IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

Primer congreso sobre Internet, derecho y política: las transformaciones del derecho y la política en la sociedad de la información

La actuación policial frente a los déficits de seguridad de Internet*

Juan Carlos Ruiloba Castilla

Resumen

Este artículo analiza las particularidades de la investigación policial de los delitos relacionados con las tecnologías de la información y la comunicación. En concreto, se examinan las deficiencias que afectan a algunos de los sistemas, redes o protocolos, relacionados con Internet, que son normalmente aprovechadas para la comisión de defraudaciones, daños informáticos, delitos contra la intimidad o la indemnidad sexual, por citar algunos de los más habituales. Se describen los ataques más frecuentes y se analiza minuciosamente un complejo caso real, del que se aporta cada paso relevante desarrollado durante la investigación policial para el conocimiento del hecho y la identificación y captura de sus responsables. Se enfatiza, además, la importancia de la prevención en esta materia a través de una correcta información a la víctima potencial y la implantación por empresas y particulares de medidas de seguridad adaptadas al tipo de actividad que se desarrolle en la red.

Palabras clave

delincuencia informática, investigación policial, ciberinteligencia policial, *phishing*, seguridad en Internet, banca *on-line*, estafa informática, cartas nigerianas, *web spoofing*

Tema

Derecho penal y sociedad de la información

Abstract

This article analyses police investigations into crimes relating to information and communication technologies. It specifically examines those deficiencies that affect certain Internet-related systems, networks and protocols and which are frequently exploited in order to commit fraud, crimes against privacy, damages to computer systems or against sexual indemnity, to cite some of the most common instances. As well as providing a description of the most frequently occurring attacks, the author also carries out an in-depth analysis of a true and highly complex case, retracing each relevant step that was taken by the police during their investigation through to the identification and subsequent capture of the perpetrators. The article also highlights the importance of preventing such crimes by providing adequate information to potential victims and introducing security measures for both individuals and companies, specifically adapted to the type of activities that they carry out on the Internet.

Keywords

computer crime, police investigation, police cyber-intelligence, phishing, Internet security, on-line banking, computer fraud, Nigerian letters, Web spoofing

Topic

Penal law and Information Society

* Artículo adaptado por la Dra. Rosa Fernández Palma a partir de la ponencia original del Congreso.

Si tú tienes una manzana y yo tengo una manzana, e intercambiamos manzanas, entonces tanto tú como yo seguimos teniendo una manzana. Pero si tú tienes una idea y yo tengo una idea, e intercambiamos ideas, entonces ambos tenemos dos ideas.

George Bernard Shaw

Introducción

La información ha sido, es y será clave en el desarrollo de la humanidad. Al amparo de las nuevas tecnologías, ha adquirido una nueva dimensión gracias a la facilidad de su difusión por innumerables vías, llegando rápidamente a la totalidad del globo y facilitando la accesibilidad popular de la misma.

Todo nacimiento de una nueva forma de ser implica una serie de inconvenientes: la sociedad debe adaptarse rápidamente a la explosión tecnológica, lo que conlleva incertidumbre, preocupación, desconfianza, expectativas, peligros de seguridad al aumentar las vulnerabilidades, falta de normas legales o inadecuación de las que existen; pero también promueve esperanza, progreso y, en definitiva, un aumento de desarrollo que debe llevar a la humanidad a su adaptación y a la superación de estos problemas para crecer en la tabla evolutiva.

En este estatus de la sociedad, la Policía, como institución garante de los derechos, libertades y seguridad de la sociedad, contribuye una vez más de forma decisiva a la atenuación de estos problemas, erradicando dichas incertidumbres y preocupaciones, adaptándose al progreso con la celeridad que le acostumbra para que las instituciones, ciudadanos y empresas puedan utilizar, participar y beneficiarse del progreso y bienestar que el uso y las aplicaciones de las nuevas tecnologías de la información proporcionan y proporcionarán a todos los ciudadanos.

1. Ciberinteligencia policial

Para conseguir una respuesta eficaz a los peligros que amenazan las nuevas redes de comunicación, es sumamente importante y prioritario identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas vulnerabilidades permiten. Esto se consigue con un trabajo de inteligencia, o mejor dicho de ciberinteligencia.

El fin prioritario de la ciberinteligencia es el cúmulo de la información necesaria para entender el funcionamiento actual y futuro de la Red, lo que lleva a que la inteligencia debe crecer continuamente con la misma velocidad que el desarrollo de las nuevas tecnologías, debe transformarse con ella para mantener la capacidad de identificar las amenazas y las contraamenazas, vulnerabilidades y respuestas frente a éstas, así como los factores desencadenantes de las distintas actuaciones maliciosas.

2. Dificultades de investigación: algunos ejemplos

2.1. Redes de intercambio de ficheros de igual a igual (*peer to peer* - P2P)

Las redes de intercambio de ficheros (P2P) permiten que los usuarios transmitan fragmentados los ficheros a través de máquinas *cachés* o espacios comunes a disposición de la comunidad, sin control por parte del propietario del espacio magnético, llegando a la situación de que los ficheros digitales están básicamente en la red a

disposición, fluyendo en un espacio virtual propiedad de todos y de nadie.

Estas redes presentan las siguientes características:

a) *Escalabilidad.* Las redes P2P necesitan ser grandes, contar cada vez con más usuarios. Si proliferan mucho este tipo de redes, podrían llegar a su fin debido a una diversificación de usuarios, porque sucedería que a cada red se conectarían muy pocos.

b) *Descentralización*. Estas redes por definición son descentralizadas.

c) *Los costes están repartidos* entre los usuarios. Se comparten o proporcionan recursos a cambio de recursos.

d) *Anonimato*. Deben permanecer en el anonimato en estas redes el autor, el editor, el lector, el servidor, el documento y la petición.

e) *Seguridad*. Puesto que el usuario abre su máquina al resto, conviene que esté seguro. Para ello los mecanismos son: encriptación multiclave, la llamada caja de arena, gestión de derechos de autor (la industria define qué puede hacer el usuario – por ejemplo, la segunda vez que se escucha una canción ésta se apaga), reputación (sólo permitir acceso a los conocidos) y cortafuegos.

En este contexto cabe preguntarse por la responsabilidad jurídica que pudiera derivarse para el particular que carece de conocimiento respecto de la distribución de un fichero que puede contener material ilícito, no solo lesivo para la propiedad intelectual, sino relacionado con la pornografía infantil o de naturaleza xenófoba o terrorista.

Sin duda no puede descartarse que este tipo de redes puedan ser empleadas por grupos de delincuencia organizada como vías de comunicación, o para permitir la comunicación entre grupos de pedófilos, por ejemplo, para el intercambio de material ilegal.

2.2. Dirección IP

El punto de partida básico para una investigación es el escenario del crimen; de ahí, se debe hacer una retroacción temporal y virtual del hecho acontecido, retrocediendo en las comunicaciones y rastreando la red hasta que llega el momento en el que, con la comisión judicial, llamamos a la puerta del presunto autor.

Para ello nos apoyamos en el funcionamiento básico de los protocolos utilizados en las redes y, en el caso de Internet, nos apoyamos frecuentemente en la dirección de Internet Protocolo (IP) del protocolo TCP/IP que creó Vinton Cerf, que es un número único temporal que identifica un elemento en la red y que es necesario para el funcionamiento y aseguramiento de la transmisión de los paquetes digitales que viajan por la Red.

Muchas veces el elemento delictivo se debe investigar por una acción en Internet que ha dejado un rastro en «logs» (ficheros de datos de flujo de información) a los cuales, por ser susceptibles de dar información relevante, (potencialmente capaz de llevar a la identificación de una persona), se debe tener acceso a través de auto judicial motivado.

La Consulta 1/99 de la Fiscalía General del Estado abordó el problema de si es necesario o no un mandamiento judicial, no ya para no interceptar la comunicación en sí, sino para que la compañía operadora facilite la identificación del abonado que haya hecho uso de la conexión en el lapso de tiempo especificado en la investigación. La Fiscalía General ha optado por considerar, de la misma forma que ya lo había hecho el Tribunal Europeo de Derechos Humanos (Sentencia de 2 de agosto de 1984 –caso Malone– o Sentencia de 30 de julio de 1998

–caso Valenzuela Contreras–), que la inviolabilidad de las comunicaciones afecta no sólo al contenido del mensaje, sino también a la constatación de la existencia misma de la comunicación, duración y otras circunstancias que permitan ubicar temporal o espacialmente el proceso de la transmisión, por encontrarse amparadas no sólo en el secreto a las comunicaciones (dado que la comunicación o bien ya ha concluido o ni siquiera ha empezado), sino tangencialmente en el derecho a la protección de datos personales asociados a dichas comunicaciones. Y continúa estableciéndose, en concordancia con la Circular 1/99, un triple estatus de las intervenciones electrónicas, atendiendo a la adopción de la medida de control (adoptada en el seno de un proceso penal, mediante auto judicial motivado, sobre la base de la apreciación de indicios delictivos, delimitada subjetivamente y objetivamente, con duración limitada y proporcionalidad), en su ejecución (también controlada judicialmente) y en su incorporación al proceso (por medio de su trascripción e incorporación de las cintas originales a la causa).

La Propuesta del Consejo de Europa incide en este tema, ya que el artículo 18 establece que «cada una de las partes adoptará las medidas legislativas pertinentes [...] para habilitar a sus autoridades competentes a ordenar a una persona presente en su territorio comunicar los datos informáticos específicos que estén bajo el control de esta persona además de almacenados en un sistema informático o en un soporte de almacenamiento informático, y, a un proveedor de servicios que actúe en el territorio de la Parte, comunicar los datos relativos al abonado que estén en su posesión o bajo su control [...]», e incluso, ya en su artículo 16, obliga a adoptar las medidas legislativas pertinentes para permitir a las autoridades competentes ordenar u obtener de otro modo la rápida conservación de datos electrónicos, incluidos los datos relativos al tráfico cuando haya razones para pensar que éstos son particularmente sensibles a los riesgos de pérdida o modificación, incluidos los datos sujetos a custodia de corta duración.

Por ello, a pesar de la bienintencionada voluntad de las autoridades a la hora de llevar a cabo una rápida intervención policial, en determinados supuestos (como el intercambio mediante publicación en un espacio virtual de ficheros conteniendo imágenes de pornografía infantil) son necesarias hasta **cuatro resoluciones judiciales**: 1) solicitud por auto judicial motivado al administrador de los *logs* de la página web de la dirección IP del equipo que ha subido los ficheros; 2) Solicitud por auto judicial motivado al Proveedor de Servicios de Internet (ISP) del número telefónico asociado a la dirección IP en cuestión en el instante de la subida del fichero; 3) Solicitud por auto judicial motivado al proveedor de servicios de telecomunicaciones del número de teléfono del titular del mismo y lugar de instalación en el instante de la conexión; y 4) Solicitud de auto judicial de entrada y registro en el domicilio donde estaba instalada la línea ubicada para el acceso al equipo informático conectado a la misma, para llegar a acceder físicamente a una máquina y su contenido, sin que se tenga siquiera entonces la certeza de haber conseguido un cúmulo tal de pruebas suficiente para imputar el delito a su autor.

La Ley de Servicios de la Información y del Comercio Electrónico LSSI-CE, en su artículo 12, establece el plazo máximo que los proveedores de servicios deberán retener estos datos, fijándolo en 12 meses, si bien no se advierte qué datos de tráfico deben registrarse y retenerse, ni por cuánto tiempo. Para evitar que cuando llegue el correspondiente auto motivado la información no exista, se establecen parámetros de actuaciones con los ISP, de modo que, sin dar la información que se requerirá judicialmente, sea salvaguardada para su futura disponibilidad.

2.3. Territorialidad

La investigación en Internet tiene otra dificultad añadida que afecta a todas las policías del mundo: el espacio de

Internet carece de fronteras y el contenido ilícito –como la pornografía infantil– circula de un país a otro en milésimas de segundos.

Las investigaciones desembocan constantemente en comisiones rogatorias o acuerdos bilaterales o multilaterales entre países que demoran cuantiosamente el tiempo del esclarecimiento de los hechos, perjudicando gravemente el resultado satisfactorio de la investigación. Ello siempre que en el país al que solicitemos la información el hecho esté también tipificado.

La solución policial se consigue gracias a la cooperación interpolicial acordada en las mesas de trabajo, reuniones, foros y congresos, donde se plantean los problemas comunes y se marcan acuerdos de cooperación básicos tendentes a agilizar, asegurar, detectar, analizar y planificar los elementos probatorios para que, cuando por medio de la autoridad judicial del país en cuestión se ordene, se pueda llevar a buen fin dicha operación.

2.4. Cibercafés, máquinas cachés, *proxies*, máquinas comprometidas, redes inalámbricas

A las dificultades ya expresadas, deben añadirse las siguientes:

- La falta de regulación de los cibercafés, locutorios, salas de informática públicas, bibliotecas, centros educativos, máquinas populares de acceso a Internet y otras donde de forma anónima las personas pueden conectarse y realizar actividades ilícitas.
- Esto mismo respecto de las redes inalámbricas libres al alcance de equipos con conexiones inalámbricas capaces de conectarse a esas redes para la conexión a Internet con el anonimato de la no pertenencia al grupo autorizado. Los cuerpos policiales, llegados al punto de identificar una de esas máquinas anónimas como la de inicio de la actividad delictiva, deben emplear técnicas tradicionales para saber quién estaba en ese lugar en el instante señalado.
- En el mismo sentido, sabiendo que una máquina está comprometida por ser accesible a través de una conexión, ya sea a través de Internet u otro tipo de red o conexión, podemos convertirnos en una *work station* virtual de dicha máquina para navegar a través de su dirección IP. El inconveniente es que circulan habitualmente por Internet direcciones de máquinas *proxies* públicas. Aquí, una vez identificada la máquina comprometida o máquina *proxy* se debe hacer un análisis informático forense para descubrir las trazas de la conexión y detectar la procedencia de la conexión a la misma.
- Las máquinas cachés utilizadas por algunos proveedores de comunicaciones para optimizar sus rendimientos están facilitando el anonimato de los usuarios para poder delinquir con un alto grado de impunidad. Las Fuerzas y Cuerpos de Seguridad del Estado se han reunido con dichos proveedores en incontables ocasiones para que adopten medidas para evitar dicha situación, e incluso se les han ofrecido alternativas no penalizadoras de su estrategia comercial para que puedan llevar un control de las conexiones, consiguiendo que en algunos protocolos de comunicación además de la dirección IP de la máquina caché dejen viajar la dirección IP de procedencia y, en su defecto, que al menos localicen el lugar de influencia de la máquina caché.

2.5. IRC

El modelo de distribución e intercambio de pornografía infantil basado en servidores de ficheros con banda ancha, concurriendo los usuarios con clave de acceso desde un canal secreto de IRC.

El empleo de servidores de IRC que enmascaran, por operatividad de su servicio, las direcciones IP de conexión no

impide que a través de la tutela judicial se pueda acceder a la información que recogen y asocian esas direcciones virtuales con la dirección IP pública del autor de los hechos delictivos.

2.6. Crimen organizado

2.6.1. Ciberterrorismo

El empleo de las comunicaciones a través de Internet con enmascaramiento, cifrado o estenografía, es una de las dificultades añadidas en la persecución de estos delitos. La solución está en emplear aquellos medios humanos y técnicos capaces de interceptar, desencriptar y analizar los mensajes que circulan.

2.6.2. Fraudes a través de Internet

Cada vez más se emplean técnicas de comunicaciones a través de Internet para cometer uno de los delitos más tradicionales de la sociedad: el del engaño para conseguir un beneficio económico. Así, el empleo de tablones de anuncios virtuales para ofertar productos apetecibles a cambio de una cantidad, para luego, amparándose en la ventaja de utilización de datos identificativos falsos y la globalización de la red, obtener dinero a cambio de un objeto distinto al ofertado, o simplemente no enviando nada a cambio. También se encuentra la variante inversa, contactando con el vendedor para que envíe el producto pagando con los datos de moneda electrónica de un tercero. Todo ello agravado por la facilidad que ofrecen los comercios virtuales y las pasarelas de pago para vender sin el suficiente control de la moneda de cambio.

En el ámbito de las defraudaciones posee especial relevancia el fenómeno de las páginas falsas (*web spoofing*), que simulan una página conocida para hacer confiar a la víctima y que ésta deposite en la misma sus datos confidenciales, que quedan a disposición de terceros sin escrúpulos que los utilizarán para su beneficio. Esta modalidad es empleada tanto para la creación de falsos *escrow*, como para simular páginas conocidas de subastas *on-line*, comercios virtuales, entidades financieras o bancos electrónicos, correo web, etc.

Y ¿cómo llega la víctima a esa trampa digital que es la falsa página? Pues de varias maneras: bien empleando técnicas de pesca electrónica (*phishing* o pesca del incauto), que consisten en el envío de correos electrónicos para intentar convencer a la víctima de que el remitente es alguien relacionado con la página real que se intenta suplantar, para que a través del hiperenlace enviado con el correo acceda a dicho destino y confíe su bien preciado tesoro; bien empleando otras técnicas de ingeniería como la mensajería instantánea, foros, grupos de noticias, listas de distribución, anuncios virtuales, subastas o compra ventas, programas de intercambio; o, finalmente, técnicas ajenas a la Red, como el teléfono, a través del que puede recibirse un mensaje de este tipo: «Llamo de Townbank, hemos variado nuestro sistema de seguridad. No me facilite la clave por teléfono, podría ser un engaño, realícelo a través de nuestra página de seguridad en la red www.secure-townbank.com ...», dominio creado ex profeso con simulación de los logos y apariencia de ser el real de la entidad.

También la víctima puede llegar a la página simulada por acción de un cambio de la configuración de su equipo informático, cambiándole la página de inicio, los ficheros de asociación locales de url a direcciones IP (*hosts*), virus o troyanos (creados para algo más que causar daños). También es habitual emplear técnicas de *spam* para inundar el ciberespacio de correo que, en vez de ser basura, contiene un mensaje malicioso capaz de alojarse en una máquina y, como nave espacial exploradora, llevar incorporados una serie de programas espías

capaces de hacer pensar y quitarse el sombrero al mejor de los *hackers*.

El supuesto real que se expone a continuación conjuga una serie de déficits de seguridad de Internet que dificultaron seriamente la persecución del autor delictivo por los cuerpos policiales:

Imagínese una organización de un país del Este que envía a nuestro país a un individuo al que se le ha encomendado la apertura en un día de varias cuentas bancarias con documentación falsa, solicitando de dichas entidades una tarjeta de débito para poder sacar efectivo desde cajeros automáticos.

Mientras tanto, la organización crea o utiliza un troyano recién creado, que la gran mayoría de antivirus no tienen todavía en sus bases de datos virales.

A ese troyano le efectúan unas pequeñas modificaciones, como por ejemplo variarle las configuraciones de comunicación, y le añaden un pequeño diccionario de palabras para activar programas anexos.

Ese troyano, que se instala por simple visualización de una página web (html), es enviado a través de un *spam* masivo utilizando un *proxy* público, a pymes españolas con presencia en la Red (fácil obtención de sus contactos e-mail).

La instalación del troyano se produce cuando el lector abre el correo. El correo incorpora, además, una técnica de *phishing* para no causar sospecha, o bien está en blanco. Una vez instalado el troyano en la máquina de la empresa víctima, éste incorpora un programa que escucha la barra de direcciones del explorador más habitualmente utilizado. Cuando en la barra aparece una de las palabras que se ha incorporado al diccionario –por ejemplo, el nombre de una entidad bancaria española, manda el control a otro programa que no es más que un programita que captura las pulsaciones del teclado (*keylogger*) ¿Qué pasa cuando alguien de la empresa atacada se conecta a una entidad bancaria en línea? Pues que existe la posibilidad de que se identifique a la misma introduciendo sus claves de acceso. Y ¿qué pasa cuando además hay un programa que escucha el teclado? Pues que esas claves, junto a la identidad de la entidad bancaria, pasan a un fichero que es enviado a una cuenta creada gratuitamente y con datos ficticios en un dominio de un país del Este. Pero este troyano traía más sorpresas: abría un puerto de comunicaciones para habilitar la máquina comprometida como proxy y un servidor ftp que se conectaba a EE.UU. para facilitar una lista de máquinas infectadas, actualizar diccionarios, etc.

Los delincuentes, una vez obtenidos los datos de acceso a la banca virtual, se conectaban a la máquina de la víctima a través del puerto que la habilitaba como proxy, y desde esta máquina se conectaban a la banca electrónica donde transferían capital a una de las cuentas que había creado el enviado en el viaje relámpago a España y de las que, a la vuelta a su país, había entregado las tarjetas de débito y los datos correspondientes. Así que, desde la impunidad que asegura realizar las acciones allí donde la jurisdicción española no llega, disponían libremente del patrimonio sustraído. No contentos todavía, se conectaron a la máquina víctima y borraron los rastros de la actividad delictiva.

Dificultades de la actuación policial

Una vez detectada la transacción económica no consentida, se pueden establecer dos vías de investigación:

a) *Destino del dinero*: lleva a una cuenta que ha sido contratada con documentación falsa. Para la investigación debe recurrirse a las grabaciones del vídeo de la entidad bancaria, fotografías de las fotocopias de la documentación, huellas digitales de los documentos que han tocado los delincuen-

tes. Asimismo, puede seguirse la pista de la retirada del dinero en cajeros de una ciudad de un país del Este.

b) *Dirección IP que ha realizado la transacción*: al utilizar la máquina de la víctima sale la propia de la empresa, lo que puede hacer creer que ha habido una colaboración interna de alguien relacionado con la empresa. Un buen análisis forense de la máquina comprometida puede hacer descubrir la realidad:

- Comprobando con el ISP si en el mismo instante de la transferencia existía una conexión de otra máquina a la máquina victima, teniendo presentes las prácticas *looping*.
- Haciendo un examen forense a la máquina víctima para descubrir programas maliciosos, aun si estos han sido borrados remotamente después de la acción.
- Si el borrado ha sido efectivo y de los que son difícilmente recuperables, puede recurrirse a las salvaguardas anteriores para detectar dichos programas maliciosos.

c) Dicho estudio nos llevará, por un lado, a descubrir la dirección IP de actuación, comprobando que pertenece a un país ajeno a la jurisdicción española y, por otro, a descubrir el famoso troyano y su vía de infección.

d) Al analizar la vía de infección, nos lleva a un *spam* a través de máquinas comprometidas que dificulta el seguimiento inicial pues dichas máquinas generalmente son de terceros países (problema territorial de la globalidad).

e) El estudio a través de ingeniería inversa del troyano nos arrojará luz sobre el procedimiento del caso: se detectan los programas que incorporaba, los bancos comprometidos, la lista en el FTP americano con la relación de máquinas comprometidas, la cuenta gratuita donde mandaba el fichero generado por el *keylogger* y de dominio de un país del Este de Europa (problema de globalidad).

f) De todos estos estudios se obtiene mucha información para explotar, pero se necesita la colaboración ìnternacional para conseguir detener a los autores y recuperar el capital sustraído.

En este caso se varió la web real por el empleo de un keylogger. En el supuesto del «hackeo» de las cuentas de Microsoft y Hotmail, se utilizó una técnica web *spoofing* de MS.

Las bancas *on-line* también incorporan déficits de seguridad, como por ejemplo emplear una clave fija para autorizar la transacciones de capital, sistema que han sustituido algunas entidades por el de coordenadas. O la introducción de la clave por el teclado, medida que algunas entidades han suprimido por el teclado virtual, si bien existen *keyloggers* que capturan las coordenadas del clic del ratón. Influye también el deficiente control de la identidad de las personas que contratan cuentas, si bien ahora ya no suelen desplazar colaboradores desde su país, sino que contactan a través de Internet con ciudadanos del país que se desea atacar para que, a cambio de un porcentaje, abran cuentas donde se puedan recibir transferencias. El capital obtenido se envía después, descontando una comisión, a través de Western Union o similares, a un destinatario en una ciudad externa.

Mención especial merece el llamado timo de las cartas nigerianas. Se le conoce como «The Nigeria Advance Fee Scam» o «Four-One-Nine»; el primero por lo del pedido del adelanto de una cuota; el segundo, por el número de la ley nigeriana contra el fraude. Antes de la existencia del correo electrónico era habitual su difusión a través de fax. El método tiene diversas variantes, si bien la técnica común es engañar a la víctima ofreciéndole la posibilidad de obtener dinero fácilmente a cambio de una pequeña inversión. El beneficio se obtendría, supuestamente, a través de la salida de fondos de Nigeria (situación real ocurrida tiempo atrás en dicho país africano), mediante

inversiones en negocios o incluso ofertas de donaciones a iglesias y otras instituciones sin fines de lucro. Viene a ser la variante tecnológica de nuestros tradicionales timos de «la estampita» o «el toco mocho».

Otra modalidad es la del agraciado con un premio en la lotería, el gordo de la primitiva, por ejemplo. A la víctima le engañan mediante el ingreso en una cuenta a su nombre en un banco *on-line* (en realidad la página falsa de una entidad bancaria conocida), pero, para disfrutar del premio, le exigen un dinero a cuenta por gastos de gestión o de impuestos.

La dificultad de persecución de estos delitos reside en la concurrencia de varios estados implicados (víctimas de países como EE.UU., Canadá, Japón, Australia, Nueva Zelanda o Arabia Saudita; lugar de comisión entre África y Europa; páginas webs en cualquier máquina de cualquier país del mundo; correos electrónicos creados ex profeso; destino del dinero estafado ocultando al máximo el destinatario.

2.6.3. Pornografía infantil

La sensación de impunidad y anonimato que proporciona Internet la convierten en lugar de obtención e intercambio de imágenes y vídeos entre pederastas. Resulta también preocupante la posibilidad que la Red otorga para la constitución de una comunidad paidófila, ya que permite a sus miembros promocionar su identidad como grupo, reforzarse y asistirse mutuamente, proporcionándose directamente material relacionado con la pornografía infantil o la información necesaria para obtenerlo por otras vías, además de ofrecerles una razón de ser, albergando la posibilidad de que la pederastia sea en el futuro una legítima opción sexual más.

En España, antes de la última reforma del Código penal, no estaba penada la posesión para uso de la pornografía infantil, lo que conllevaba un problema para la persecución de estas personas si no se probaba la distribución o la corrupción directa de los menores para la obtención de dicho material. Dentro de los delitos más habituales relacionados con las nuevas tecnologías, éste es uno de los que menos objeciones presentan a la hora de obtener información tendente al esclarecimiento del hecho, ya que en el fondo esta lucha no es sino un tratamiento sintomático de otro fenómeno mucho más grave, la agresión sexual y abuso de menores de edad.

2.6.4. Descubrimiento y revelación de secretos y/o daños informáticos

Cada vez existe mayor incidencia de estos tipos delictivos cometidos a través de la Red. Pueden clasificarse en dos tipos principales: los relacionados con personas físicas y los relacionados con personas jurídicas. En los primeros, el móvil es obtener datos personales de la víctima con fines de diversa índole, como venganza y acceso a la intimidad. Generalmente, el autor está o ha estado relacionado con la víctima y es todavía muy bajo el índice de detección de los casos reales que se producen, salvo que la información obtenida sea divulgada o se produzcan daños en el equipo informático o lo denuncie la propia víctima. Pero lo preocupante es el aumento de hechos que se producen en los medios empresariales para perjudicar la actividad de una empresa, ya sea obteniendo información confidencial o causándole daños que perjudiquen su imagen o actividad. Los móviles también suelen estar acotados y realizados principalmente por antiguos empleados con afán de venganza, ex directivos con la intención de crear una nueva empresa en el sector o empresas rivales por competencia desleal. La inseguridad de Internet se ve aquí potenciada por el conocimiento de los sistemas de seguridad por parte de los ex empleados, sobre todo si éstos son informáticos o ex directivos con participación en el control de seguridad. Al tiempo esos conocimientos de control permiten atacar los datos más vulnerables, sustrayéndolos, alterándolos y

destruyéndolos, ocultando, enmascarando o borrando los registros *logs* de actividad. Aquí se da un problema añadido que es valorar el reflote de la actividad empresarial o salvaguardar las evidencias para el procedimiento judicial, problema que hay que dilucidar en tiempo muy escaso, valorando gran cantidad de factores que hacen decantar la decisión en un sentido, en otro o en posiciones intermedias.

3. Soluciones a las dificultades de la investigación

A lo largo de esta exposición hemos visto algunos problemas y sus posibilidades de solución. Pero la actuación policial no se limita a intentar resolver esos problemas de una forma puntual, cuando el hecho es uno y el problema se suscita. La policía, aquí, emplea todas las posibles vías de investigación para tener un conocimiento lo más amplio posible del hecho, reconstruyéndolo, conociendo los protocolos empleados, la línea temporal, las máquinas involucradas, las personas implicadas directa o indirectamente y las necesidades técnicas para llevar a cabo el suceso, ya sean humanas como materiales. Se comprueba si el hecho es puntual o múltiple y si ha habido otros hechos relacionados antes, contemporáneos o posteriores; se examinan los vestigios que ha producido el hecho en su ejecución, las situaciones que se han producido en el entorno humano, social y empresarial, y muchas más variables que, conjugadas con un buen análisis de esta información, permiten a los investigadores abrir vías de investigación.

Pero, como se ha dicho, los problemas de la seguridad de Internet no sólo se intentan paliar con posterioridad a los hechos, sino también procurando anticiparse a un riesgo potencial de modo que, cuando éste se detecta, se transmite, se intercambian posibles soluciones y se discute en foros, congresos, conferencias, cursos, encuentros, reuniones y mesas de trabajo, entre los diferentes cuerpos de seguridad, instituciones y organismos, empresas relacionadas, técnicos y especialistas en las materias involucradas.

Asimismo, se comunica a las potenciales víctimas, ya que el particular puede obtener información cuando es víctima de un ataque, aportando datos como la forma de realización del hecho o la identificación del posible autor. Es aconsejable que las víctimas potenciales conozcan las modalidades delictivas para no caer en ellas. En las empresas son muy recomendables las políticas de seguridad, tanto en implementación de sistemas, mantenimiento, actualización y control sobre accesos a aplicaciones o sistemas de usuarios autorizados, como respecto a la información de lo que son contraseñas seguras y su custodia, o la gestión de la red por un responsable cualificado. Estas medidas son esenciales para evitar un altísimo porcentaje de incidencias en la red.

En cuanto a la técnica, conocer el medio mejor que los atacantes permite obtener información más allá de lo imaginado por el autor del delito, pese a que, si su sapiencia se lo permite, habrá intentado camuflar, modificar o incluso borrar su rastro. Pero, como siempre, lo absoluto es improbable por no decir imposible de conseguir: siempre quedan vestigios no controlados por el delincuente, ya sean por procesos automatizados propios de las comunicaciones, sistemas, políticas de seguridad, funcionamiento de optimización de los equipos o incluso fallos de funcionamiento que vierten información en lugares insospechados.

En cuanto a los ilícitos cometidos a través de cibercafés, IP *proxys*, máquinas cachés, y lugares de acceso público a Internet, sería precisa su regulación futura.

La formación actualizada y constante sobre las nuevas tecnologías, como campo e instrumentos utilizados para la actividad criminal, son dados a conocer constantemente a jueces y fiscales a través de las diligencias informes, y los contactos directos con los mismos por parte de los funcionarios de los grupos especializados en la investigación de estos delitos tecnológicos son, sin duda, una de las mejores estrategias y herramientas que podemos emplear para la lucha contra la *ciberdelincuencia.*

Una de las medidas actualmente más urgentes es dotar de más efectivos a los grupos especializados en la lucha contra la *ciberdelincuencia*, ya que el número de investigaciones aumenta considerablemente, permaneciendo invariable el número de funcionarios dedicados a su investigación, lo que implica una sobresaturación de casos que dificulta enormemente su seguimiento de forma correcta, debiendo priorizar las actuaciones y tomar decisiones no tan adecuadas como sería deseable para la eficacia de las correspondientes acciones.

Cita recomendada

RUILOBA, Juan Carlos (2006). «La actuación policial frente a los déficits de seguridad de Internet». En: «Primer congreso sobre Internet, derecho y política: las transformaciones del derecho y la política en la sociedad de la información» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. N.º 2. UOC. [Fecha de consulta: dd/mm/aa].
<http://www.uoc.edu/idp/2/dt/esp/ruiloba.pdf>
ISSN 1699-8154

Juan Carlos Ruiloba Castilla
barcelona.dtb@policia.es

Jefe del Grupo de Delincuencia Tecnológica y Delitos contra la Propiedad Intelectual e Industrial de Barcelona y coordinador regional. Lleva 23 años de servicio en la Policía Nacional, la mayor parte de los cuales los ha desarrollado realizando tareas relacionadas con la ciberdelincuencia. Ha participado en numerosos cursos de especialización y en la actualidad colabora como docente con las Universidades de Barcelona y Autónoma de Barcelona, así como con el Colegio de Detectives Privados de Cataluña, en materias como la informática forense, la pericia caligráfica en documentos electrónicos y la firma digital, etc.