativo. Google registra todo lo que puede. En todas tus búsquedas, Google registra tu identificativo, tu IP, la fecha y la hora, tus términos de búsqueda, y la configuración de tu navegador. De esta forma, Google va personalizando cada vez más, los resultados de tus búsquedas basándose en tu IP. A esto se le suele llamar "entrega basada en geolocalización"."

6. **Directiva 2002/58/CE** – La Protección de Datos sobre tráfico de telecomunicaciones está prevista en esta Directiva del Parlamento Europeo y del Consejo, relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas (Diario Oficial L 201/37), en virtud de la cual el tratamiento de datos de tráfico está permitido, en principio, para facturación y para pagos de interconexión. Tras debates prolongados y explícitos, la retención de datos de tráfico con vistas a la aplicación de ley debería respetar estrictas condiciones de conformidad con el apartado 1 del artículo 15 de la Directiva: es decir, en cada caso sólo por un período limitado y cuando constituye una medida necesaria proporcionada y apropiada en una sociedad democrática[13].

4. Política de Estados Unidos en materia de Protección de datos

[12] www.noticiasdot.com "La cara oculta de Google: Afirman que viola la privacidad de los usuarios y vigila sus actividades online". Página visitada viernes 30 abril 2004.
[13] Dictamen 5/2002 aprobado el 11 de octubre de 2002, sobre la Declaración de los Comisarios responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de setiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones.

Con carácter general podemos decir que en Estados Unidos se ha buscado la protección a través de la autorregulación y el sistema funciona en base a los principios de puerto seguro.

¿Pero qué sucede con el espionaje de las comunicaciones?

Afirma Nacho García que[14]: "las agencias estatales de espionaje siempre han tratado de obtener información a través del llamado espionaje humano (Human Intelligence, Humint), es decir, utilizando a agentes infiltrados. Sin embargo, hay otros sistemas técnicos para llevar a cabo esta misión. Se trata de la inteligencia de señales (Signals Intelligence, Sigint[15]), actividad que consiste en obtener información interceptando las señales electromagnéticas del país objeto de espionaje, sean cuales sean esas señales. Dentro de la actividad del Sigint, una de las facetas más importantes es el espionaje de las comunicaciones (Communication Intelligence, Comint), que consiste en interceptar sólo aquellas trasmisiones que transporten información mediante la interceptación de comunicaciones extranjeras por personas distintas a las que esa información va dirigida.

A partir de 1970, ante la abundancia de información interceptada, programaron computadoras para que las propias máquinas seleccionaran las comunicaciones realmente interesantes, descartando el resto. Este proyecto recibió el nombre de Echelon, que en español puede traducirse como "escalafón", "escalón" o "grado". Los ordenadores contaban con un "diccionario" de palabras clave para buscar entre los mensajes interceptados y entresacar sólo aquellos que contuvieran las citadas palabras. Cada "diccionario" se actualiza regularmente con las llamadas "listas de vigilancia", que iban cambiando en función de las necesidades de información de los gobiernos implicados en la trama de espionaje global[16].

En 1998 nace Echelon II, como una ampliación de la primera. La Agencia de Seguridad Nacional contrató –entre otros- al ingeniero Bruce McIndoe. En 1998, fecha en que Bruce McIndoe abandonó la NSA, Computer Sciences Corporation (empresa contratada por la NSA) concluyó el proyecto para crear Echelón II, lo que coincide con la puesta en funcionamiento de la "máquina de transcripción de la voz humana", ya que la Agencia de Seguridad Nacional solicitó su patente en 1997[17].

La Agencia de Seguridad Nacional no está autorizada para espiar a ciudadanos norteamericanos porque la ley se lo impide. Pero quien puede hacerlo es la Oficina Federal de Investigación (FBI), cuya jurisdicción se circunscribe al interior de las fronteras norteamericanas.

---

[14] GARCIA MOSTAZO Nacho. "Libertad vigilada. El espionaje de las comunicaciones".Ob. Cit., página 16.

[15] http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/04-01.htm Directiva número 6 del Consejo de Seguridad Nacional sobre Inteligencia (NSCID nº 6). "La Agencia de Seguridad Nacional y el Servicio Central de Seguridad".Departamento de Defensa de Estados Unidos, 23 de diciembre de 1971.

[16] GARCIA MOSTAZO Nacho. "Libertad vigilada. El espionaje de las comunicaciones". Ediciones B Grupo Z. Barcelona, enero 2003. Página 18.

[17] GARCIA MOSTAZO Nacho. "Libertad vigilada. El espionaje de las comunicaciones". Ob. Cit., página 116.

En los años 90 el FBI desarrolló un programa llamado "Carnivore" capaz de hacer el seguimiento de un usuario a través de la Red.

En 1994 el Congreso de Estados Unidos aprobó la Ley de Asistencia en Comunicaciones para los Cuerpos de Seguridad (Communications Assistance for Law Enforcement Act, CALEA)[18]. Se establece en esta norma la obligación legal de los operadores de telecomunicaciones y los fabricantes de equipos informáticos de incluir dispositivos de vigilancia en toda la red telefónica de Norteamérica.

Carnivore se instaló a partir de abril del 2000 en los Proveedores de Servicios de Internet (ISP) , se desveló la existencia del mismo por la oposición de una empresa a instalarlo. Como sonsecuencia el programa cambió de nombre y se le denominó DCS1000 Digital Collection System (Sistema de Recolección Digital)[19].

Otro programa es el llamado "Linterna Mágina" que se desarrolló durante el año 2001. Este troyano podría enviarse a cualquier sospechoso, como un adjunto a un mensaje aparentemente inocente. Aprovechándose de algunas vulnerabilidades, podría incluso instalarse sin el conocimiento del destinatario, y a partir de allí capturaría las contraseñas usadas por el supuesto terrorista, enviándolas a las oficinas del FBI.
Linterna Mágica sería parte de un programa más complejo de vigilancia, llamado Cyber Knight (Caballero cibernético), el cuál incluiría una base de datos que permitiría al FBI cruzar información proveniente de e-mails, salas de chat, mensajeros instantáneos tipo ICQ y llamadas telefónicas por Internet. Algunas fuentes consultadas del FBI, ni negaron ni admitieron la noticia, pero declararon que no es nada nuevo que la organización ha estado trabajando con especialistas de la industria de la seguridad, para crear una herramienta que fuera eficaz en combatir tanto al terrorismo, como a otros actos delictivos. Y aunque no debería ser una sorpresa, tampoco es apropiado que se revelen las tecnologías que específicamente se usarán[20].

Las "puertas traseras" que tienen determinados software también son formas de obtener información de los usuarios que utilizan dicho sistema. Un ejemplo de esto fue el caso de Lotus Notes, descubierto por el gobierno sueco en 1997. Se dice que los navegadores fabricados por Microsoft y Netscape tienen incorporados estos sistemas.

El espionaje electromagnético se basa en el hecho de que cualquier aparato eléctrico o electrónico desprende campos electromagnéticos involuntariamente cuando está en funcionamiento. Por lo cual con una antela direccional, un osciloscopio, un sintonizador especial y otros dispositivos capaces de captar y reconstruir a distancia por ejemplo los caracteres que estoy tipiando en un computador.

---

[18] www.askcalea.net Página visitada el 13 de junio 2005.

[19] "Carnivore: The FBI's Email Sniffer"
http://facultyweb.maconstate.edu/jashford/Class%20projects/6pmclass/CarnivorePaperandQuestions.doc

[20] LOPEZ José Luis. "El FBI y sus troyanos". http://www.vsantivirus.com/22-11-01b.htm Página visitada 13 de junio de 2005.

¿Es verdad que nos espían?

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[21]. El informe de Duncan Campbell "Interception Capabilities 2000"[22] se presentó ante el Parlamento Europeo el 22 de febrero de 2000 en sesión abierta a la prensa demostrando la existencia de Echelon, una red mundial de espionaje de las telecomunicaciones.

Los acontecimientos del 11 de setiembre de 2001 en Estados Unidos 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, se reconsidere la legislación existente en materia de protección de datos. 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.

Respecto al programa Carnivore en enero de este año aparece la siguiente noticias[23]: "El Gobierno de EEUU ha abandonado el uso de un programa especial de vigilancia por Internet concebido para leer mensajes electrónicos y otras comunicaciones entre presuntos criminales, espías y terroristas, se informó hoy. La Oficina Federal de Investigaciones (FBI) ha informado al Senado y la Cámara de Representantes del abandono de ese sistema y de que ahora utilizará programas informáticos comerciales para revisar el tráfico informático en el marco de sus investigaciones".

"Los países del tratado UKUSA (Acuerdo secreto firmado en 1948 entre Estados Unidos y Reino Unido, al que adhirieron Canadá, Australia y Nueva Zelanda, entre otras naciones) no son los únicos que lanzaron satélites de espionaje, pincharon cables o instalaron bases para interceptar las comunicaciones de otras naciones. También Alemania, Francia, Israel y Rusia tienen sus sistemas de vigilancia.

5. Las nuevas amenazas (malware) en la Red

5.1 Spyware

El "spyware" es una de las nuevas formas de espionaje en Internet, son programas que se ocultan en los ordenadores de los usuarios y controlan sus

[21] 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.
[22] CAMPBELL Duncan. "Interception Capabilities 2000". http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm
[23] http://www.noticiasdot.com/publicaciones/2005/0105/2001/noticias200105-24.htm Página visitada jueves 20 enero 2005.

actividades. Este tipo de espionaje puede debilitar la potencia del ordenador, averiar la máquina y presentar a los usuarios una gran cantidad de anuncios no solicitados. El objetivo puede ser obtener contraseñas, números de tarjeta de crédito y otros datos de valor.

El problema del espionaje es el hecho de lograr que los consumidores tomen conciencia ya que como las actividades no son visibles como otro tipo de amenazas 'online' no se les presta la atención necesaria o no se toman medidas adecuadas.

Por ejemplo el 'spam' es molesto y por tanto combatido, a pesar que no es peligroso como lo es el espionaje.

Existen algunos programas que han sido etiquetados como "spyware" pueden ser inofensivos, e incluso pueden ayudar al internauta. Muchos programas populares como Kazaa y Morpheus, que permiten a los usuarios copiar música y películas de los discos duros de otros vienen con aplicaciones, sirven anuncios 'pop-up' y otras herramientas de marketing como una forma de subvencionar costes. Los programas "Adware", que pueden instalarse gratuitamente pero incluyen anuncios, como WhenU, no recopilan información personal de los consumidores, según varios ejecutivos, y los usuarios pueden retirarlos con facilidad si lo desean[24].

Hay "spyware" que pueden inhabilitar el ordenador y luego anunciar software para solucionar el problema, otros permiten a través de virus por correo electrónico, obtener el número de cuenta bancaria del usuario y otra información importante. También hay casos que controla el tráfico de Internet, siguiendo la pista de los usuarios sin que los mismos sean concientes y puede resultar difícil de eliminar.

El estado de Utah ha aprobado ya una ley que prohíbe el "spyware". WhenU, al que se impedirá proporcionar anuncios 'pop-up' a los habitantes de Utah, ha recurrido esta ley. Otras compañías dicen que esta norma es demasiado amplia y podía declarar ilegal sin darse cuenta actividades legítimas como apoyo técnico y filtración de contenido. Otros dos proyectos de ley están pendientes en el Congreso de EEUU para prohibir este tipo de espionaje, pero los observadores dicen que es poco probable que se tome una decisión en este año electoral[25].

En febrero de este año se difundió la noticia que WhenU gana su segunda batalla judicial respecto al tema "spywares legales"[26]:

"Una juez estadounidense se negó a bloquear a un proveedor de anuncios 'online' en la modalidad 'pop-up', diciendo que era improbable que pudieran confundir

[24] www.noticiasdot.com lunes, 19 abril 2004

[25] www.noticiasdot.com lunes, 19 abril 2004

[26] http://www.noticiasdot.com/publicaciones/2005/0205/0202/noticias020205/noticias020205-09.htm

Página visitada 2 de febrero de 2005.

a los usuarios de Internet que buscan préstamos para viviendas u otros servicios financieros, informa Reuters. La decisión de la juez de distrito estadounidense Nancy Edmunds es la segunda victoria legal para la firma de anuncios en Internet WhenU, que ha sido demandada por algunos comerciantes 'online' que no quieren que los visitantes de sus propias páginas web vean anuncios 'pop-up' de sus rivales. Wells Fargo & Co. y Quicken Loans demandaron a WhenU, argumentando que la compañía no debería estar autorizada para enviar anuncios a sus visitantes en la web porque esos 'pop-ups' dificultaban la visión de sus sitios y violaban su marca registrada. Pero Edmunds dijo que las compañías no habían demostrado que resultaran perjudicadas por los anuncios de WhenU, que son generados por medio de un 'software' instalado en el ordenador que se instala en este cuando un usuario descarga algunos programas shareware o de libre distribución. Acusado de "spyware" por expertos y sitios especializados, la herramienta usada por WhenU monitoriza la actividad del usuario y muestra "mensajes personalizados" en relación al sitio que se esta visitando o de acuerdo con las preferencias de este. Los usuarios deberían ser capaces de diferenciar fácilmente entre el sitio web que pretenden visitar y los anuncios de WhenU que aparecen en otras ventanas o por debajo del sitio principal, según la opinión de la juez. Otra demanda legal contra WhenU, de la firma de alquiler de camiones U-Haul, unidad de Amerco, fue desestimada en septiembre. La resolución judicial muestra la dificultad de anunciantes y usuarios de protegerse de empresas que de "manera legal" actúan violentando la privacidad del usuario y sus hábitos online".

Tenemos que tener en cuenta que en estos casos que el usuario autoriza la inclusión de estos software al descargar herramientas como Kazaa, eDonkey entre otras.

Pero en la mayoría de las oportunidades, el spyware se incluye en paquetes de instalación, los usuarios instalan el "paquete al completo" desconociendo que están incorporando un intruso en su computador que vigilará sus actividades y que, además, se dedicará a mostrar anuncios publicitarios en su pantalla.

La barra de Google es Spyware[27]: "La barra de herramientas que Google proporciona gratis, también registra cada página por la que navegas. La política de privacidad de la Toolbar de Google así lo afirma, pero sólo y exclusivamente porque había un precedente. Alexa perdió un juicio, cuando su barra de tareas hacía lo mismo, pero en la política de privacidad no constaba ni se explicaba".

Earthlink, proveedor de servicios de Internet, ha escaneado 1,06 millones de sistemas durante el primer trimestre de año, concluyendo que cada PC tiene, en promedio, 28 programas espía o spyware[28].

Un caso muy reciente es de un malware diseñado para el espionaje industrial[29]: Detenidos en Israel 18 personas, entre las cuales destacan altos ejecutivos de tres grandes corporaciones, por espionaje industrial a través de troyanos. Durante la investigación se ha localizado, en posesión de los acusados, documentos e imágenes

[27] www.noticiasdot.com "La cara oculta de Google: Afirman que viola la privacidad de los usuarios y vigila sus actividades online". Página visitada viernes 30 abril 2004.

[28] http://www.noticiasdot.com/publicaciones/2004/0404/2104/noticias210404/noticias210404-7.htm

[29] http://www.hispasec.com/unaaldia/2410 Página visitada 13 de junio 2005

de la competencia y terceras empresas de un enorme valor comercial. Estiman que el espionaje se llevó a cabo durante más de un año. Dejando a un lado los detalles concretos del caso, el problema es que no nos encontramos ante un caso aislado. El hecho de que este tipo de espionaje a través de malware profesional no salga más a la luz se debe en gran parte al sigilo y éxito con el que se llevan a cabo los ataques, no a la ausencia de ellos. Una imagen vale más que mil palabras: desde documentos confidenciales, hasta la foto de la hija que un directivo tiene como fondo de escritorio, pasando por un vídeo que muestre todo lo que visualizó su pantalla durante varias horas la jornada anterior.

5.2 Adware

El adware es la versión "legal" del spyware.

Son pocas las diferencias existentes entre uno y otro. El adware fue instalado en nuestro ordenador de "manera legal", mientras que el segundo llego a nuestro equipo camuflado en un virus o visitando una página web cuyo propietario carece totalmente de escrúpulos. Ambos, sin embargo, actúan de la misma manera, monitorizando la actividad del usuario y violando su privacidad.

El adware es uno de los malware (amenazas) más difundidos en Internet, el que en términos simples consiste en una aplicación diseñada para mostrar al usuario publicidad no solicitada. Todos hemos sido víctimas, más de una vez, de los ataques o más bien de la lluvia de publicidad que inunda el correo electrónico, sin que sepamos cómo dieron con nuestra dirección o cómo notaron qué productos nos gustaban[30].

Pero el adware es una clase de licencia de software, la cual se acepta para utilizar determinados programas. Dicha licencia ofrece el uso de una aplicación con el único costo de visualizar una serie de mensajes publicitarios.

Sin embargo, hay oportunidades en que estos programas reúnen información acerca de los hábitos de navegación del usuario, las páginas visitadas o el inventario de las aplicaciones instaladas en el equipo, con el fin de enviar y vender dichos datos a empresas de publicidad en Internet.

En otras ocasiones, muchos adware se instalan de forma “simulada”, ya que piden permiso al usuario pero mostrándole mensajes intercalados en las pantallas de instalación de otros programas. De esta forma, la persona da su “consentimiento” para la instalación del adware, sin fijarse realmente en lo que está haciendo.

Una vez que un adware se instaló en un sistema, se conecta a un servidor que le indica los anuncios que tiene que mostrar. Para ello, mientras el usuario se encuentra navegando por Internet, el adware abre una conexión con la máquina remota para, acto seguido, abrir una ventana publicitaria ante los ojos del usuario. En muchas ocasiones, éste no sabe si el pop-up corresponde a la página que está visitando, o si tiene algún adware instalado en el sistema. De por sí, este proceso ya es perjudicial

[30] http://www.noticiasdot.com/publicaciones/2005/0205/0902/noticias090105/noticias090205-15.htm Página visitada miércoles 09 febrero 2005

para el usuario, ya que estas consultas al servidor bajan la velocidad de la conexión a Internet[31].

5.3 Phishing

Los ataques de estafa a través de Internet por el método de "phishing" que significa "pesca" en el argot informático se han ido incrementando.

El Grupo de Trabajo Anti-Phishing (APWG por sus siglas en inglés) avisó en su último informe[32], que cada vez se usan con más frecuencia los programas capaces de registrar lo que escribe el usuario en su teclado. Estos programas aprovechan los "agujeros" del software -habitualmente del Internet Explorer, de Microsoft- y reenvían esta información, en la que se incluyen nombres de usuario y contraseñas, a los atacantes. APWG destacó que existieron unas diez variantes de este tipo de programa cada semana durante los meses de febrero y marzo, y más de 100 páginas web diseñadas para engañar al usuario. El informe indica que se recibieron 13.000 alertas de ataques en el mes de marzo y muestra que EEUU es el país que hospeda más sitios de "phishing", seguido de China y Corea del Sur.

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.

Durante el miércoles 8 y el jueves 9 de junio de 2005, se han celebrado en las instalaciones de la Dirección General de la Policía en Madrid unas jornadas sobre fraude en Internet, concretamente sobre phishing bancario. Se ha definido al phishing como “un acto de crimen organizado, y como tal debe ser tratado, que los actores que participan en el escenario del fraude tienen todos su porción de responsabilidad y que es preciso transmitir y recordar a los usuarios de banca electrónica que no deben desconfiar del canal bancario electrónico, sino que deben ser conscientes de que han de contemplarse medidas preventivas para evitar ser víctimas de los engaños. La banca electrónica es, salvo excepciones extraordinarias, segura y confiable. En éste punto hubo total consenso entre los ponentes, e Hispasec se une a éste mensaje[33].

---

[31] http://www.noticiasdot.com/publicaciones/2005/0205/0902/noticias090105/noticias090205-15.htm Página visitada 9 de febrero de 2005.

[32] (EFE) Fecha: 05/05/2005 | 17:49 http://www.observa.com.uy/Osecciones/ciencia/nota.aspx?id=32383 Página visitada 6 de mayo de 2005.

[33] http://www.hispasec.com/unaaldia/2421 Página visitada 13 de junio 2005.

Pero ya se habla de una nueva generación de phishing. Hispasec[34] demuestra como 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.

Hasta el momento las recomendaciones que se hacían para acceder de forma segura a la banca electrónica eran: comprobar que la URL del navegador comenzara por https:// seguido del nombre de la entidad y comprobar el certificado de que se había ingresado en un servidor seguro, haciendo doble click en el candado que aparece en la parte inferior del navegador.

En la dirección http://www.hispasec.com/directorio/laboratorio/phishing/demo se encuentran tres videos en los cuales se ilustra como operan estas nuevas modalidades de phishing.

6. ¿Existen soluciones?

Las soluciones podemos analizarlas desde dos instancias diferentes: en primer lugar como formas de prevenir estos problemas, de evitar los intrusos en nuestros sistemas, de bloquear el acceso a los espías a nuestro ordenador. En esta instancia contaremos con la seguridad informática, ya que la misma tecnología nos da herramientas para contrarrestar los ataques, a través de software especializados, la encriptación de datos cuando no es considerada "tecnología de doble uso", etc.

Pero también en el ámbito preventivo se hace necesario estar informados de las regulaciones jurídicas en la materia. Aquí no nos referimos únicamente a la Declaración de Derechos Humanos o a la Constitución de la República como normas que protegen nuestros Derechos Fundamentales. Nos referimos a las medidas preventivas a la hora de realizar contratos informáticos o telemáticos, a la implementación de estrategias para disminuir el impacto de estos ilícitos a nivel empresarial. A estar preparados para que de producirse un fraude, puedan trabajar el área jurídica e informática en forma coordinada y eficaz para no perder evidencias digitales, para determinar los culpables en la esfera penal y para recuperar activos cuando hay pérdidas materiales.

Para finalizar, quiero hacer hincapié en que somos los primeros custodios de nuestros datos personales y de la información de nuestra propiedad, que debemos estar alertas, de la misma forma que lo estamos con nuestros bienes materiales, ya que es posible que en forma disimulada, como en el fondo de la transparencia (en la presentación), a través de los bites, "alguien" nos esté mirando.

Montevideo, 17 de octubre 2005

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

Av. Libertador Lavalleja 1872 - Of. 506 - Tel: (598) 2924 4340 - estudio@viegasociados.com