Cibercrimen, cibercriminales y cibervíctimas

Fernando Miró Llinares

PID_00195951

UOC
Universitat Oberta de Catalunya

Índice

Introducción

Es innegable que los avances en la tecnología también provocan cambios estructurales en la sociedad y por consiguiente, también tienen su reflejo en la criminalidad como fenómeno social que es.

Por lo que es importante hacer un análisis detallado de las diferentes formas de la cibercriminalidad así como de los actores implicados en la misma.

Así, este módulo está formado por cuatro apartados que permiten hacer un estudio global de la fenomenología del cibercrimen, su clasificación, así como conocer las características generales del perfil de los ciberdelincuentes y cibervíctimas de cada uno de los tipos de cibercriminalidad.

Objetivos

En los materiales didácticos de esta asignatura, el estudiante encontrará las herramientas básicas para alcanzar los objetivos siguientes:

1. Consolidar los conocimientos sobre la fenomenología de los distintos tipos de cibercrímenes.

2. Aprender a clasificar los diferentes delitos realizados en el ciberespacio.

3. Comprender los procesos de victimización de los diferentes cibercrímenes.

4. Conocer los diferentes perfiles de los ciberdelincuentes así como sus características.

5. Conocer los diferentes perfiles de las cibervíctimas así como sus características.

1. Introducción: hacia una clasificación criminológica de los delitos en el ciberespacio

Son varias las clasificaciones existentes sobre la cibercriminalidad. Para el presente módulo se propone otra clasificación atendiendo a los distintos intereses sociales con trascendencia jurídica que pueden ver afectados por los mismos. Se trata de una clasificación criminológica que nos permite conocer la fenomenología de los diferentes cibercrímenes y, a su vez, analizar el perfil de los sujetos que realizan los delitos y los objetivos que persiguen.

Ved también

En el módulo "Delincuencia asociada al uso de las TIC", se ha dado una clasificación de cibercriminalidad distinta de la que se da en el presente módulo. En aquel módulo se clasifica la cibercriminalidad según la incidencia de las TIC en el cibercrimen.

En este sentido, se pueden distinguir tres categorías de delitos en el ciberespacio:

- En primer lugar, distinguimos aquellos ataques que tienen como objetivo último la obtención de un beneficio patrimonial.
- En segundo lugar, se agrupan todos aquellos ataques que tienen como objeto una persona individual, en cualesquiera de los aspectos de su desarrollo personal.
- Y en tercer y último lugar, otra categoría que engloba todos los comportamientos que tienen un objetivo ideológico o institucional.

La primera categoría se denomina **cibercriminalidad económica** puesto que el propósito de este tipo de delitos es la obtención de un beneficio económico por parte de quienes realizan el delito. La segunda categoría, denominada **cibercriminalidad social**, tiene que ver con las relaciones sociales entre las personas y que no son más que la trasposición al ciberespacio de los crímenes tradicionales derivados de los conflictos entre personas. La tercera categoría incluye todos los delitos ideológicos como la difusión por Internet de mensajes de odio racial y el ciberactivismo político, por lo que se ha denominado **cibercriminalidad política**.

Las tres categorías corresponden a su vez a los tres grandes ámbitos funcionales del uso de las TIC. Es indudable que el ciberespacio se ha convertido en un espacio para el intercambio económico transnacional. Al principio, el ciberespacio tuvo mucha más trascendencia para el desarrollo de relaciones económicas, para mejorar la comunicación entre empresas y clientes, lo cual conllevaba la entrada en el ciberespacio de bienes económicos (en forma de dinero, de datos valiosos, de nuevos servicios, etc.), consecuencia de lo cual las primeras formas de criminalidad se centrarán en aprovechar ese nuevo medio para obtener beneficios económicos. Pero hoy en día, Internet también sirve

para que las personas contacten con otras personas, para crear redes de amigos, para comunicarse y relacionarse como seres sociales, lo que hace que las esferas más privadas de la personalidad de los que se relacionan socialmente en el ciberespacio puedan verse también afectadas.

Tampoco hay que olvidar que el ciberespacio también se ha convertido en un ámbito para el desarrollo de las relaciones institucionales y supranacionales de carácter no económico. Ahí entra el cibercrimen político, aquel que se realiza bien por parte de sujetos individuales o bien por parte de instituciones o grupos, incluso de estados, que utilizan Internet como forma de difusión de un determinado mensaje político o como forma de ataque a un Estado o a concretas instituciones no gubernamentales. Al fin y al cabo, el ciberespacio es un magnífico medio para la difusión de ideas y mensajes, un instrumento poderoso para la captación de personas sobre la base de sus concepciones políticas o ideológicas, y un ámbito de riesgo para las instituciones que pueden ver atacados sus servicios por medio de ataques de denegación de servicios o de envíos de *malware* que afecten a sus sistemas y a los datos en ellos contenidos.

Pese a que las tres categorías comparten el medio de comisión, son fenómenos distintos, ya que la finalidad con la que actúan los cibercriminales es distinta, los objetivos son distintos y por ende, los perfiles de los actores implicados son distintos, como veremos a lo largo de este módulo.

2. Cibercrímenes económicos

Los cibercrímenes económicos es una categoría que, como ya se ha comentado, engloba a todos los comportamientos criminales que tienen la finalidad de obtener un beneficio patrimonial, por lo que tienen cabida todos los ataques que afectan al patrimonio de las personas individuales o al sistemas económico en relación con las transacciones comerciales en Internet, pero también aquellos que afectan a otros bienes jurídicos, como la intimidad, seguridad de los sistemas, etc., pero que tienen el objetivo final de obtener un beneficio económico.

2.1. Caracterización de los ciberdelitos con móvil económico

En muchas ocasiones, para obtener el beneficio económico final es necesario realizar una cadena de ataques, por lo que podemos distinguir dos tipos de cibercrímenes económicos. Por un lado, encontramos los mediales o instrumentales y por otro lado, los económicos en sentido estricto, siendo los primeros actos preparatorios de estos últimos.

Un ejemplo claro es el envío de *spam*, que es una forma de ataque a innumerables terminales que en muchos casos es el primer paso para una posterior infección con *malware*. Este hecho se lleva a cabo con intención destructiva de información de usuarios o de empresas (a veces con propósito de extorsión), o con intención de incorporar una *backdoor*, que permita el acceso ilícito al sistema para el apoderamiento de información privada o para convertir el sistema informático en un *bot*. A su vez, este último permitirá, posteriormente, su uso como *botnet* para un ataque de denegación de servicios a otra web o para el envío de cantidades ingentes de *spam*, con la consiguiente "vuelta a empezar" de la cadena de ataque, o, en la mayoría de casos, para el envío de publicidad falsa. Como consecuencia de ello, existe un ataque de *phishing*, cuyo propósito puede ser, de nuevo, la infección con *malware* para la consecución del fraude, o el engaño directo para que sea el usuario el que envíe la información privada bancaria.

También es habitual el ataque en cadena con otros cibercrímenes relacionados con la distribución ilícita de contenidos.

Por ejemplo, la distribución de material pornográfico, sea o no de menores, que puede encerrar un primer paso para un ataque de *phishing* o de *pharming* por parte del cibercriminal. También con la descarga de material protegido por derechos de autor, que puede esconder en muchos casos virus troyanos o infecciones de *botnet*.

En el caso de la distribución de material pornográfico "lícito", se aprovecha el enorme potencial de difusión de este contenido para atraer a los usuarios con ofertas de gratuidad. De nuevo la cadena comienza con un ataque de *spam*, en el que el correo electrónico reenvía a una página de *phishing* que contiene material pornográfico y en la que al registrarse el usuario con la promesa de material pornográfico gratuito de mayor impacto (contactos con otros usuarios, videochats pornográficos, etc.), se descarga involuntariamente un *malware* con el propósito de la posterior obtención de datos privados bancarios.

En el caso de la distribución de material pornográfico ilícito, usualmente de menores, los cibercriminales muchas veces controlan las propias redes de difusión del citado contenido. Aprovechan la vulnerabilidad del sujeto que trata de descargarse este material y el hecho de que la víctima del ataque final difícilmente denunciará unos hechos que le convertirían a él mismo en autor de un delito, para incluir entre los objetos descargados algún tipo de *malware*, que permita posteriormente el acceso a las cuentas corrientes de

la víctima o para utilizar su sistema informático como parte de una *botnet* que realice posteriores ataques de *spam* o de denegación de servicios.

En cuanto a la descarga de obras audiovisuales o musicales, las redes p2p se han convertido en un ámbito de riesgo en el que los cibercriminales simulan el *malware* como archivos de obras protegidas, con la consiguiente infección de los sistemas cuando el usuario descarga los mismos.

La perspectiva criminológica nos permite comprender, pues, que incluso los ataques que parecen tener menor lesividad como los ataques de *spam*, suelen formar parte de una cadena de ataque que puede terminar en una defraudación del patrimonio de la víctima o en la utilización de su sistema para la comisión de otro tipo de infracciones. La prevención de tales comportamientos de menor lesividad, por tanto, es esencial para evitar la proliferación de ciberataques económicos de todo tipo.

Sin entrar en si los mismos merecen o no una respuesta penal, lo que es indudable es que la gravedad de estos comportamientos no puede valorarse teniendo en cuenta únicamente los bienes individuales que se ven afectados, sino que en términos de riesgo penal deben interpretarse como lo que son, auténticos actos preparatorios esenciales de los ataques lesivos más dañinos.

También es otra modalidad de cibercrimen económico el *hacking* más directo, en el que se accede directamente a la información bancaria o incluso a la entidad para realizar el fraude, generalmente aprovechando las vulnerabilidades del sistema o las que ha ido creando la propia víctima. A veces incluso ni siquiera es necesario acceder al sistema y se puede recopilar la información necesaria para el fraude por medio de programas *sniffers*. En otros casos, incluso el procedimiento puede ser más sofisticado y, por medio de la minería de datos, accediendo a estos a través de los perfiles de la víctima en las redes sociales y otras, se puede lograr información sobre una vulnerabilidad, o bien configurar un *spam* personalizado con más posibilidades de éxito que el masivo.

La cibercriminalidad económica es, por tanto, un primer gran ámbito de delincuencia en Internet, que si bien abarca múltiples tipologías de conducta diferentes entre sí, todas ellas son parte del puzle requerido para lograr el fraude económico final.

2.2. Los ciberdelincuentes económicos

Pese a que la mayoría de las conductas criminales se incluyen dentro de esta categoría y son la extensión de conductas que ya se realizan en el espacio físico, los perfiles de quienes realizan uno y otros delitos se ven modificados. De hecho, no existe un perfil único de ciberdelincuente, existen muchos tipos, como ocurre en la delincuencia realizada en el espacio físico, como iremos viendo a lo largo del módulo.

La mayoría de los crímenes en el ciberespacio que se realizan con intención económica se relacionan con *hackers* que buscan vulnerabilidades y superan barreras en sistemas o en redes, bien sea para el acceso a un sistema, o para la configuración de una red telemática o de cualquier otro tipo, interrumpen y saturan servidores y sistemas, o diseñan herramientas específicas con la intención final de obtener por su actividad un beneficio económico directo o indirecto en el caso de que sean *hackers* contratados por grupos organizados.

Pero no hay un solo tipo de *hacker*, de hecho, este ha ido evolucionando a lo largo del tiempo. Los primeros fueron los denominados *truehackers*, aficionados a la informática en los años sesenta, pasando por los hardware *hackers* de los setenta, que desarrollaron algunos de los equipos y tecnologías más importantes, y por los *gamehackers* en los años ochenta, que desarrollaron aplicaciones de software para juegos. La penúltima meta es la conformada por la dualidad *hacker*/*cracker* de los años noventa, que incluye a quienes utilizan las tecnologías informáticas para acceder ilícitamente a sistemas o redes y los diferencia, según su modo de actuación sea inocuo o malicioso, hasta llegar a los *hackers* clandestinos de la Web 2.0 y de la era de la tipificación delictiva del acceso informático ilícito. Estos últimos pueden dedicarse tanto a la intromisión informática, a la realización de ataques DoS, a la creación de webs para el fraude, al diseño de virus, a la infección de *bots* o al envío de *spam*, y todo ello con finalidad económica (generalmente) o bien política en el caso de los ciberhacktivistas, y actuando de forma individualizada o formando parte de un grupo, que bien puede ser una banda organizada tradicional que opera ahora en el ciberespacio, como una ciberbanda de *hackers* que unen sus esfuerzos para un fin criminal común.

Hackers

Hay que tener en cuenta que el término *hacker* puede ser empleado desde una concepción amplia para referirse a cualquier persona con conocimientos informáticos que realiza alguna actividad ilícita, o simplemente no autorizada, en el ciberespacio. O, desde una concepción más estricta, para hacer referencia al experto informático que busca superar barreras por el mero hecho de su existencia, si bien sin entrar en el campo de lo delictivo, en ocasiones incluso usando sus conocimientos para las mejoras de la seguridad de las redes y sistemas.

El término *hacker* no hay que confundirlo con el de *cracker*, que fue creado por los primeros para referirse a quienes el acceso informático para robar información relevante o causar algún otro tipo de daño, y diferenciarlos así de quienes superaban las barreras de acceso por el mero hecho de hacerlo. Aunque la frontera entre *hackers* y *crackers* es tan estrecha que algunos de ellos la saltan una y otra vez, pasando de actividades lícitas a ilícitas y utilizando para ello *nicks* distintos.

En la gran parte de los *hackers-crackers* ya no son expertos informáticos sino que también comienzan a realizar tales actividades usuarios, generalmente jóvenes, con conocimientos básicos de informática que aprovechan programas y aplicaciones sencillas para realizar sus incursiones. Estos son los denominados *scriptkiddies*, que, no siendo expertos *hackers* capaces de acceder a sistemas mediante programaciones propias, realizan sus ataques informáticos, generalmente eligiendo las víctimas al azar, aprovechando programas y *scripts* básicos y causando daños en muchos casos, más fruto de su impericia o de la dañosidad del *malware* utilizado, que de sus habilidades.

No solo son *hackers* los que realizan cibercrímenes económicos. Otro cibercriminal clásico es el *insider*, que aprovecha su posición dentro de la institución o empresa para realizar su ataque. Son los principales protagonistas de los *data breaches*, cualquier forma de destrucción, modificación o acceso a datos de empresas o de particulares. Generalmente suelen tener éxito, dado que es más posible que pasen desapercibidos y además suponen un mayor riesgo que los ataques externos pues tienen mayor acceso a la información.

Sin embargo, los últimos estudios apuntan a que los grupos organizados están creciendo de forma cualitativa y cuantitativa. Cada vez destaca más la interrelación entre cibercriminalidad y delincuencia organizada. Son múltiples las pruebas que muestran que las bandas organizadas se han aprovechado de las TIC para facilitar o mejorar la comisión de delitos como el tráfico de secretos empresariales obtenidos por Internet, la extorsión y los ciberfraudes, el blanqueo de dinero a través de sistemas de pago *online*, la distribución ilegal de materiales a través de Internet y el uso de Internet como un mercado de venta ilegal de productos falsificados y de las drogas farmacéuticas.

Dentro de la cibercriminalidad organizada, hay que diferenciar dos tipos de grupos: por un lado, las organizaciones tradicionales (mafia siciliana, mafias rusas, tríadas chinas o yakuzas, etc.), que suman a sus múltiples actividades la realización de delitos por medio de Internet; y por otro lado, las ciberbandas organizadas o conjunto de *crackers*, que se organizan como grupo criminal y cuyo único ámbito de actuación es el ciberespacio.

Finalmente, dentro de los perfiles de los cibercriminales económicos hay que destacar la figura de las **cibermulas**, que no son, desde una perspectiva criminológica, cibercriminales, puesto que no son autores del delito en el ciberespacio, sino colaboradores o recolectores de los beneficios en Internet, que luego envían por medios seguros de transmisión del dinero a los autores del delito (las ciberbandas) o a los responsables de los grupos organizados tradicionales que operan en Internet.

Cibermuleros

Los cibermuleros son reclutados por Internet bajo la promesa de la recepción de importantes cantidades de dinero que tienen que transmitir quedándose un porcentaje como ganancia. Generalmente, estos cibermuleros son los únicos detenidos por estos delitos y pueden ser hechos responsables de los mismos como cooperadores necesarios o cómplices.

2.3. Las víctimas de los ciberdelincuentes económicos

Al igual que sucede con los perfiles de los ciberdelincuentes económicos, existen **múltiples perfiles de víctimas**. De hecho, cualquier usuario puede ser víctima de cibercrímenes de muy distintos tipos, dependiendo del tipo de actividad que realice el usuario.

La mayoría de las conductas que sufren los usuarios de Internet son cibercrimenes económicos, y de forma concreta, la infección de virus, *hacking* y la utilización de *spyware*. Estas formas de ataque tienen la finalidad de obtener un beneficio económico y suelen ser adoptadas para el posterior fraude una vez se dispone de la información necesaria.

Este tipo de criminalidad depende de la falta de incorporar sistemas de autoprotección y de las acciones que realice el usuario dentro del ciberespacio, como entrar en un determinado tipo de página o descargar archivos sin conocer con seguridad su contenido.

Internet, con las facilidades que presenta, ha hecho que se haya convertido en un ámbito de comercio. Ante el aumento del uso de Internet para comprar o realizar movimientos bancarios, ha conseguido que en los últimos años se haya convertido en un ámbito de victimización.

El primer factor que parece estar directamente relacionado con la victimización por ciberfraude es realizar **compras en Internet**, pues incrementa la posibilidad de ser objetivo de un ciberfraude en un 377%. Si se tiene en cuenta que el número de usuarios de Internet que realizan transacciones económicas sigue incrementando, podemos comprender la importancia de este factor y la necesidad de incrementar la protección para los compradores en el ciberespacio.

Los compradores por Internet tienden a ser personas de **nivel cultural medio o alto** que, además, disfrutan de niveles de ingresos más bien altos. De hecho, parece que existe una relación entre tener altos ingresos y tener un nivel formativo más alto, con el hecho de comprar más por medios *online*. Y aún más clara parece la relación entre el género y la actividad de compra *online*. Según todos los estudios, los hombres suelen hacer más compras *online* que las mujeres aunque pasen el mismo tiempo conectados. La explicación es que al igual que los **hombres** compran más *online*, también harán, seguramente, e independientemente de que pasen el mismo tiempo que las mujeres en el ciberespacio, otras conductas no seguras, como la descarga de archivos, etc., que explicará que tengan un mayor índice de victimización que las mujeres.

Relacionar la compra *online* con la victimización por ciberfraude tiene sentido si tenemos en cuenta que muchos de los ciberfraudes existentes tienen que ver con esta actividad, pero también si pensamos que al pagar *online* generalmente se acaban "tecleando" los datos bancarios personales, incluyéndolos así en el sistema como objeto potencial de ataque. Obviamente, no es la propia actividad de compra sino lo que viene unido a ella lo que incrementa el riesgo de ser víctima del delito.

3. Los cibercrímenes sociales

Esta segunda categoría viene a recoger todos los comportamientos criminales realizados en el ciberespacio relacionados con la comunicación interpersonal y que en realidad son crímenes tradicionales que ahora se realizan en el ciberespacio y que, por las características que presentan, les hace parecer nuevos delitos.

3.1. Caracterización de los ciberdelitos sociales

Pese que en sus orígenes Internet se concibió como un ámbito dedicado al plano económico y empresarial, es innegable que en los últimos años ha revolucionado la comunicación interpersonal convirtiéndose así en una herramienta fundamental para establecer relaciones sociales.

Son muchos los sistemas que se han creado en este sentido, desde las propias páginas web hasta el correo electrónico, pasando por la creación de otros sistemas de comunicación, como son las salas de chat, los programas de mensajería instantánea como es el "Messenger" o la creación de redes sociales como Facebook, MySpace, Twitter, etc. En definitiva, ofreciendo nuevas formas de comunicación social.

Son precisamente las redes sociales las que han dado un giro importante a la comunicación por las implicaciones que llevan aparejadas. Aunque ya existían mecanismos que permitían establecer perfiles de amigos y otras funcionalidades de las redes sociales, no es **hasta mediados de la década pasada**, con la popularización de Myspace, primero, y de Facebook y otras redes más localizadas geográficamente, después, cuando **las páginas web que facilitan y fomentan las relaciones entre personas sin los límites especiales y temporales tradicionales**, se convierten en un elemento esencial de la vida social para muchas personas y muy especialmente para el sector de los jóvenes. Una de las razones, aunque no única, del éxito de las redes sociales reside en que han logrado la convergencia de muchos servicios que ya ofrecían las TIC que hasta el momento estaban separados, como el correo electrónico, la mensajería directa, los chat, la creación de webs, los diarios electrónicos, álbumes de fotos, selección de música, vídeos, etc. Esto permite a los usuarios controlar el nivel de comunicación con las personas y convierte a las redes sociales, por una parte, en esferas de desarrollo del ocio y de las relaciones sociales en las que el nivel de intimidad plasmado en la web puede llegar a ser muy alto, pero también en un medio integral de gestión de la propia identidad, de su personalidad y de las relaciones sociales.

Redes sociales y juventud

El papel que juegan y pueden desempeñar estas redes sociales en el desarrollo de las relaciones sociales es aún mucho más significativo en los jóvenes. En la etapa adolescente y preadulta, donde la construcción de la identidad propia ocupa una dimensión muy significativa, un instrumento para la comunicación y el contacto social como son las redes sociales puede desempeñar un papel crucial en la vida de los jóvenes. Según las investigaciones existentes, los adolescentes usan Internet para comunicarse con los amigos, para buscar otros nuevos, para buscar pareja, para compartir información personal, etc.

Lo cierto es que las redes sociales en particular e Internet en general constituyen hoy en día un nuevo ámbito de desarrollo personal, un nuevo espacio vital en el que cada individuo pasa varias horas al día, se comunica con otros, crea relaciones, etc. Lo hace desde su casa o desde el trabajo, si atendemos al espacio físico que ocupa, pero ese espacio no tiene ya relevancia alguna cuando el sujeto está en Facebook comentando una opinión política, en Tuenti hablando de un compañero o en su blog personal cargando un vídeo concreto. A los efectos que nos interesan, por tanto, puede afirmarse que todas las esferas personales que al relacionarse con los demás pueden ser puestas en peligro lo están también en el ciberespacio; y que todas las conductas criminales de ataque a las personas que no requieran de una inmediatez física también van a acabar realizándose por medio de Internet.

Como cualquier otro medio de difusión de contenidos, Internet está sirviendo desde hace tiempo para la comisión de calumnias, injurias y amenazas ejecutadas por medio de *e-mails* o por su publicación en páginas web. También la **violación de la intimidad personal**, y no solo como parte del cibercrimen económico como medio para la consecución del futuro fraude, sino con el mero fin de desvelar secretos personales y dañar la intimidad de la víctima, empezó a mostrarse como conducta delictiva en el ciberespacio debido a la ingente cantidad de información personal que los particulares colocan en sus sistemas informáticos y comparten en sus correos electrónicos y que entran en riesgo al estar tales sistemas conectados en Red. Incluso la libre formación de la sexualidad de los menores también podía ser atacada, no solo por medio de la pornografía infantil, que generalmente utiliza el ciberespacio solo para transmitir los contenidos grabados previamente en el espacio físico, sino por parte de abusadores sexuales, que utilizan las salas de chat o sistemas de comunicación como el Messenger para realizar proposiciones sexuales a menores, que luego tratan de convertir en realidad mediante un contacto con sus víctimas.

Con el aumento de popularidad de las redes sociales unido a su uso a través también de los sistemas de telefonía móvil, el catálogo de comportamientos criminales que pueden afectar a las esferas más personales del individuo aumenta cuantitativamente, pero también en lo cualitativo en su dañosidad significativamente superior.

Todas las formas de acoso de una persona o grupo de personas a otra se están comenzando a dar también en el ciberespacio, con el simple uso del correo electrónico o de otras formas de comunicación que sirvan para enviar mensajes ofensivos contra la víctima o de forma algo más elaborada por medio de las redes sociales, que permiten tanto la exclusión de una persona por parte de un grupo como la creación de perfiles falsos y la difusión de imágenes, vídeos y textos relativos a la víctima con el ánimo de ofenderla y dañar su imagen o su dignidad.

Ciberacoso entre adolescentes

Aunque esto ya está comenzando a darse en el ámbito laboral como parte de las dinámicas de *moobing*, aún más usual es encontrarnos con acoso entre adolescentes, especialmente en el ámbito escolar y no solo utilizándose el ciberespacio en estos casos como forma de reforzar el acoso de un grupo de menores contra otro que ya tiene lugar en el ámbito del colegio, con la publicación de imágenes difamatorias, de mensajes o similares, sino incluso constituyendo la principal o única forma de acoso, pero con similar potencialidad lesiva a la ejercida en el ámbito "real".

También la Red es un ámbito propicio para el ***stalking*** o acoso continuado a una persona con permanentes solicitudes de contacto que son continuamente rechazadas por la víctima.

El autor del *cyberstalking* aprovecha las facilidades para la comunicación que ofrece Internet para sumar al típico acoso telefónico, el envío masivo de correos electrónicos, la solicitud de ser agregado a las redes sociales en las que está la víctima, bien directamente por parte de ella o bien por parte de los amigos de esta, la creación de blogs y webs en los que se narra la relación con la persona acosada, entre otras posibles conductas.

También se incluyen dentro de esta categoría las conductas de **acoso sexual** especialmente a menores y que, si bien puede llevarse a cabo por medio de mensajes de correo electrónico o en redes sociales, es más común que se den en salas de chat en las que la comunicación entre el agresor y la víctima es más directa. Según los estudios existentes, uno de cada siete jóvenes de 13 a 17 años ha recibido una proposición sexual en el ciberespacio.

La dinámica del ***child grooming*** se divide en cuatro fases:

1) La primera de ellas consiste en el primer contacto del ciberagresor con un menor a través de Internet, generalmente usando el Messenger, chat o redes sociales frecuentadas por menores. Finge ser alguien atractivo para el menor (otro menor de edad similar, buen parecido físico, gustos similares, etc.) para finalmente ganarse su confianza.

2) En la segunda fase, el acosador consigue que el menor le envíe alguna foto comprometida, que encienda la webcam, pose medio desnudo, etc.

3) Una vez conseguido, en la tercera fase, cuando el menor no accede a sus pretensiones, le amenaza con difundir la imagen que le haya capturado con mayor carga sexual a través de Internet y/o enviarlas a los contactos personales del menor.

4) Y por último, se suceden el abuso y/o agresiones sexuales, cuando el menor, por miedo a represalias, accede a los caprichos de los agresores, incluso pudiendo llegar a ocurrir el contacto físico.

Otra de las conductas realizada por menores y que merece atención es el ***sexting***, consistente, como se ha dicho, en el envío a otro menor por mensajería telefónica (aunque también por medio de correos electrónicos o sistemas de mensajería en redes sociales) de fotografías de desnudos, posturas eróticas o partes del cuerpo, con intención de formar parte de algún mensaje de tipo sexual, realizadas generalmente por un menor.

No es esta la única conducta de entre las que estamos calificando como cibercriminalidad llevada a cabo por menores, en la que se utiliza el teléfono móvil, puesto que el mismo también sirve para el envío de mensajes dentro de las dinámicas del *cyberbullying*, etc. Su singularidad estriba, en cambio, en la dificultad de su consideración como ilícito, dado que en este caso es el propio menor el que se realiza la fotografía de sí mismo y en muchos casos la envía con consentimiento a otro menor.

El teléfono móvil como instrumento de grabación o realización de fotografías en Internet en general y en las redes sociales en particular como vehículo para la difusión de lo grabado, convergen generando otro tipo de conductas violentas en las que, si bien el acto criminal principal se realiza en el espacio físico y no es propiamente un cibercrimen, sí que deben ser mencionadas, dado que la utilización de tales imágenes en el ciberespacio puede tener una entidad lesiva singular y propia.

En este caso hablamos de ***happy slaming***, que son conductas realizadas por grupos de menores o jóvenes adultos consistentes en la grabación de comportamientos violentos o vejatorios contra otras personas, generalmente menores conocidos víctimas de *bullying*, pero también personas mayores o cualesquiera otros individuos que puedan ser objeto de violencia y burla.

Finalmente, el *cyberbullying* es la modalidad *online* del acoso escolar, y fue definido por Smith y otros como:

> "Comportamiento agresivo e intencional repetido a través de medios electrónicos realizado por un grupo o individuo contra el que la víctima no puede defenderse por sí misma".
>
> (Smith y otros, 2008, pág. 376)

Existen diferentes clasificaciones de los tipos de acoso dependiendo de a qué ámbito haga referencia. En función de la vía por la que se produce el acoso, podemos distinguir:

- mensajes de texto recibidos en el teléfono móvil;
- fotografías o vídeos realizados con las cámaras de los móviles y posteriormente enviadas o usadas para amenazar a la víctima con hacerlo público;
- llamadas acosadoras al teléfono móvil;
- e-mails insultantes o amenazantes;
- salas de chat en las que se agrede a uno de los participantes o se excluye socialmente;
- el acoso mediante los programas de mensajería instantánea y páginas web donde se difama a la víctima, se "cuelga" información personal o se hacen concursos en los que se ridiculiza a los demás.

También se puede clasificar a partir del tipo de acción que se realiza:

- provocación incendiaria,
- hostigamiento,
- denigración,
- suplantación de la personalidad,
- violación de la intimidad,
- exclusión y
- amenazas o infundir miedo.

Por último, podemos distinguir dos tipos de *cyberbullying*: el reforzador del *bullying* ya emprendido y el acoso entre iguales a través de TIC sin antecedentes. En el primer tipo, el agresor es fácilmente identificable y los efectos de las víctimas son sumativos a los que padecía pero también los amplifica e incrementa. En el segundo tipo, se trata de una forma de acoso indirecto altamente premeditado e intencionado, donde el acosador es desconocido, lo que magnifica el sentimiento de impotencia por parte de la víctima. Se caracteriza por: exigir dominio y uso de las TIC, tiene muchas formas o tipos de acoso; provoca el sentimiento de desamparo legal ya que aunque se cierre una web se puede abrir otra instantáneamente; invade ámbitos de privacidad y aparente seguridad, como es el hogar; y el acoso se hace público.

3.2. Los ciberdelincuentes sociales

De la misma forma que sucede con los ciberdelincuentes económicos, es muy difícil establecer características generales de los delincuentes que realizan ciberdelitos sociales y todo ello porque esta categoría incluye delitos con motivaciones muy dispares.

Ante la incapacidad de poder analizar cada uno de los perfiles de los autores de todos los cibercrímenes sociales, nos vamos a centrar en aquellos que más incidencia tienen en el plano de la comunicación social como son el *cyberstalking*, el *cybergrooming* y el *cyberbullying*.

Respecto al *cyberstalker*, los pocos estudios apuntan a que el perfil varía del *stalker offline*. Suelen ser hombres solteros con trabajo, que tienen conocimientos medios o altos de informática, cuya edad media es de 40 años aunque el rango de edad puede variar de 18 a 67 años.

Existen cuatro tipos de *cyberstalker* siguiendo la clasificación propuesta por Bocij y McFarlane:

- el vengativo (*vindicative*),
- el integrado (*composed*),
- el íntimo (*intimate*) y
- el colectivo (*collective*).

De acuerdo con la clasificación, el *cyberstalker* de tipo vengativo se corresponde con el tipo más violento, que generalmente presenta antecedentes delictivos. Además, suele tener un nivel alto de manejo de las tecnologías y usan una amplia gama de métodos para acosar a sus víctimas, como el envío de correos masivos, el envío de troyanos, el robo de identidad, etc. El tipo integrado tiene como objetivo molestar e irritar a sus víctimas sin intención de mantener algún tipo de relación sentimental con ellas. Presentan un nivel alto de manejo de Internet y, a diferencia del *cyberstalker* de tipo vengativo, no suelen tener antecedentes delictivos ni presentar historial psiquiátrico previo. La tercera categoría propuesta, los denominados *cyberstalkers* íntimos, tienen como objetivo establecer una relación íntima con sus víctimas y el medio que suelen emplear para contactar con ellas es el correo electrónico y las webs de citas. El nivel de manejo de Internet de este tipo de *cyberstalkers* varía desde el que apenas tiene conocimientos hasta el que tiene conocimientos altos. Y finalmente, se define como *cyberstalkers* colectivos aquellos casos en los que dos o más personas se unen para acosar a una misma víctima a través de medios tecnológicos. Este tipo de agresores se caracterizan por tener conocimientos amplios de informática y por emplear técnicas muy variadas para acosar a sus víctimas.

Respecto al perfil de *cybergroomer*, a diferencia de lo que ocurre con el *cyberstalking*, sí que sufre modificaciones con respecto al agresor en el espacio físico. Desde una perspectiva criminológica, el *cybergroomer* es menos peligroso que el agresor tradicional. Mientras que el agresor tradicional suele llevar a cabo sus ataques contra niños como forma de autogratificación debido a una necesidad de ejercer dominio, poder o control sin ser consciente del daño que provocan, el ciberagresor realiza su ataque como respuesta a sus fantasías sexuales, provocadas por sus desordenes psicológicos, necesidad de escapar de la soledad, dificultad en sus relaciones personales, baja autoestima; pero sí que son conscientes de su conducta y del daño que pueden hacer. No tienen intención real de llevar a cabo sus fantasías y en la mayoría de los casos son sujetos que se dedican a molestar a menores en Internet, que no entrarían siempre en la categoría de pedófilos y agresores violentos o sádicos.

En definitiva, los ciberagresores tienen mayor empatía con las víctimas, mayor autocontrol, menor impulsividad y menor índice de desviación sexual que los agresores tradicionales.

Uno de los factores que está presente es la relación entre el aislamiento social y la existencia de una sexualidad compulsiva. Internet facilita vencer la barrera del aislamiento y comunicarse con otros factores que, sumados a otros, como poder investigar previamente el perfil de las posibles víctimas y elegir a la más vulnerable, aumenta el número de potenciales abusadores sexuales que lleguen a serlo. Otro punto a tener en cuenta es que el ciberespacio favorece el anonimato y aumenta la sensación de seguridad del agresor, en el sentido de que disminuye la percepción del riesgo a ser descubierto.

Finalmente, una de las formas de cibercriminalidad que más repercusión está teniendo en los medios es el *cyberbullying*. Respecto al perfil de agresores, se pueden diferenciar dos tipos: por un lado, los proactivos, que son aquellos que cometen ataques para conseguir un fin; y por otro lado, los reactivos que agreden como respuesta a una provocación, agresión o amenaza. La mayoría de los estudios sitúan la prevalencia de los agresores entre un 4% y un 18%.

Respecto a las características de los *ciberbullies*, suelen darse en mayor medida en los cursos de segundo y tercero de secundaria, como ocurre en el *bullying* tradicional. En cuanto al sexo de los agresores, la mayoría de los estudios indican que suelen ser chicos; no obstante, este resultado no se replica en todos los estudios, encontrándose algunos estudios donde las chicas igualan a los chicos en agresiones e incluso llegan a superarlos. Teniendo en cuenta las características que presentan, las conductas de *cyberbullying* son de tipo psicológico y emocional, como insultar, extender rumores falsos, hablar mal, etc.; no

es de extrañar que sean las chicas quienes las perpetren, pues en el *bullying* tradicional son estas las conductas que más ejecutan las chicas, siendo las relacionadas con la fuerza física y las amenazas las que ejecutan los chicos.

Por último, se han encontrado factores que potencian que un alumno se convierta en agresor, entre los que desatacan: tener una percepción favorable sobre las conductas de acoso escolar, tener conocimientos específicos de Internet así como usarlo frecuentemente, tener acceso a un ordenador privado y hacer uso de él en dependencias poco vigiladas.

3.3. Las víctimas de los ciberdelincuentes sociales

En los últimos tiempos, el ciberespacio se ha convertido en un ámbito de comunicación social donde, especialmente en la redes sociales, los usuarios pueden crear un perfil y trasladar al mundo virtual elementos de representación de su realidad física.

Ante la multiplicidad de tipos de victimización social existente, se hace muy difícil extraer elementos comunes que nos permitan establecer un perfil único de cibervíctima social, si bien es cierto que algunos estudios apuntan a que en la mayoría de casos las víctimas son jóvenes; y no es de extrañar, puesto que, como muestran los estudios, la victimización social está relacionada con la cantidad y tipo de uso que se hace de Internet. Hoy en día se cuenta con multitudes de herramientas, como la mensajería instantánea y las redes sociales, que permiten realizar actividades de riesgo, y especialmente desde su fácil acceso con los *smartphones*, como colgar fotos personales para que las vean los amigos, hacer comentarios sobre el estado de ánimo o acerca de noticias y temas de actualidad, poner información personal sobre el lugar de nacimiento o el estado civil en la web personal, agregar a personas al círculo de contactos individual, comentar las fotos de otros, tener conversaciones verticales en páginas propias o ajenas, mantener conversaciones privadas en chats de las redes, etc. Todas estas formas de comunicación están más generalizadas entre la población juvenil y por lo tanto, no resulta extraño que sean quienes más sufren este tipo de victimización. Aun así, no son solo los jóvenes las víctimas de este tipo de ataques, también los adultos pueden ser víctimas de ciberacoso en la Red.

Son precisamente los adultos quienes sufren más las conductas de *cyberstalking*. El primer problema al que se enfrentan los investigadores a la hora de estudiar la victimización por este tipo delictivo es que **abarca muchas conductas,** como acoso, contacto repetido no deseado, robo de identidad, recibir insinuaciones sexuales, amenazas, etc. y que **dificultan establecer características generales de los victimizados**.

Un ejemplo claro de esta dificultad son los datos de prevalencia del fenómeno tan dispares. Así, el porcentaje de víctimas ofrecido por los estudios varía entre el 4% y el 41%, dependiendo generalmente del modo en el que se evalúa. Entre las conductas que más se padecen están las de recibir el contacto repetido no deseado de personas a las que previamente se les ha pedido que paren, publicar información sin autorización y la suplantación de identidad, dándose en menor medida las conductas de amenazas y acoso sexual.

Pese a los escasos estudios existentes sobre los perfiles de las **víctimas de *cyberestalking***, parece que hay concordancia con las características de la modalidad *offline*, siendo estas en su mayoría de los casos **mujeres de menos de 30 años no casadas o divorciadas**. Efectivamente, todos los estudios indican que tienen más riesgo de sufrir este tipo de cibervictimización las mujeres, hasta dos veces más que los hombres, aunque estos también son víctimas de este tipo de delincuencia. Una de las diferencias que se dan con el *stalking* es que es mucho más probable que la víctima no conozca a su agresor.

También se ha comprobado que **la víctima más probable es el agresor**, al menos así se constata en el estudio en el que determinaron que aquel que realiza más comportamientos desviados en Internet, como contactar con alguien en repetidas ocasiones cuando le han pedido que pare, acosar o molestar a alguien por Internet, solicitar sexo a alguien que no quiere, amenazar por Internet, descargar música o películas pirata y enviar o recibir imágenes de contenido sexual, incrementa la probabilidad de sufrir actos de *cyberstalking* o, quizás con más precisión, de *cyberharrassment*. Concretamente, multiplica por seis la probabilidad de que alguien contacte en repetidas ocasiones cuando previamente se le ha pedido que no lo haga, por diez la probabilidad de sufrir acoso *online*, por quince las solicitudes de sexo no deseado y el *cyberstalking* en general aumenta catorce veces.

Otros factores de riesgo asociados es el uso constante de las redes sociales y de una forma específica, el mayor número de fotos subidas a las redes sociales, el número de actualizaciones de estado y el número de cuentas de redes sociales. También la mensajería instantánea y el contacto con extraños. Esto viene a decir que **el comportamiento de la víctima en Internet son predictores significativos de la victimización**.

Ved también

Elementos que, como veremos en el módulo "La prevención del ciberdelito", son necesarios tenerlos en cuenta de cara a la prevención del delito y sobre todo si tenemos en cuenta las graves consecuencias que puede llegar a tener para las víctimas.

Si bien es cierto que las consecuencias pueden variar mucho dependiendo de los múltiples factores que intervienen, se han encontrado que entre las consecuencias que más se repiten están los cambios bruscos de humor y sueño, tener pesadillas, trastornos de alimentación, ansiedad, angustia, impotencia y temor por la seguridad.

Para finalizar con el perfil de las víctimas de *cyberstalking*, es conveniente destacar que aunque no existen estudios que permitan establecer la cifra negra, sí que hay estudios que hablan de las **razones por las que las víctimas prefieren no denunciar su situación de acoso en la Red** y son principalmente por tres motivos:

- El primero de ellos es que hay tipos de conductas que la víctima no puede denunciar como acoso porque no están contempladas.

- En segundo lugar, porque hay ocasiones en las que la víctima considera que los actos no son constitutivos de delito o son los suficientemente graves como para que la policía los tenga en cuenta.

- Y en tercer lugar, porque consideran que denunciar no va a servir para nada. En ocasiones se menosprecia este tipo de delincuencia y se minimiza su gravedad al no existir un contacto físico entre el acosador cibernético y la víctima, sin embargo, puede ser tan amenazante y aterrador como los casos de acoso tradicional.

El siguiente punto a tratar dentro de este apartado está representado por un sector que también es víctima de cibercrimenes sociales, pero que requiere de una mayor protección por parte de todos los sectores de la sociedad por su especial vulnerabilidad, el de los **menores**.

Si la casa y la escuela, la protección familiar e institucional, parecían barreras complejas de superar, algo menos lo son desde el momento en que se ha abierto a los menores, y también a los potenciales agresores de los mismos, una ventana tan grande para la intercomunicación social como es el ciberespacio.

Cita

"Internet terminó con la era de la casa como refugio, al igual que la artillería acabó con la del castillo como fortaleza."
K. Pease (2001, pág. 24)

De entre los usuarios privados potenciales victimarios de la cibercriminalidad, destacan en la actualidad, por su importancia social y por el crecimiento exponencial de su incorporación al ciberespacio, los menores de edad, nacidos ya en la era de Internet, acostumbrados totalmente al uso de las TIC y tendentes a pasar mucho más tiempo en el ciberespacio que cualesquiera otros usuarios, en los que centraremos posteriormente un análisis más pormenorizado.

Los menores pueden ver atacado su **patrimonio**, al tratar de utilizar su ingenuidad para la realización sobre ellos de estafas tradicionales realizadas por medios informáticos o al dañarse los datos informáticos que posean mediante los ataques de *malware*; pero no es ese el bien jurídico más en riesgo en su caso. Más bien son bienes jurídicos personalísimos, como la intimidad, la libertad sexual o la libre formación de la sexualidad para los que estén en periodo de formación en este ámbito, los que pueden verse especialmente afectados por la cibercriminalidad.

En cuanto a la **intimidad**, hoy la Red es la forma de interrelación social más poderosa que existe, y en una época en que la búsqueda de la identidad lleva a la multiplicación de la comunicación social como la adolescencia, instrumen-

tos como el correo electrónico o las redes sociales pueden ser tanto un magnífico instrumento para conocer a otros jóvenes, como un peligroso modo de difundir información privada que puede ser utilizada con malos fines.

Algo similar ocurre con la **libertad sexual** y la **libre formación de la sexualidad** en el caso de los menores de trece años: para estos últimos Internet no solo es un medio de información que puede llegar a ser peligroso sin algún tipo de control educativo, sino que especialmente es un medio de proliferación de la difusión de pornografía infantil que revierte en la multiplicación de este fenómeno y en la consiguiente explotación de miles de menores en todo el mundo para el lucro de organizaciones criminales poderosas. En el caso de los adolescentes, la Red también puede convertirles en objetivo de acosadores sexuales que aprovechen el anonimato del ciberespacio para hacerse pasar por "iguales" y entablar un primer contacto para tratar de lograr posteriormente el contacto sexual.

El uso de Internet por parte de los menores está aumentando de forma exponencial y lo seguirá haciendo durante los próximos años. Los últimos estudios apuntan a que se adquiere el primer móvil sobre los 10 años y el primer *smartphone* entre los 12-14 años. Pero lo que resulta significativo es que este masivo uso de Internet por parte de los jóvenes se realiza sin apenas control de los padres.

Son muchos los estudiantes que usan sus ordenadores personales, *smartphones* y otros servicios móviles y los de sus amigos, sin ningún tipo de supervisión parental, y sin ningún tipo de orientación previa, ni de la familia, ni de las instituciones escolares o demás instituciones públicas sobre el uso seguro de Internet. Y esto se corresponde con la constatación de que la mayor parte de los padres, profesores y adultos en posiciones de responsabilidad en relación con los niños están desinformados sobre los riesgos del ciberespacio y no son capaces de educar para la prevención de los ataques a los menores en el ciberespacio. La cuestión es importante, pues según estudios recientes, la monitorización por parte de los padres del comportamiento de los menores en Internet reduce significativamente el riesgo de estar expuesto a materiales o a conductas peligrosas.

También se constata en el mismo estudio, sin embargo, que la eficacia de tal actividad de monitorización disminuye conforme aumenta la edad de los menores. A esto hay que sumar la conclusión de otros estudios relativos a los efectos de las medidas de protección parental para evitar la victimización *online* de los menores. La instalación de filtros y otras formas de software para el control parental no tiene efectos significativos en la exposición de los menores a contenidos nocivos o en la victimización por cibercrímenes.

El análisis de las conductas que realizan los menores en Internet es necesario para conocer el proceso de victimización. Respecto a las redes sociales, el 55% las usa como forma de comunicación social para sus relaciones de amistad, amorosas y familiares, pero también para contactar con desconocidos o con conocidos compañeros del colegio. Y el uso no es del todo ocasional: el 23% de los jóvenes visita su perfil varias veces al día, el 34% por lo menos una vez al día, y el 17% por lo menos una vez a la semana; de todo lo cual no hay conocimiento mayoritario de los padres según los propios menores: el 42% de los encuestados que accedían a las redes sociales afirmaban que sus padres conocían la existencia de su perfil, pero solo el 26% confirmaban que su familia lo había visitado.

El acceso y utilización de redes sociales conlleva, de algún modo, la realización de actividades que pueden incidir en una potencial victimización:

- El 49% "postea" información personal relativa a la escuela en la que estudia;
- el 29% el nombre completo;
- y el 29% la dirección de correo electrónico;
- pero también es llamativo comprobar el 59% intercambia imágenes con contenido sexual, entre los que destaca las fotos con desnudos parciales de hombres con un 28% y de mujeres un 17%.

Junto con las redes sociales también es habitual el uso de los canales de chat por parte de los menores y, conforme se verá posteriormente, tal ámbito de comunicación conlleva un mayor riesgo de victimización que otros, como las redes sociales, debido al tipo de contacto virtual inmediato que le caracteriza. El porcentaje de menores que hace uso de este tipo de herramienta es de un 18% pero todo parece indicar que se está dejando de usar y se sustituye por otras formas de interrelación personal con las redes sociales.

Algo similar sucede con el uso del *e-mail* por parte de los menores de edad: pese a tratarse de una poderosa herramienta para la comunicación entre personas, su uso está esencialmente asociado a la comunicación profesional y, por tanto, al entorno laboral, siendo escaso (el 14%) su uso por parte de los menores de edad según los estudios existentes.

Por el contrario, los blogs son herramientas de comunicación que han comenzado a ser muy populares entre los adolescentes. El porcentaje de adolescentes que han creado un blog o diario personal en el ciberespacio pasó de un 19% en el 2004 a un 28% en el 2006. Hay significativas diferencias entre su uso según el sexo: las adolescentes crean blogs en un porcentaje mucho más alto

(35%) de lo que lo hacen los adolescentes (20%), creciendo tal diferencia de porcentaje con la edad (las adolescentes de 15 a 17 años los crean un 38% frente al 18% de los adolescentes de la misma edad).

Entrando a analizar de forma concreta los perfiles de los menores víctimas, estos dependerán del tipo de comportamiento delictivo al que hagamos referencia. Aun así, de forma general la investigación demuestra que la mayoría de los menores son victimizados por personas cercanas a su entorno.

En cuanto al caso concreto del *cyberbullying*, el porcentaje de menores que dicen haber sufrido algún tipo de conducta está entre el 20% y el 50%, reduciéndose este porcentaje entre un 2% y un 7% cuando la violencia sufrida es severa. Y esta variación de datos se debe a las diferencias metodológicas en los estudios, lo que imposibilita generalizar sobre la prevalencia e incidencia del fenómeno.

Tampoco hay coincidencia en los porcentajes relativos al género. Algunos estudios informan sobre la tendencia de los chicos a ser agresores y las chicas a ser víctimas, mientras que otros estudios no encuentran diferencias. Datos que, pese a la necesidad de mayor investigación, apuntan a contradecir las cifras del *bullying* tradicional, donde tanto agresores como víctimas son en su mayoría chicos, salvo en determinadas conductas como "hablar mal", que las hacen y las reciben más las chicas.

En cuanto a la edad, sucede algo parecido. Hay estudios que señalan que cuanta más edad hay más probabilidad de riesgo, mientras que otros sitúan la franja de mayor riesgo entre los 12 y 15 años, incluso se encuentran otros estudios donde lo importante no es la edad sino las acciones que realiza el estudiante, como se muestra a continuación.

Uno de los mayores predictores, que aumenta la probabilidad de ser víctima en un 70%, es ser agresor. Esto enlaza con otros estudios, como el de Patchin e Hinduja, que muestra como un elemento significativo y configurador del ciberagresor el haber sido previamente víctima. Por el contrario, los estudiantes que habían sido víctimas tenían un índice de riesgo ligeramente inferior de ser ciberacosador que los estudiantes que no lo habían sido.

Lectura recomendada

S. Hinduja; J. Patchin (2008). "Personal Information of adolescent on the Internet: A Quantitative Content Analysis of MySpace". *JA* (vol. 31, núm. 1).

Otro factor asociado a la victimización es la frecuencia de acceso a Internet tanto para chicos como para chicas. Respecto al uso concreto, los jóvenes que participaron en más actividades en línea son más propensos a experimentar el acoso en línea. De forma concreta, es el uso de la mensajería instantánea y de las webcams el que aumenta la probabilidad de ser acosados de forma repetida.

También se ha demostrado que los niños con padres menos involucrados en Internet tienen mayor probabilidad de convertirse en víctimas. En relación con los adultos, es necesario destacar que más de la mitad de las cibervíctimas no les informan de los incidentes y solo el 35% de los alumnos que son testigos de este tipo de acciones lo hacen, lo que puede estar indicando que, del mismo modo que sucede en el *bullying* tradicional, impera la ley del silencio.

Por otra parte, y muy relacionado con las especiales características del nuevo ámbito de oportunidad criminal que es el ciberespacio, parece que existe una relación entre el anonimato que puede brindar Internet y la victimización por ciberacoso en el ámbito escolar. Esta conclusión podría derivarse del dato de que casi la mitad de las víctimas cibernéticas no conoce a sus acosadores. Frente a la necesidad de un contacto personal y directo que conlleva el *bullying*, con los consiguientes riesgos que ello lleva aparejado para el agresor, así como la propia percepción del daño que se está causando, el ciberacoso permite ocultar la identidad del agresor y evitar así las consecuencias o, cuanto menos, evitar el efecto de las mismas en la motivación del agresor.

Por último, la investigación ha demostrado que el *cyberbullying* tiene consecuencias psicológicas para las víctimas, entre las que destacan que el 42,5% se siente frustrado, el 40% enfadado y el 27% triste. Otros estudios hablan de la ansiedad y la depresión como factores de riesgo para sufrir victimización, sin embargo, hay que tener cautela con estas conclusiones puesto que estos factores pueden ser tanto causa como consecuencia del fenómeno.

Riesgos para el agresor

Especialmente el riesgo a ser identificado, pero también a recibir represalias, o a percibir un reproche social.

Junto con el *cyberbullying* el comportamiento criminal en el que puede existir una significativa victimización de jóvenes es el *online grooming* o ciberacoso sexual en Internet. El *grooming*, término con el que los analistas de los depredadores sexuales se refieren a las conductas de acercamiento de los pederastas a sus víctimas, previas al propio contacto o ataque sexual, ha pasado de los parques a La Red, donde por motivos obvios son muchos más los menores, especialmente las chicas, que pueden ser objeto de un ataque de ese tipo.

En la cuestión del perfil de las víctimas potenciales del *grooming*, y dejando de lado el estudio de los rasgos de la personalidad que inciden en el riesgo de sufrir un ataque de este tipo, resulta de especial interés a los efectos de valorar posteriormente el modelo penal de intervención la cuestión de la edad de la víctima. El Código penal ha situado el tope legal en 13 años, frente a lo primeramente establecido por la enmienda, que presentó la necesidad de la tipificación del precepto que se remitía como límite a la "minoría de edad". En el *grooming* tradicional, el llevado a cabo por el pedófilo, el objetivo del agresor era, como se ha visto, el menor de 12 años, sin embargo, los estudios existentes señalan que en el *grooming* que usa las TIC, la edad de la víctima aumenta. El 99% de las víctimas de intentos de ataques sexuales a través de Internet comprendía edades entre los 13 a los 17 años, quedando el 1% para víctimas de 12 años, y no encontrándose ataques a menores de dicha edad. Es significativo, además, que el 48% de los ataques de *grooming* se llevaban a cabo

sobre menores de 13 y 14 años. Esto concuerda con la forma de comportarse de los jóvenes en Internet y con la evolución de la "inocencia" en los menores: hasta los 14 años los menores tienden a retraerse y a tener gran cuidado a la hora de tratar esas temáticas y de contactar con extraños en Internet. Esto cambia a partir de los 15 años, cuando los menores comienzan a tener riesgos, a contactar con personas desconocidas y a renunciar a parte de su privacidad.

Interesa ahora, por el contrario, el análisis de la victimización y, especialmente, lo relativo a la propia conducta de la víctima en relación con el riesgo de ser víctima de un ciberataque de *grooming*.

Pues bien, el análisis de la conducta de ciberacoso sexual a menores constata que prácticamente todas las modalidades de ataque se configuran en torno a una similar dinámica, en la que el paso inicial suele ser el previo envío, por parte de la víctima, de información personal a personas desconocidas.

En efecto, los estudios victimológicos existentes parecen demostrar que mientras que el mero hecho de colgar información personal en páginas web o redes sociales no es un factor que incide en el aumento de riesgo de recibir un ataque de *grooming*, sí lo es el enviar directamente información personal a desconocidos. El dato es importante si tenemos en cuenta que el 55% de los usuarios jóvenes de 12 a 17 años hacen pública parte de su información en webs o redes sociales, y también es lógico si partimos de que el sujeto que realiza *grooming* lleva a cabo un acercamiento personal que tendrá más posibilidades de ser exitoso si es la propia víctima la que ya se ha prestado a enviar información privada al agresor.

De nuevo las actividades cotidianas de la víctima, en este caso una de ellas íntimamente ligada con su privacidad, constituye un elemento decisivo en la selección del agresor de la víctima del ciberataque.

4. Los cibercrímenes políticos

El ciberespacio también se ha convertido en un medio de comunicación poderoso que sirve a los estados e instituciones para la aplicación de políticas. Internet puede convertirse, por tanto, en un instrumento para la lucha política o ideológica de muchas formas distintas: puede ser vehículo de transmisión de la información, que a su vez puede ser una forma de captación ideológica muy poderosa, puede ser un medio para el ataque a servicios estatales o institucionales de todo tipo en un momento en el que todos los estados dependen de alguna forma y en muchas de sus funciones del funcionamiento de Internet, y puede ser un medio sencillo de comunicación entre individuos o grupos separados geográficamente pero unidos por una misma finalidad política o ideológica.

4.1. Caracterización de los ciberdelitos políticos

Entre las distintas formas de cibercriminalidad política destaca especialmente el **ciberterrorismo**, que se refiere a la utilización de Internet para la realización de ataques terroristas que atenten contra la vida o salud de miles de personas en todo el mundo.

El término *ciberterrorismo* se utilizó en un primer momento bien para referirse a los ataques a sistemas informáticos con efectos tan graves que generaban un temor comparable al que produce el terrorismo tradicional, o bien para englobar los ataques a sistemas informáticos motivados políticamente y realizados para intimidar o coaccionar a los Estados a cambio de determinadas prestaciones; hoy se utiliza este, en sentido amplio, como forma de referirse a los efectos de riesgo social que conlleva la unión entre terrorismo global y nuevas tecnologías de la información y la comunicación; esto es, para englobar todo un grupo de comportamientos distintos llevados a cabo por organizaciones terroristas pero caracterizados todos ellos por la utilización de la Red para la difusión y comunicación de contenidos relacionados con la actividad de la banda armada o para la realización de ataques informáticos directos, tal y como ya han demostrado algunos estudios criminológicos.

A su vez, los delitos de ciberterrorismo se pueden dividir en tres categorías:

1) incitación y propaganda terrorista,
2) actividades de apoyo informacional y
3) ciberataques directos.

1) Dentro del primer grupo, **incitación y propaganda terrorista**, se incluirían aquellas categorías relacionadas con el uso de las TIC para llevar a cabo amenazas contra sujetos, en particular, Estados, organismos o formas de organización social y cultura, como foros de propaganda de terrorismo islamista en el que se ensalcen y justifiquen sus actividades, etc.

2) En el segundo grupo, las **actividades de apoyo informacional**, se incluyen aquellas en las que se hace uso de las TIC para la difusión de mensajes internos, de órdenes explícitas o incluso para recaudar fondos a través de páginas web de supuestas asociaciones benéficas o de ONG; como forma de reclutamiento de futuros terroristas a través de foros, chats y canales IRC, visitados por individuos receptivos a tal ideología extremista; como "campo de entrenamiento virtual" para los terroristas, con la transmisión de los conocimientos necesarios para realizar los atentados o para dotarse de los instrumentos requeridos para hacerlo.

3) En tercer lugar, los **ciberataques directos**, entre los que destacan principalmente la denegación de servicios contra objetivos sensibles del Estado al que se ataca, bien siendo este el objetivo directo, o bien como forma de impedir el ejercicio de los servicios de inteligencia o cualesquiera otros servicios necesarios para la defensa del Estado de que se trate. También entrarían dentro de esta última modalidad el envío de *malware* o el propio acceso informático ilícito siempre que el objetivo sea dañar una estructura de defensa del "enemigo".

Otras de las formas destacadas de cibercriminalidad política es la **ciberguerra** o la guerra cibernética, que consiste en la utilización de Internet por parte de gobiernos de todo el mundo para realizar ataques contra otros Estados o instituciones.

Ejemplos de ciberguerra

Un claro ejemplo de ciberguerra fue el ataque de denegación de servicios de Rusia a Georgia durante la guerra de Ossetia y la infección con el virus Stuxnet a los sistemas informáticos del programa nuclear iraní llevado a cabo por Israel.

Finalmente, podríamos incluir dentro del tipo de cibercriminalidad política los ataques de ***ciberhacktivismo*** que cada vez están adquiriendo más relevancia. Engloba todo un conjunto de ataques llevados a cabo por *hackers* informáticos, pero no con una finalidad maliciosa de defraudar a las víctimas, de robarles información para traficar con ella o de causar daños para perjudicarles económicamente, ni siquiera con la mera voluntad de superación de barreras que parecía distinguir a *hackers* y *crackers*, sino con la intención de lanzar un mensaje ideológico, de lucha política y defensa de ideas generalmente relacionadas con la libertad en Internet, aunque teniendo cabida cualesquiera otras convicciones ideológicas.

El hacktivismo o ciberactivismo político se puede manifestar en ataques de distinto tipo, desde ataques de denegación de servicios contra páginas web, hasta la entrada ilícita en webs ajenas para cambiar el contenido público de las mismas y adecuarlo a sus mensajes, pasando por la difusión libre de software que permita la realización de estos ataques por parte de otros usuarios, la

creación de blogs y webs o de grupos en las redes sociales más importantes, en los que se informa de los objetivos político-ideológicos del hacktivismo, se organizan protestas y acciones y se definen los objetivos que se deben combatir.

4.2. Los ciberdelincuentes políticos

No existe un perfil único de ciberdelincuente político, pues, como se ha visto en el subapartado anterior, la cibercriminalidad política abarca delitos dispares, que aun teniendo un objetivo político o ideológico, presenta perfiles muy distintos. No es lo mismo el cyberhate que la ciberguerra llevada a cabo por servicios de inteligencia de Estados o el ciberterrorismo cometido por grupos organizados.

La primera tipología que vamos a destacar es la de los grupos más o menos organizados que realizan tanto el ciberhacktivismo como el ciberterrorismo. Estos grupos suelen ser agrupaciones en forma de células horizontales unidas en lo vertical únicamente por un mensaje o idea común que se transmite a todas y que cada una de ellas ejecuta a su propio modo. Esta estructuración propia del terrorismo de Al Qaeda puede estar presente de forma más tenue en los grupos terroristas más tradicionales que operan en el ciberespacio y que siguen bajo el estricto orden jerárquico, pero sobre todo lo está en el terrorismo yihadista, que utiliza el ciberespacio como forma de transmisión global de mensajes de odio y de incitación a la violencia. Este mismo tipo de funcionamiento organizativo en el que el único orden jerárquico es ideológico o "de mensaje", en el que existen a partir de ahí unas relaciones horizontales y no verticales entre todos los miembros del grupo, parece imperar también en el hacktivismo, tal y como muestra, según los datos existentes hasta el momento, el desarrollo del grupo Anonymous.

Anonymous

Anonymous es un grupo de hacktivistas abierto e indefinido, conformado por *hackers,* entre los que hay desde expertos hasta meros iniciados, a los que unen convicciones ideológicas antisistema, en general, y en particular contrarias a las restricciones legales en Internet, que venían realizando actividades *hacker* en general y ataques DDoS en particular a Estados y organizaciones empresariales.

Los ciberactivistas suelen ser grupos abiertos e indefinidos de personas con conocimientos informáticos pero entre los que puede haber desde *hackers* a meros iniciados, generalmente jóvenes, a los que unen convicciones ideológicas antisistema, en general, y en particular contrarias a la restricción de Internet. El poder de este tipo de grupos estriba, por una parte, en la fácil sustituibilidad de sus miembros unida a la inmutabilidad de la idea o mensaje; por otra, en lo atractivo que resulta para un sector de la población como el juvenil que prácticamente ha entrado en la etapa adulta al mismo tiempo que ha explotado el ciberespacio como lugar de interconexión mundial, las ideas consistentes en fomentar que Internet se mantenga libre de intromisiones y censuras.

Además de los grupos organizados, también es posible que los cibercrímenes políticos sean perpetrados por un sujeto sin relación organizativa con otros sujetos. Esto suele ocurrir con el *cyberhate*, donde una persona crea una web en la que difunde mensajes de odio sin depender de ninguna estructura organizativa y con el hacktivismo, donde una persona ataque a otras webs o instituciones por convicciones políticas.

Jester

Jester es un *hacker* que durante el 2009 y el 2010 realizó ataques contra lo que él había definido como "webs yihadistas" utilizando el programa que denominó Xerxes y afectó a más de 29 webs.

4.3. Las víctimas de los ciberdelincuentes políticos

Las **víctimas de los ciberataques políticos** tampoco responden a un perfil concreto, de hecho, hay tantos como tipos de cibercrímenes existen. Sin embargo, a diferencia de las víctimas que ya se han estudiado en este módulo, presentan una particularidad: por lo general **van dirigidos a un colectivo o a un Estado**.

Dos ejemplos: denegación de servicios a Georgia e infección del virus Stuxnet

Dos ejemplos claros son el ataque de denegación de servicios de Rusia a Georgia durante la guerra de Ossetia y la infección con el virus Stuxnet a los sistemas informáticos del programa nuclear iraní llevado a cabo por Israel.

El primero de ellos se produjo en agosto del 2008, cuando tropas militares rusas respondieron a lo que consideraron una provocación de Georgia por haber entrado en el territorio semiautónomo de Ossetia. No solo atacaron con bombas y balas, sino también con un ataque de DDoS, que afectó a múltiples páginas web del Gobierno de Georgia, dejando sin uso varios servicios de Internet y obstruyendo y dificultando la comunicación de varias de las oficinas con sus tropas y ciudadanos. Los ataques de denegación de servicios vinieron unidos a otros ataques de *hackers*, en los que se modificaban las webs oficiales del Gobierno de Georgia con mensajes de propaganda nacionalista rusa. Aunque Georgia acusó al Gobierno Ruso de perpetrar un ciberataque contra ellos, Rusia negó el patrocinio o el apoyo de tales conductas alegando que provendrían probablemente de personas con un excesivo sentimiento nacionalista y como respuesta a la agresión de Georgia.

Precisamente en relación con Rusia tuvo que ver también el ataque perpetrado contra Estonia en primavera del año anterior, 2007, cuando se decidió retirar una estatua de bronce al "soldado soviético" de un parque del puerto marítimo de Tallin. Las autoridades del país esperaban protestas airadas de los rusos o de los habitantes de su país de origen ruso, pero no todo ese conjunto de ciberataques, generalmente de denegación de servicios, que tuvo prácticamente paralizado durante varias semanas el ciberespacio de aquel país y que duró casi un mes hasta que el Gobierno pudo estabilizar la situación.

Otro ataque, quizás el más llamativo, fue el del virus gusano Stuxnet, presuntamente creado por el Gobierno de Israel, y destinado a infectar los sistemas informáticos utilizados en el programa nuclear iraní. Aunque los ciberataques entre Israel y los países árabes o los *hackers* islamistas radicales (muy particularmente un grupo de *hackers* marroquís pero también de otros países) existen desde 1999 cuando empezó una guerra de ataques cibernéticos que no ha parado, el capítulo del Stuxnet es distinto, pues supone un boicot informático de primer orden que habla por sí solo del poder del ciberespacio. Además, lo cierto es que el Stuxnet parece haber tenido éxito, cuanto menos según las noticias que llegan a Occidente: este virus ha logrado, aprovechando una vulnerabilidad desconocida del sistema, tomar el control de parte del sistema operativo que debía ser de uso exclusivo de los iraníes para el control de su programa nuclear, y está retrasando este de forma más que significativa.

Enlace recomendado

Podéis leer el artículo del virus Stuxnet en: http://www.europapress.es/internacional/noticia-israel-iran-israel-probo-gusano-informatico-sabotear-instalaciones-nucleares-iranies-20110116062133.html.

Finalmente, es necesario destacar que el análisis de este tipo de victimización es realmente complicado, sobre todo teniendo en cuenta que las víctimas pueden sentirse tentadas a no divulgar los ataques puesto que pueden evidenciar la vulnerabilidad de sus propios sistemas.

Resumen

En resumen, desde una perspectiva criminológica podemos distinguir tres tipos de delitos que responden a los sujetos que realizan el delito y sus objetivos, pudiendo diferenciar, por tanto, aquellos delitos que tienen como objetivo la obtención de un beneficio patrimonial, los que tienen como objetivo el ataque a una persona individual y los que tienen un objetivo ideológico o institucional.

Estas tres categorías responden a su vez a los tres grandes ámbitos funcionales del uso de las TIC, que pasó de ser un ámbito dedicado al plano económico a convertirse en un medio de comunicación interpersonal y también en un medio poderoso que sirve a los Estados e instituciones para la aplicación de políticas.

Esta evolución de las TIC conlleva la aparición de múltiples formas de criminalidad que, si los objetivos que persiguen los cibercriminales son distintos, también estos responden a perfiles distintos como se ha podido comprobar. Incluso hemos podido constatar cómo la evolución de las TIC también ha repercutido en los cibercriminales cambiando las características específicas de su perfil.

Es necesario, por tanto, hacer un estudio detallado de cada uno de los ciberdelitos, así como de las características de los actores implicados, y hacer evaluaciones periódicas que permitan obtener la información necesaria para elaborar medidas destinadas a prevenir la ciberdelincuencia.

Ejercicios de autoevaluación

1. El término *ciberterrorismo* en sentido amplio se refiere a...

a) los ataques a sistemas informáticos con efectos tan graves que generan un temor comparable a los que produce el terrorismo tradicional.
b) los ataques realizados para coaccionar a un Estado.
c) los efectos de riesgo social que conlleva a la unión del terrorismo global y las TIC.
d) Ninguna de las respuestas anteriores es cierta.

2. El acosador que se dirige a sus víctimas de forma calmada y tranquila y cuyo propósito es causar malestar a las víctimas a través de una variedad de comportamientos amenazantes es un ciberagresor...

a) vengativo.
b) colectivo.
c) integrado.
d) íntimo.

3. El *cyberbullying* es un cibercrimen de tipo...

a) social.
b) económico.
c) político.
d) puro.

4. El comportamiento que lleva a cabo un adulto a través de Internet para ganarse la confianza de menores con el fin de concretar encuentros para obtener concesiones de índole sexual es denominado...

a) *cyberstalking*.
b) *cybergrooming*.
c) *cyberbullying*.
d) *stalking*.

5. El cyberhate consiste en...

a) el acoso a menores aprovechando las posibilidades de las cámaras web.
b) la realización de fotografías de desnudos totales o parciales para colgarlas en las redes sociales.
c) infligir daño de forma voluntaria o repetida a través de texto electrónico.
d) la incitación al odio racial en el ciberespacio.

6. Un conjunto de ataques llevados a cabo por *hackers* informáticos con la intención de lanzar un mensaje ideológico, de lucha política y defensa de ideas, generalmente relacionadas con la libertad en Internet, se denomina...

a) *cybergrooming*.
b) ataque DoS.
c) *spam*.
d) hacktivismo.

7. Entre las diferencias entre el *child grooming* del mundo virtual y el del mundo físico encontramos que...

a) el perfil del agresor es el mismo en las dos modalidades.
b) el agresor en el mundo virtual es menos peligroso que en el mundo físico.
c) el perfil de la víctima coincide en las dos modalidades.
d) Todas las opciones son verdaderas.

8. ¿Cuál de las siguientes características no es típica de las víctimas de *cyberstalking*?

a) Tener pareja.
b) Ser joven.
c) Ser mujer.
d) Ser hombre.

9. Cuando hablamos del sujeto que accede a un sistema informático para robar información o causar algún otro tipo de daño, nos referimos al ciberdelincuente denominado...

a) *hacker.*
b) *cracker.*
c) *insider.*
d) *scriptkiddies.*

10. Respecto a las víctimas de los cibercrímenes económicos,...

a) los hombres son los que más sufren este tipo de delincuencia.
b) suelen tener un nivel formativo bajo.
c) suelen tener un nivel económico medio bajo.
d) las mujeres son las que más sufren este tipo de delincuencia.

Solucionario

Ejercicios de autoevaluación

1. c

2. c

3. a

4. b

5. d

6. d

7. b

8. a

9. b

10. a

Glosario

backdoor *m* Se trata de un programa que se introduce en el ordenador y establece una puerta trasera a través de la cual es posible controlar el sistema afectado sin conocimiento por parte del usuario.

blog *m* Abreviatura de weblog. El término fue acuñado por Jorn Barger en 1997. Aunque en la actualidad se confunde con el uso de las webs, pretende ser una publicación de un diario *online*, donde los textos aparecen del más reciente al más antiguo.

bot *m* Tipo de virus que permite el acceso remoto del sistema informático a través de la Red.

botnet *m* Conjunto de redes de ordenadores comprometidos y controlados por el mensajero.

bullying *m* En español se emplea el término *acoso escolar* y es definido como el comportamiento dañino, intencional y repetido a manos de una o más personas, dirigido contra quien tiene dificultad para defenderse.

ciberagresor *m y f* Sujeto que utiliza las TIC para realizar un crimen, generalmente mediante el ataque a otra u otras personas.

cibermula *m y f* Dícese del colaborador o recolector de los beneficios en Internet y que luego envía el dinero, por medios seguros de transmisión, a los autores del delito.

cibervíctima *m y f* Persona que sufre los efectos de un ciberdelito.

data breach *m* Cualquier forma de destrucción, modificación o acceso a datos de empresas o de particulares.

gusano *m* Programa que realiza copias de sí mismo, alojándolas en diferentes ubicaciones del ordenador con el fin de colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios.

hacking *m* Cualquier conducta por la cual un sujeto accede a un sistema o equipo informático sin autorización del titular del mismo, de una forma tal que tiene capacidad potencial de utilizarlo o de acceder a cualquier tipo de información que esté en el sistema.

hacktivismo *m* Difusión de mensajes de protesta en Internet generalmente dirigidos contra organismos o Estados en relación, con la voluntad de mantener libre de normas el ciberespacio.

moobing *m* Acoso laboral.

nick *m* Abreviatura de *nickname*. Apodo que utiliza un usuario para identificarse y comunicarse en la Red.

pharming *m* Táctica fraudulenta que consiste en cambiar los contenidos del DNS, ya sea a través de la configuración del protocolo TCP/IP o del archivo lmhost, para que el usuario, cuando teclea la dirección web de su entidad bancaria en su navegador, entre en realidad a una web falsa muy parecida o igual a la original, en la que acaba desvelando sus datos bancarios.

phishing *m* Mecanismo criminal que emplea tanto ingeniería social, como subterfugios técnicos para robar los datos de identidad personales de los consumidores y los de sus tarjetas de crédito o cuentas bancarias.

protocolo p2p (*peer-to-peer*) *m* Protocolo que permite el intercambio directo de información, de igual a igual.

scriptkiddies *m y f pl* Son jóvenes que, no siendo expertos *hackers* capaces de acceder a sistemas mediante programaciones propias, realizan sus ataques informáticos, generalmente, eligiendo las víctimas al azar, aprovechando programas y *scripts* básicos y causando daños en muchos casos, más fruto de su impericia o de la dañosidad del *malware* utilizado, que de sus habilidades.

sexting *m* Envío a otro menor por mensajería telefónica (aunque también por medio de correos electrónicos o sistemas de mensajería en redes sociales) de fotografías de desnudos, posturas eróticas o partes del cuerpo, con intención de formar parte de algún mensaje de tipo sexual, realizadas generalmente por un menor.

smartphone *m* Teléfono móvil que ha sido diseñado para permitir al usuario la instalación de aplicaciones.

sniffer *m* Programa de captura de tramas de información que no están destinadas a él.

stalking *m* Acoso continuado a una persona con permanentes solicitudes de contacto que son continuamente rechazadas por la víctima.

troyanos *m pl* Programas maliciosos que mediante ventanas emergentes recogen claves; y en general cualquier otra técnica que, utilizando software permite perfeccionar el engaño haciendo creer a la víctima que está fuera de peligro.

Bibliografía

Alleyne, B. (2010). "Sociology of Hackers Revisited". *TSR* (vol. 58).

Boyd, D. M.; Ellison, N. B. (2007). "Social network sites: Definition, history, and scholarship". *JCMC* (vol. 13, núm. 1).

Brown, I.; Korff, D. (2009). "Terrorism and the Proportionality of Internet Surveillance". *EJC* (vol. 6, núm. 2).

Calmaestra Villén, J. (2011). *Cyberbullying: prevalencia y características de un nuevo tipo de bullying indirecto*. Tesis doctoral. Córdoba: Servicio de Publicaciones de la Universidad de Córdoba.

Cano Paños, M. Á. (diciembre, 2008). "Internet y terrorismo islamista: aspectos criminológicos y legales". *Eguzkilore* (núm. 22). San Sebastián.

Curran, K.; Concannon, K.; Mckeever, S. (2008). "Cyber terrorism attacks". En: L. J. Janczewski; A. M. Colarik (eds.). *Cyber Warfare and Cyber Terrorism*. Hershey-Londres: IGI Global.

De la Corte Ibáñez, L.; Giménez-Salinas Framis, A. (2010). *Crimen.org. Evolución y claves de la delincuencia organizada*. Barcelona: Ariel.

Green, J. (noviembre, 2002). "The myth of ciberterrorism". *WM*.

Henson, B. (2010). "Cyberstalking". En: B. S. Fisher; S. P. Lab (eds.). *Encyclopedia of victimology and crimeprevention*. Thousand Oaks, CA: Sage.

Hinduja, S.; Patchin J. (2008). "Personal Information of Adolescents on the Internet: A Quantitative Content Analysis of MySpace". *JA* (vol. 31, núm. 1).

Jagatic, T.; Johnson, N.; Jakobsson, M.; Menczer, F. (dic., 2005). "Social Phishing". *Communications of the ACM*. Bloomington.

Janczewski, L. J; Colarik, A. M. (eds.) (2008). *Cyber Warfare and Cyber Terrorism*. Hershey-Londres: IGI Global.

Kohlmann, E. F. (julio, 2008). "'Homegrown' Terrorists: Theory and Cases in the War on Terror's Newest Front". *ANNALS* (núm. 618).

Lenhart, A. (2009). "Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging". *PIALP*. Washington D.C. Disponible en http://www.pewinternet.org/Reports/2009/Teens-and-Sexting.aspx.

Li, Q. (2007). "Bullying in the new playground: Research into cyberbullying and cyber victimization". *Australasian Journal of Educational Technology*.

Livingstone, S. (2008). "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression". *NMS* (vol. 3, núm. 10).

Mason, K. L. (2008). "Cyberbullying: A Preliminary Assessment for School Personnel". *Psychology in the Schools* (vol. 4, núm. 45).

Mcfarlane, L.; Bocij, P. (2003). *An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers* (vol. 9, núm. 8).

Mitchell, K. J.; Finkelhor, D.; Wolak, J. (2007). "Youth internet users at risk for the most serious online sexual solicitations". *AJPM* (vol. 32, núm. 6).

Ortega, R.; Calmaestra, J.; Mora-Merchan, J. (2008). "Cyberbullying". International Journal of Pychology and Psychological Therapy (vol. 2, núm. 8). Disponible en http://redalyc.uaemex.mx/redalyc/pdf/560/56080204.pdf.

Pease, K. (2001). "Crime futures and foresight: Challenging criminal behaviour in the information age". En: D. Wall (ed.). *Crime and the Internet*. Londres: Routledge.

Pittaro, M. L. (2007). "Cyber stalking: An Analysis of Online Harassment and Intimidation". *IJCC* (vol. 1, núm. 2).

Pittaro, M. (2011). "CyberStalking: Typology, Etiology, and Victims". En: K. Jaishankar (ed.). *CyberCriminology. Exploring Internet crimes and criminal behavior*. Boca Raton: CRC Press.

Pratt, T. C.; Holtfreter, K.; Reisig, M. D. (2010). "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory". *Journal of Research in Crime and Delinquency*.

Raymond, E. S. (2001). *How To Become A Hacker*. Disponible en http://www.catb.org/~esr/faqs/hacker-howto.html.

Reyns, R. W.; Henson, B.; Fisher, B. S. (2011). "Being Pursued Online: Applying Cyber-lifestyle-Routine Activities Theory to *Cyberstalking* Victimization". *CJB*.

Rollins, J.; Wilson, C. (enero, 2007). "Terrorist Capabilities for Cyberattack: Overview and Policy Issues". *CRS Report for Congress*.

Smith, P. K.; Mahdavi, J.; Carvalho, M.; Fisher, S.; Russell, S.; Tippett, N. (2008). "Cyberbullying: Its nature and impact in secondary school pupils". *Journal of Child Psychology and Psychiatry* (vol. 49, núm. 4, pág. 376-385).

Spitzner, L. (2000). "Know Your Enemy: The Tools and Methodologies of the Script Kiddie". Disponible en http://www.project.honeynet.org/papers/enemy/.

Subrahmanyam, K.; Reich, S. M.; Waechter, N.; Espinoza, G. (2008). "Online and offline social networks: Use of social networking sites by emerging adults". *JADP* (núm. 29).

Taylor, P. A. (2005). "From hackers to hacktivists: speed bumps on the global superhighway?". *NMS* (vol. 7, núm. 5).

Vandebosch, H.; Van Cleemput, K. (2009). "Cyberbullying among youngsters: profiles of bullies and victims". *New Media and Society*.

Yar, M. (2006). *Cybercrime and society*. Londres: Sage.