CAPÍTULO 3

CIBERDELINCUENTES Y CIBERVÍCTIMAS

José Luis de la Cuesta Arzamendi y Ana Isabel Pérez Machío

SUMARIO: I. Introducción. II. El delincuente informático. 1. El perfil del ciberdelincuente. 2. Los denominados hackers. 3. Los denominados crackers. 4. Los denominados phreackers. 5. Los denominados viruckers. 6. ¿Una nueva generación de ciberdelincuentes? III. Las víctimas de la cibercriminalidad. 1. La contribución de la víctima a la comisión del ciberdelito. 2. Cifra negra y víctimas. IV. Bibliografía.

I. Introducción

Como en la mayor parte de los hechos delictivos, también en la cibercriminalidad el estudio de los sujetos presenta un interés fundamental desde el prisma criminológico.

De un lado, el estudio de los sujetos activos, los ciberdelincuentes, cuyos perfiles y características resultan claves de cara a una adecuada prevención de los hechos delictivos. Pero igualmente, el análisis de las víctimas de la cibercriminalidad; en efecto, distintos posicionamientos victimológicos han analizado el perfil y el papel que ocupa la víctima en la denominada «delincuencia tradicional».

II. El delincuente informático

1. El perfil del ciberdelincuente

Individualizados los elementos que inciden en las dificultades de detección y averiguación de los ciberdelitos y en los correspondientes a la identificación de los autores y a la concreción de la norma aplicable, corresponde igualmente a la Criminología la elaboración del perfil del conocido como delincuente informático. Aunque algo ya se ha adelantado ante-

riormente sobre la necesidad de que domine el medio informático, es preciso profundizar en la presente cuestión para verificar si dichos conocimientos han de ser exhaustivos, si ello limita el colectivo de autores a una determinada clase social o a un colectivo específico y si, en definitiva, estamos ante la creación de una nueva categoría de autores, ajena a los planteamientos clásicos existentes acerca de los delincuentes y su perfil.

Por lo que respecta al delincuente cibernético, tal y como se ha venido manifestando, el procesamiento electrónico de datos se convierte en un relevante factor criminógeno que acrecienta las posibilidades de actuación ilícita y la posición cualificada de quienes poseen especiales conocimientos en esta materia y de quienes están encargados del manejo de tales sistemas informáticos[1].

Desde esta perspectiva, la concreción del perfil del delincuente informático ha experimentado una cierta trasformación o desplazamiento. En efecto, tradicionalmente se consideraba que la delincuencia informática era propia de jóvenes –de clase media– obsesionados por el medio –que perseguían la obtención de poder, conocimientos o una mejor consideración entre sus compañeros[2]– y de empleados que actuaban con ánimo de venganza y sin fines lucrativos inmediatos[3].

En todo caso, en la actualidad, los planteamientos basados en la personalidad de los autores de las infracciones tradicionales devienen insuficientes, en la medida en que aquélla puede ser relevante cuando la informática es instrumento para la perpetración de esos delitos, pero no cuando ésta es sólo el objeto de los actos delictivos[4]. En el sentido mencionado anteriormente, la delincuencia informática afecta no sólo a la delincuencia

---

[1] MATA Y MARTÍN, *Delincuencia informática*, pg. 25, destaca que la mayor facilidad de acceso y el conocimiento de la información procesada o almacenada proporciona una plataforma y la ocasión para quienes se sitúan en contacto con los sistemas informáticos, convirtiéndose en autores de hechos punibles.

[2] Así lo viene destacando GALLARDO RUEDA, «Delincuencia informática», pg. 372.

[3] Así lo recogían SINNROD y REILLY, «Cyber-crímenes», pg. 184, cuando apuntaban que más del 80% de los ataques sufridos por sistemas operativos de entidades o empresas eran cometidos por empleados que, estando autorizados para acceder al sistema, abusaban de dicha confianza y producían daños económicos muy graves a las entidades.

[4] Véase, GÓMEZ NAVAJAS, *La protección de los datos personales*, pg. 54.

económica sino que comprende también ataques a otros bienes jurídicos, con lo que el perfil del delincuente, lejos de limitarse a empleados o a jóvenes que se plantean el acceso ilícito como un reto intelectual, con propósito lúdico, o por venganza[5] o mera curiosidad[6], se desplaza hacia otra clase de sujetos que, sin despreciar el perfil clásico, intensifican sus objetivos[7], destacándose los propósitos lucrativos y otras finalidades más agresivas que, de forma indiscriminada, se dirigen contra las instituciones básicas para el funcionamiento del Estado[8], afectando gravemente a la seguridad, integridad y fiabilidad de la información de los datos que la representan.

En este orden de cosas, la peculiaridad de los medios empleados para la comisión de esta clase de delincuencia (sistema informático) permite individualizar un perfil muy concreto de delincuente que no coincide con el delincuente marginal, sino con sujetos que tienen conocimientos del medio informático. En efecto, mientras la Criminología clásica y tradicional ha venido destacando los aspectos sociales, económicos y culturales como determinantes para la comprensión de una específica delincuencia, fundamentada en el fenómeno de la exclusión social, la complejidad del cibercrimen rompe con esta forma de entender y de explicar el fenómeno criminal. El acceso a los sistemas informáticos requiere de una cierta destreza y de determinados conocimientos que se alejan sobremanera de los motivos vinculados al fenómeno de la exclusión social[9].

Sin embargo, si bien se requieren unos conocimientos mínimos relacionados con el medio informático, a tenor de la diversidad de comporta-

---

[5] En este sentido, ROMEO CASABONA, «Poder informático», pg. 40; MORÓN LERMA, «Internet y Derecho Penal», pg. 72; ALASTUEY DOBÓN, «Apuntes sobre», pg. 460; ROVIRA DEL CANTO, *Delincuencia informática*, pg. 108.

[6] Un ejemplo significativo de delincuencia informática motivada por mera curiosidad es la de los «hackers». Así se ha plasmado por varios autores; véase, en este sentido, ESBENSHADE «Hacking», pg. 54.

[7] En este sentido, ROMEO CASABONA, *Poder Informático*, pg. 36.

[8] ANARTE BORRALLO, «Incidencias de las nuevas tecnologías», pg. 203, donde, junto a estos perfiles destaca la heterogeneidad que presenta el perfil conjunto y la necesidad de tomar en cuenta perfiles específicos como el de «pederasta internauta».

[9] En este sentido YAR, *Cibercrime and Society*, pg. 19, subraya la necesidad de construir nuevos paradigmas teóricos que desde la perspectiva criminológica permiten explicar la realidad de este nuevo fenómeno criminal.

mientos susceptibles de ser considerados como delitos informáticos, en general, los sujetos activos de los mismos no precisan de especiales conocimientos técnicos cualificados[10], bastando con que se ostente un coeficiente intelectual medio y que se tengan oportunidades de realizar el hecho y las aprovechen[11]. Por eso la doctrina distingue una diversidad de autores que se agrupan en los siguientes: 1º los operadores, programadores u otros sujetos que acceden legítimamente a la elaboración del programa[12]; 2º cualquier sujeto, a través de las terminales públicas o interceptando las líneas de transmisión de datos a distancia[13]; 3º los titulares legítimos del sistema[14].

Las características inherentes al perfil del delincuente informático y la primacía del elemento subjetivo de ánimo de lucro configuran una categoría de autores hasta ahora poco conocida. Los estudios criminológicos que tradicionalmente se han venido ocupando del perfil de los delincuentes dibujaban a sujetos motivados por diversos móviles que procedían a la comisión de determinados ilícitos, sin que fueran requeridos conocimientos técnicos específicos para llevar a cabo tales comportamientos (piénsese en cualquiera de los delitos contra bienes jurídicos personalísimos o contra el patrimonio e, incluso todos aquellos ilícitos en los que se requiere la condición de funcionario público al sujeto activo de los mismos).

---

[10] RUIZ VADILLO, «tratamiento de la delincuencia informática», pg. 64.

[11] ALASTUEY DOBÓN, «Apuntes sobre», pgs. 456 y 460. En idéntico sentido, ACURIO DEL PINO, «La delincuencia informática», pg. 13, donde viene considerando como sujetos activos de esta modalidad delictiva a aquellas personas que tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informáticos, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

[12] ÁLVAREZ VIZCAYA, «Consideraciones político-criminales», pg. 267.

[13] CAMACHO LOSA, *El delito informático*, pgs. 83 y 84. En idéntico sentido, REYNA ALFARO, «La víctima en el delito informático», pg. 6, cuando considera que el 90% de los delitos informáticos son ejecutados por empleados de las empresas o instituciones afectadas.

[14] CORCOY BIDASOLO/JOSHI JUBERT, «Delitos contra el patrimonio», pg. 137. En este mismo sentido, VELÁZQUES BAUTISTA, *Derecho de las tecnologías*, pg. 245, entiende que quienes ejecutan las conductas tipificadas pueden estar vinculados a la empresa donde el delito se produce o no, por lo que estos casos implican una relación laboral o de prestación de servicios.

Ahora bien, los sujetos que intervienen en las prácticas constitutivas de cibercriminalidad deben poseer una serie de conocimientos técnicos mínimos del medio informático que les permita acceder al sistema; la ausencia de dicha capacidad impedirá su participación en este proceso criminal. Por lo tanto, si bien no se puede afirmar que se trata de una modalidad delictiva limitada a una determinada clase social, sí se trata de un fenómeno relegado a un colectivo específico de autores, esto es, aquellos que ostenten un coeficiente intelectual medio, que les permita tener conocimientos informáticos y tengan oportunidad de acceder al sistema y realizar el hecho ilícito, entre los que cabe destacar a los hackers, los crackers, los phreackers y los viruckers, entre otros.

2. Los denominados hackers

El término hacker encuentra sus orígenes en 1959, cuando surgió un grupo de programadores con mucho talento que desarrollaron un conjunto de programas que eliminaban otros programas dentro de un mismo sistema operativo.

Hoy en día no sólo están interesados en las vulneraciones de seguridad que pueda presentar un cierto sistema informático, sino también en conocer el porqué de las mismas. La problemática reside en que esta práctica es potencialmente muy peligrosa si las motivaciones del hacker no tienen buena intención, de aquí que, en no pocos sistemas, se vaya tipificando ya directamente como delito.

Aunque la imagen pública de los hackers no es muy buena, se dice que disponen de una serie de normas ampliamente conocidas, que es lo primero que se transmite a cualquiera que quiera introducirse en el entorno. Dentro de ésas podemos encontrar las siguientes:

- No hacer daño intencionadamente.

- Modificar sólo lo estrictamente necesario para entrar y evitar ser localizado.

- No hackear nunca ni por venganza, ni por intereses personales o económicos, así como no comentar con nadie las acciones realizadas.

No se mueven por premios tradicionales, como la aceptación social o los beneficios económicos, sino que su mayor logro sería superar el reto que se les había planteado. El principal motor de sus acciones es burlar la seguridad de que disponen los sistemas; se dedican a curiosear cómo funcionan los sistemas, sin buscar hacer daño, cómo inutilizar, alterar o destruir la información almacenada.

Un hacker considera su ocupación como un reto intelectual, apoyado en el siguiente código:

– El acceso a los ordenadores y a cualquier cosa que te pueda enseñar cómo funciona el mundo debería ser ilimitado y total. Siempre deberías poder ponerle las manos encima.

– Toda la información debería ser gratuita. Si no tienes el acceso a la información necesaria para arreglar las cosas ¿cómo vas a arreglarlas? Además, un intercambio libre de información permite una mayor creatividad en general y evita tener que reinventar la rueda una y otra vez.

– Desconfía de la autoridad. Lo mejor para favorecer el intercambio de información es un sistema abierto sin fronteras entre un hacker y la información que necesita.

– Los hackers deberían ser juzgados por sus «hacks», no por criterios extraños como calificaciones académicas, edad, raza o posición. De hecho, uno de los hackers originales era Peter Deutsch, un niño de doce años que dominaba el TX-0 y que estaba por ello perfectamente integrado en el grupo.

– Puedes crear arte y belleza en un ordenador; aparte de la belleza en su sentido tradicional, los hackers creen que el código de un programa tiene una belleza propia, sobre todo cuando está escrito con maestría.

– Los ordenadores pueden mejorar tu vida. Si sabes cómo pedírselo, un ordenador hace lo que tú le pidas y eso para los hackers representa la posibilidad de que cada usuario tenga a su disposición una herramienta poderosísima con la que puede hacer cualquier cosa que desee.

Como se puede comprobar, los hackers tradicionales no pueden ser considerados vándalos, puesto que lo más que solían hacer era dejar tarjetas de visita, no siendo extraño que el propio hacker comunicara al admi-

nistrador del sistema hackeado los fallos de seguridad encontrados y propusiera una posible forma de solucionarlos. Dicha actitud se llegó incluso a profesionalizar, creando empresas encargadas de asaltar equipos informáticos para detectar y corregir dichos fallos.

3. Los denominados crackers

Este término se usa para los que realizan acciones dañinas. Fue acuñado por los propios hackers hacia 1985 en defensa contra el uso no apropiado por parte de los medios de comunicación del término hacker. El origen se encuentra en la traducción del término «crack», que significa «romper» en inglés. Un cracker debe conocer perfectamente tanto el software como el hardware.

Usan software propio, desarrollado para sus fines, o en muchas ocasiones los que se distribuyen de forma gratuita en muchas páginas webs, como generados aleatorios de números o rutinas desbloqueadoras de claves de acceso para con ello lograr romper las claves de acceso a los sistemas.

Se relacionan en grupos relativamente pequeños y muy secretos, donde es difícil entrar. En alguna ocasión se les ha denominado cyberpunks[15], por la filosofía antisistema que manejan, que les lleva en muchas ocasiones a atacar los sistemas informáticos de grandes corporaciones que suelen acumular beneficios cuantiosos. A diferencia del hacker, que observa pero no destruye ni modifica, el cracker sí tiene intención de destruir o lucrarse con su actividad. El entrar en un sistema, robar información, copiarla y venderla a un módico precio es una práctica que está a la orden del día en el mundo informático.

Su trabajo suele ser dañino y destructivo, desde el borrado de información al robo de información, con el único objetivo de venderla al mejor postor, normalmente la competencia. Se observan dos tipos de sujetos: 1) los que atacan un sistema informático, roban información y producen

[15] Como se destaca en el informe de Criminología Virtual de McAfee, pg. 6, el cyberpunk es un delincuente en línea que utiliza sus habilidades computacionales para irrumpir en sistemas y redes computacionales.

destrozos en mayor o menor medida, y 2) los que desprotegen software auténtico con protecciones anticopia para hacerlo plenamente operativo.

Dentro de las variantes de los crackers nos encontramos con los que se dedican al:

– Carding: uso ilegal de tarjetas de crédito.

– Trashing: basurero, obtención de información en cubos de basura, como números de tarjetas de crédito, contraseñas, directorios o recibos[16].

Este tipo de delincuentes informáticos pueden ser empleados frustrados de la empresa, con fines maliciosos, que conocen bien las entrañas de la misma y por dónde es más vulnerable, o bien individuos ajenos a la empresa que simplemente quieren demostrar sus habilidades delante de un teclado o con el único fin de divertirse, diversión que obtienen al sabotear sistemas y dañar la organización a la que pertenecen dichos sistemas.

4. Los denominados phreackers

El campo de conocimiento de un phreacker son los sistemas telefónicos, tanto fijos como móviles. En la actualidad, se encuentran centrados en el mundo de la telefonía móvil, aunque deben poseer también grandes conocimientos de informática puesto que el control de la red móvil, así como los datos de usuario que se manejan en la misma, se realiza a través de este tipo de sistema.

Son capaces de construir equipos artesanales que interceptan llamadas o realizan llamadas desde teléfonos móviles sin que el dueño del mismo sea consciente de ello. Realizan la distribución por Internet de instrucciones, componentes o diseño de placas electrónicas para construir dichos aparatos.

---

[16] Como destaca el Informe McAfee sobre Criminología Virtual: la delincuencia organizada en Internet, pg. 13, a menudo la gente no se da cuenta del valor de la información que desecha. Los delincuentes han estado recogiendo información confidencial rebuscando en la basura. Ahora los ciberdelincuentes se han dado cuenta de que la mayoría de las veces, cuando se desecha un ordenador, sigue conteniendo gran cantidad de archivos y datos que se pueden usar con fines lucrativos o de engaño.

Los phreackers tratan tanto de demostrar conocimientos y habilidades, burlando las redes públicas y corporativas de telefonía, como de obviar el pago por el servicio que están usando o conseguir lucrarse con reproducciones no autorizadas de tarjetas SIM de telefonía móvil, cuyos códigos obtienen accediendo a los sistemas de información de las compañías que los almacenan.

El objetivo fundamental de los phreackers son las empresas de telefonía y, en segundo lugar, las grandes multinacionales, a las que derivan la factura de los servicios que utilizan. Por lo general, el phreacker no busca la riqueza en sus estafas, sino más bien enmendar las estafas que, según su punto de vista, las compañías telefónicas ejercen sobre el resto del mundo.

Su motivación es extrínseca y, por lo tanto, económica, puesto que, aun cuando no buscan el dinero de forma directa, tratan de no pagar una factura, lo que es traducible en beneficio económico. En el resto de aspectos son muy similares a los crackers y no disponen de la ética de los hackers.

Son más peligrosos que los hackers, puesto que pueden llegar a ejercer el control de los sistemas de telefonía, realizando escuchas telefónicas que pueden ser usadas como una herramienta realmente útil para cometer un delito.

5. Los denominados viruckers

El ataque realizado por los viruckers consiste en la intrusión en un sistema informático para introducir virus en el mismo, con el objetivo de destruir, alterar y/o inutilizar la información almacenada en el mismo.

Existen diferentes tipos de virus:

- Benignos, que molestan pero no hacen daño.
- Malignos, que destruyen la información o inutilizan el sistema.

Son capaces de instalarse en un sistema informático ajeno con el fin de usar los recursos del mismo para contagiar otros programas y/o sistemas sin el conocimiento del dueño y/o responsable del sistema. Las carac-

terísticas psicopáticas de este colectivo les acerca al grupo de crackers, con una dinámica psíquica reflexiva con un estilo épico.

No existe comunicación puesto que les gusta actuar de forma individual y aislada, sin disponer de un código ético que rija su comportamiento. Este grupo de delincuentes informáticos es altamente peligroso y con gran difusión en el mundo informático.

6. ¿UNA NUEVA GENERACIÓN DE CIBERDELINCUENTES?

Si la extendida caracterización de los ciberdelincuentes como personajes que actúan fundamentalmente solos y hasta más motivados por la publicidad que por el dinero no deja de ser certera, parece corresponderse ya a una etapa anterior. En efecto, los estudios más recientes ponen de manifiesto que, junto con la extensión de los ordenadores, las redes computacionales e Internet, devenidos elementos integrantes de la actividad empresarial y social, se ha producido igualmente una extensión sin precedentes de la multiplicación de las amenazas potencialmente maliciosas y de la generalización de la utilización de los medios y redes informáticos, con fines criminales, favorecidas por el anonimato y alcance internacional de Internet[17].

Como indica el informe de Criminología Virtual de McAfee, a principios de la era computacional el cibercrimen significaba el robo de un PC o el acceso ilegal a un mainframe para obtener información o tiempo adicional de procesamiento. Actualmente, el crimen computacional, sin embargo, contempla una amplia gama de delitos que afectan a las empresas y al valor almacenado en las redes computacionales[18].

La utilización de equipos informáticos (laptops equipados con software de crackeo de contraseñas, en combinación con dispositivos inalámbricos wifi o bluetooth con el fin de apoderarse de bienes muebles o de acceder a todo tipo de bienes inmuebles protegidos por medios electrónicos) y

---

[17] En este sentido, véanse, BRENNER, «Cybercrime, Cyberterrorism and Cyberwarfare», pg. 620 y CÉDRAS, «Un aspect de la Cybercriminalité en Droit français», pg. 596, entre otros.

[18] Informe de Criminología Virtual de McAfee: Estudio Norteamericano sobre crimen organizado e Internet, pg. 2.

hasta de la red con fines criminales: extorsión, todo tipo de fraudes (unidos a trucos psicológicos, como el «Spear Phishing»), apropiación masiva de informaciones (p. e., datos bancarios de consumidores de equipos electrónicos), lavado de dinero, todo ello por no hablar de las modalidades de espionaje –de profesionales (funcionarios, jueces, periodistas) o de personas comunes, espionaje de cuentas de correo electrónico, espionaje o sabotaje entre empresas (hackers y crackers a sueldo)– o de las redes de pederastia o de «happy slapping», constituyen hoy comportamientos criminales habituales[19].

En realidad si atendemos al informe McAffe sobre Criminología Virtual, el crimen cibernético ya superó su etapa de gestación. Ahora es un gran negocio en el que los empresarios del crimen pueden obtener rápidas ganancias con un riesgo mínimo, hecho que está engrosando cada vez más sus filas. Con la continua evolución de la tecnología, las oportunidades para cometer delitos se están globalizando y ya trascienden las geografías, idiomas y apariencias[20].

Ciertamente no ha desaparecido, sino todo lo contrario, la conducta de empleados, contratistas y proveedores (antiguos o presentes) que se aprovechan de los inadecuados sistemas de seguridad para obtener información interna con fines lucrativos, pero lo actualmente más relevante es que el crimen organizado se ha percatado perfectamente de las ventajas de la cibernética y de la red para el logro de sus objetivos y cabe hablar de una «nueva generación de criminales cibernéticos que utilizan tácticas similares a las empleadas por la KGB durante la guerra fría». Así se recluta a los mejores alumnos de las principales instituciones académicas, a fin de proporcionarles las habilidades necesarias (financiándoles incluso estudios informáticos o de otras disciplinas que pueden ayudarles a alcanzar puestos en las empresas que les interesan) para cometer delitos de alta tecnología a nivel masivo[21].

---

[19] Informe de Criminología Virtual de McAfee: Estudio Norteamericano sobre crimen organizado e Internet, pg. 3.

[20] Así se recoge en el Informe McAfee sobre Criminología Virtual: la delincuencia organizada, pg. 7.

[21] En este sentido, GRABOSKY, «Recent Trends in Cybercrime», pg. 18.

Simultáneamente, hay que poner de manifiesto la incursión cada vez mayor de menores en el crimen virtual. Frente a la presencia de los mismos como víctimas de diversos delitos (pornografía infantil o de otro tipo de conductas vinculadas con el abuso de la vulnerabilidad de los mismos en la red), lo cierto es que cada vez son más los menores y jóvenes que llegan a convertirse en protagonistas activos de una buena parte de los delitos cometidos en la red, como los contrarios a la intimidad o los lesivos de otra clase de bienes jurídicos protegidos (agresiones que se graban en el móvil y se cuelgan en Internet, cyberbulling, etc.).

Desde esta perspectiva, la enorme facilidad para la captación de imagen o de voz de cualquier sujeto, conocido o desconocido que han supuesto los avances técnicos de las últimas dos décadas, así como la sencillez de volcar en cualquier parte del mundo y en segundos lo captado o grabado, incrementa la incidencia del fenómeno.

El protagonismo numérico, al menos de estas infracciones, ha pasado de los medios de comunicación en los que adultos violentaban la intimidad de otros adultos, a un nuevo escenario, donde los jóvenes y menores actúan sin la cortapisa que constituyen los medios de comunicación, sus estructuras jerárquicas, los códigos deontológicos y la competencia y denuncia de otros medios[22].

Otro de los ámbitos donde destaca la intervención de menores y jóvenes en la red son los supuestos de hostigamiento y acoso también denominados como mobbing o, atendida la especialidad de los sujetos a los que ahora nos referimos, más acertadamente considerados como prácticas de cyberbulling. Desde esta perspectiva, Internet es un espacio ideal para la ejecución de actos de acceso a través del correo electrónico, los chats, o los portales de vídeos o imágenes en los que puede darse un proceso de denigración de la víctima, de cara a un colectivo de espectadores incuantificable, por lo que se impone el seguimiento de los contenidos de las páginas webs en las que se producen estos ataques y proceder a una interpretación conjunta de los actos atribuibles a menores o jóvenes que puedan ser considerados autores de una conducta de acoso en la red[23].

---

[22] En este sentido, RUIZ RODRÍGUEZ, «Nuevos riesgos, nuevos lenguajes», pg. 105.

[23] RUIZ RODRÍGUEZ, «Nuevos riesgos, nuevos lenguajes», pg. 108.

Se trata de adolescentes con amplio dominio de Internet y escasa edad, que se sienten atraídos por el crimen cibernético, tanto por la fama de los criminales de alta tecnología, como por las expectativas de beneficios y la escasez de riesgos frente a los delitos tradicionales; en no pocas ocasiones los hechos se realizan en lugares públicos: cibercafés y bares o cafeterías con conexión wifi, complicando la ya difícil tarea de detección y persecución.

En definitiva, la complejidad de Internet, a la que venimos aludiendo a lo largo del presente trabajo, dificulta no sólo la tarea de persecución e investigación del denominado cibercrimen, sino también la fijación de unas características específicas de aquellos sujetos responsables de todas ellas. Si bien inicialmente el cibercrimen se habría venido vinculando a autores movidos por razones económicas, lo cierto es que en la actualidad, el perfil del ciberdelincuente pasa tanto por sujetos motivados por razones puramente económicas, como por autores que encuentran su satisfacción personal en el mero acceso ilícito, haciéndose extensivo el colectivo de los mismos incluso a jóvenes y menores que parecen encontrar en la red una mayor seguridad a la hora de cometer todo tipo de conductas lesivas de bienes jurídicos protegidos, amparados en el anonimato.

III. Las víctimas de la cibercriminalidad

Concretadas las circunstancias que explican las dificultades existentes en la determinación tanto de los comportamientos cibernéticos como de sus autores, es papel de la Victimología centrar especialmente la atención en la figura de la víctima de los delitos, su perfil e, incluso, su contribución personal al proceso delictual.

Pues bien, al margen de aquellas cuestiones victimológicas vinculadas al perfil, interesa, en este momento, habida cuenta de la complejidad técnica intrínseca a la realidad de la cibercriminalidad, centrar la atención en dos aspectos victimológicos que, de alguna forma, fomentan la impunidad. Se trata tanto de la específica contribución personal de la víctima a la comisión de las prácticas constitutivas de ciberdelitos, como de la incidencia de la misma en la denominada «cifra negra».

1. La contribución de la víctima a la comisión del ciberdelito

Desde una perspectiva victimológica, diversas teorías han resaltado que la conducta de la víctima no suele ser un elemento neutro, si se busca una explicación a muchos delitos.

La cibercriminalidad se presenta, a este respecto, como una modalidad de delincuencia ocupacional que se concentra en particulares espacios y se vincula a las oportunidades existentes en los mismos[24]. Como algunos autores vienen destacando, los delincuentes adoptan diferentes decisiones a la hora de cometer el delito y estas decisiones están basadas en su conocimiento previo de lo que constituyen buenos objetivos o víctimas. De esta forma, cuando el delincuente identifica una buena oportunidad criminal, es cuando se dan las condiciones para que el mismo decida cometer el delito[25].

Pues bien, en esta forma de entender el fenómeno criminógeno, en cuanto delincuencia ocupacional vinculada a la oportunidad del mismo, destaca la contribución de la víctima a la comisión del concreto delito.

Las teorías del control social tradicionalmente han servido para explicar la racionalidad espacial y temporal de lo que se viene conociendo como delincuencia común, incidiendo en el papel que el espacio y los lugares desempeñan en la distribución del delito. Frente a las teorías del control social que explican el fenómeno de la Cibercriminalidad a partir de la contribución de las propias víctimas, surgen las teorías de la prevención situacional, cuyo objetivo es influir en las actitudes de las potenciales víctimas con la finalidad de reducir las oportunidades delictivas y hacer más difícil la comisión del delito. La teoría situacional reposa en una teoría individual de elección racional de los agresores, que presupone que los delincuentes son, hasta cierto punto, racionales y que consideran muchos factores antes de cometer un acto delictivo, como pueden ser: las características de la víctima, los riesgos de ser descubiertos, la disponibilidad de los objetivos, las posibles ganancias, el tiempo requerido, el peligro físico,

---

[24] Así lo manifiestan Sinrod y Reilly, «Cyber-crimes», pg. 178, cuando subrayan que este fenómeno, desarrollado a través de Internet, se basa fundamentalmente en las oportunidades de acceder a los sistemas.

[25] Véase Medina Ariza, «El control social del delito», pg. 286, siguiendo en este punto a Brantlingham y Branthingham.

la pericia que se necesita y la familiaridad con el método[26]. Pues bien, frente a esta realidad de oportunidades situacionales que favorecen la comisión del delito, las teorías de la prevención situacional proponen una serie de medidas de reducción de oportunidades, que se reconducen a tres grupos.

–En primer lugar, medidas que incrementan el esfuerzo necesario para cometer un delito, entre las que destacan: el endurecimiento de objetivos (barreras físicas, cualquier estrategia de protección); control de acceso (contraseñas); desviación de transgresores (evitar la acumulación de personas conflictivas en el mismo lugar y a la misma hora); control de facilitadores (armas de fuego).

–En segundo lugar, medidas que incrementan el riesgo, como por ejemplo: control de entradas y salidas, vigilancia formal, vigilancia por empleados, vigilancia natural

–En tercer lugar, estrategia de reducción de ganancias[27].

Las medidas de reducción de oportunidades de las teorías de la prevención situacional tienen perfecto acomodo en la prevención de la delincuencia informática, habida cuenta de la estrategia de oportunidades reales para el delincuente y la «contribución» de la víctima a este fenómeno criminógeno.

La cibercriminalidad, vinculada, como se acaba de poner de manifiesto, a la racionalidad espacial del delito a la que contribuyen las enormes oportunidades que determinados sistemas operativos ofrecen a los delincuentes informáticos, tiene mucho que ver con las conductas de sus víctimas. En efecto, en el concreto ámbito de la cibercriminalidad los análisis empíricos tradicionalmente han venido mostrando que la mayoría

---

[26] BARBERET, «La prevención de la victimación», pg. 243.

[27] Para una mayor profundización de esta clase de medidas véanse, entre otros, GARRIDO/STANGELAND/REDONDO, *Principios de Criminología* y MEDINA ARIZA, «El control social del delito».

de los casos de delincuencia informática se ve favorecida o, como mínimo, se simplifica, por la ineficacia o carencia de sistemas de seguridad[28].

Desde esta perspectiva, puede decirse que en no pocos casos las víctimas favorecen y motivan la delincuencia informática, dotando a los autores de las mismas oportunidades reales que una y otra vez facilitan la comisión de todo tipo de ilícitos cibernéticos. La no adopción de sistemas de seguridad o de controles informáticos y el acceso público gratuito de un nutrido grupo de personas (normalmente trabajadores) a determinados sistemas operativos con una misma clave común, son situaciones que evidencian tanto la fragilidad de muchos de los sistemas informáticos de las grandes empresas y de los usuarios particulares, como la oportunidad espacial de la comisión de un concreto delito informático.

Bastaría, en este sentido, con que las potenciales víctimas (empresas, particulares) adoptaran medidas preventivas adecuadas para la seguridad del sistema informático que permitieran disuadir al potencial delincuente cibernético de la comisión del ilícito[29]: incrementando el esfuerzo necesario para cometer el delito (mejora de los sistemas de seguridad del sistema operativo; asignando a todos los usuarios de ordenadores una clave personal de acceso; impidiendo el acceso público y libre; impidiendo que exista un ordenador de uso común para una pluralidad de sujetos sin clave personal[30]); incrementando el riesgo (vigilancia de las entradas y salidas a los sistemas operativos; existencia de un especialista en materia de seguridad informática y de delincuencia informática que asesore en las empresas sobre esta realidad); y, por último, en la medida de lo posible, implantando estrategias de reducción de ganancias que, si bien tradicionalmente se han venido asociando al desplazamiento de bienes, en el caso específico de la cibercriminalidad, puede relacionarse con las intervenciones sobre cuentas

---

[28] Como ya destacara SIEBER, «Las medidas de seguridad», pg. 83, en el concreto caso de empresas víctimas de este fenómeno criminógeno, la inexistencia de medidas de detección de accesos ilícitos necesarias para reducir el riesgo y las pérdidas favorecen la habitualidad en los comportamientos ilícitos, generando unas innecesarias pérdidas.

[29] Véase, entre otros, KATYAL, «Criminal law cyberspace», pg. 1077.

[30] La realidad demuestra que, a día de hoy, son muchos los ordenadores que permiten un acceso libre a cualquier usuario, sin que el principal haya recurrido a una herramienta tan simple como un código de acceso inicial.

corrientes –supuestos de estafa informática– y con los cambios continuos de las claves de acceso a modo de protección del potencial objeto material del delito.

A pesar de la efectividad que parece derivarse de las medidas vinculadas a la teoría de la prevención situacional, éstas tradicionalmente no han estado exentas de críticas en un doble sentido. Por un lado, vinculando este paradigma de prevención con un modelo de sociedad clasista en la que los ciudadanos con medios económicos suficientes se protegerían con innumerables medidas de seguridad, frente a una gran masa poblacional que carecería de recursos suficientes para lograr dichas cotas de protección[31]; y, por otro, considerando que la teoría de la prevención situacional sólo puede servir para frenar la conducta delictiva convencional (delincuencia menor, pequeños hurtos, vandalismo), no resultando eficaz para la prevención de delitos violentos[32].

Ahora bien, ante la efectiva contribución al delito por parte de potenciales víctimas que carecen no ya de sistemas de seguridad eficaces, sino de una mera contraseña o clave personal que, de alguna forma, disuada a cualquier sujeto de acceder a su sistema operativo, las medidas derivadas de la teoría de la prevención situacional se presentan como una vía efectiva de prevención de la delincuencia cibernética, puesto que inciden en la modificación del comportamiento de la víctima y, consiguen, por ende, una reducción de los riesgos derivados de las oportunidades espaciales derivadas de no adopción de simples medidas preventivas ligadas a la seguridad informática[33].

---

[31] MEDINA ARIZA, «El control del delito», pg. 313.

[32] En este sentido, MEDINA ARIZA, «El control del delito», pg. 303, donde recoge las opiniones más críticas que interpretan que este modelo nunca podrá aplicarse con garantías para prevenir delitos violentos en los que la razón no tiene cabida y todo es cuestión de emociones encontradas.

[33] Ésta ha sido precisamente una de las críticas que han recibido algunas de las medidas preventivas adoptadas en el Estado español, donde en nombre de la «seguridad pública y de la seguridad nacional» se han implantado, por ejemplo, cámaras de videovigilancia, que implican directamente una injerencia en la intimidad de los ciudadanos. Así lo ha venido destacando MEDINA ARIZA, «El control del delito», pg. 313.

2. Cifra negra y víctimas

Como ya se ha mencionado en diversas ocasiones a lo largo del presente trabajo, una de las principales características de los delitos informáticos es su elevado nivel de tecnicidad con una clara incidencia en el ámbito probatorio, hecho éste que provoca una alta probabilidad de impunidad que, a su vez, también se vincula a la elevada «cifra negra» existente frente a esta clase de criminalidad.

Lejos de entrar, sin embargo, en cuestiones relacionadas con la tecnicidad de estos comportamientos, que excederían los límites de este trabajo, vamos a centrar la atención en la impunidad derivada de la conocida como «cifra negra» y el papel de las víctimas en la misma. Tal y como se acaba de poner de manifiesto, la contribución de la víctima a la comisión del delito cibernético es determinante en numerosas ocasiones para entender la elevada tasa de criminalidad, pero también la alta cifra negra, al no reconocer su condición de víctima, no presentar denuncias o no continuar hasta el final sus pretensiones procesales[34].

Por lo que respecta a los supuestos en los que las víctimas desconocen su condición de tales, éstos se explican como consecuencia de las dificultades de naturaleza técnica existentes. El sistema de trabajo a tiempo real, que permite el tratamiento instantáneo de los datos o las modificaciones de los programas, o la copia de unos y de otros, por lo general, sin dejar huella de las operaciones realizadas, favorece un fenómeno criminal en el que la víctima desconoce la lesión sufrida o, en última instancia, toma constancia de la misma transcurrido cierto tiempo, desde la comisión del hecho[35]. Son los supuestos de ataques dirigidos contra personas naturales, en los que la cifra negra se relaciona con la llamada «invisibilidad del delito informático»[36]. Esta invisibilidad tendría su razón de ser en la relatividad del espacio y tiempo, anteriormente mencionada, a través de la cual el delincuente se inviste con los más absolutos atributos de intemporalidad y ubicuidad[37]. El carácter anónimo provoca en la víctima la sensación de que la justicia penal no podrá dar con el responsable y siente que se

---

[34] En este sentido, Anarte Borrallo «Incidencias tecnológicas», pg. 206.

[35] Romeo Casabona, *Poder Informático*, pg. 38.

[36] Reyna Alfaro, «La víctima en el delito informático», pg. 7.

[37] Herrera Moreno, «El fraude informático», pg. 931.

enfrenta a un ser invisible frente a cuyos ataques sólo queda resignarse, por lo que pocas veces denuncian los hechos que se dan en su perjuicio[38].

Cuando los ataques delictivo-informáticos son dirigidos contra empresas o corporaciones, la «cifra negra» de criminalidad encuentra también su razón de ser en la «publicidad negativa» que ello significa para las propias empresas atacadas[39]. Los incidentes en Internet suelen ser asociados con el nivel de seguridad informática que poseen las empresas o corporaciones atacadas. Ello genera, como es evidente, desprestigio en la empresa atacada, descrédito de la fiabilidad de la gestión de la propia empresa[40] y, en diversas ocasiones, temor a que como consecuencia de las investigaciones policiales se lleguen a desvelar estrategias o secretos comerciales, industriales o científicos[41]. Por esa razón un alto número de incidentes de seguridad en Internet son mantenidos en reserva por decisión de las propias víctimas[42].

En general, bien sea por el desconocimiento de la intromisión ilegítima, bien por el desprestigio que conlleva la denuncia de un ataque informático, la realidad de la «cifra negra» en el ámbito de la cibercriminalidad se hace más patente que en otros supuestos y genera inevitablemente un sentimiento de impunidad a la hora de afrontar la comisión de estos delitos[43], a pesar de las ventajas de la presentación de denuncias[44].

---

[38] En este sentido, REYNA ALFARO, «La víctima en el delito informático», pg. 8; MORÓN LERMA, *Internet y Derecho Penal*, pg. 27.

[39] REYNA ALFARO, «Aproximaciones victimológicas», pg. 101.

[40] ACURIO DEL PINO, «Delincuencia informática», pg. 17.

[41] ROMEO CASABONA, *Poder Informático*, pg. 39.

[42] Véanse, por todos, HERRERA MORENO, «El fraude informático», pg. 932; MORÓN LERMA, *Internet y Derecho Penal*, pg. 37; y REYNA ALFARO, «La víctima en el delito informático», pg. 8.

[43] ÁLVAREZ VIZCAYA, «Consideraciones político-criminales», pg. 268.

[44] Así lo destacan ROMEO CASABONA, *Poder Informático*, pg. 39 y SARZANA, «Observaciones sobre la victimación informática», pg. 52, cuando señalan como ventajas de la denuncia las siguientes: a) se está en condiciones de apreciar el nivel de riesgo; b) se ven indirectamente incitadas a adoptar sistemas de prevención y de descubrimiento de los delitos; c) se estimula indirectamente la atención del legislador sobre la conveniencia de tomar medidas legales para prevenir y reprimir este fenómeno; d) los órganos judiciales se ven estimulados a profundizar en estos hechos, incluidos los aspectos técnicos, con el fin de encontrar cauces legales adecuados para su persecución y castigo.

Tal y como se ha puesto de manifiesto, la posición de la víctima no favorece la reducción de la cifra negra. Las oportunidades de las que disponen los potenciales autores, frente a colectivos de víctimas que carecen de medidas preventivas eficaces, llegando, incluso, en ocasiones, a no percibir su condición de tales, se presenta como otro elemento adicional que incide nuevamente en la impunidad de estas conductas, al favorecer la invisibilidad de los comportamientos cibernéticos. Con todo, en el sentido manifestado, la potenciación del papel de la víctima, frente a la cibercriminalidad, como para reducir la elevada tasa de cifra negra, se convierte, desde una perspectiva victimológica, en un objetivo fundamental a tener en cuenta, como primeros factores para la erradicación y sanción de estas conductas. En efecto, sólo la adopción de estrategias preventivas de incremento del riesgo y del esfuerzo en la comisión del delito se presentan como instrumentos eficaces en la lucha contra la cibercriminalidad. Si a ello se añade la presentación sistemática de denuncias se conseguirá aminorar la invisibilidad de muchas de estas conductas[45], cuya esencia, junto a la complejidad técnica de los procesos en los que se ubican, reside igualmente en el desconocimiento de las mismas por parte de la propia Administración de Justicia.

IV. Bibliografía

ACURIO DEL PINO, S., «La delincuencia informática transnacional y la Unidad de Delitos Informáticos», en *Revista de Derecho Informático*, 95, 2006, 1-49; ALASTUEY DOBÓN, M. C, «Apuntes sobre la perspectiva criminológica de la delincuencia patrimonial», en *Informática y Derecho: Revista iberoamericana de derecho informático*, 4, 1994, 453-464; ÁLVAREZ VIZCAYA, M., «Consideraciones político-criminales sobre la delincuencia informática: el papel del derecho en la red», en *Internet*

[45] Así lo recoge ACURIO DEL PINO, «Delincuencia informática», pg. 17, cuando destaca que, mediante la divulgación de las posibles conductas ilícitas derivadas del uso de computadores y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración en la administración y la importación de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática.

y Derecho. Cuadernos de Derecho Judicial, 2001, 255-279; ANARTE BORRALLO, E., «Incidencias de las nuevas tecnologías en el sistema penal. Aproximación al Derecho Penal en la sociedad de la información», en *Derecho y Conocimiento*, vol. 1, 2002, 191-25; BARBERET, R., «La prevención de la victimación», en *Manual de Victimología*, coordinado por Baca Baldomero, Echeburúa Odriozola, Tamarit Sumalla, Valencia, 2006, 235-252; BRENNER, S., «Cybercrime, Cyberterrorism and Cyberwarfare», en *International Review of Penal Law*, 77, 2006, 453-473; CAMACHO LOSA, L. *El delito informático*, Madrid, 1987; CÉDRAS, J., «Un aspect de la Cybercriminalité en Droit Francais: le télechargement illicite d'oeuvres protégées par le droit d'auteur», en *International review of Penal Law*, vol. 77, 2006, 589-610; CORCOY BIDASOLO, M./JOSHI JUBERT, U., «Delitos contra el patrimonio cometidos por medios informáticos», en *Revista Jurídica de Cataluña*, 87, 1988, 679-700; ESBENSHADE, Ph., «Hacking: juveniles and undeterred recreacional cybercrime», en *Journal of Juvenile law*, vol. 23, 2002-2003, 52-64; GALLARDO RUEDA, A., «Delincuencia informática: la nueva criminalidad de fin de siglo», en *Cuadernos de Política Criminal*, 1998, 365-373; GARRIDO, V./STANGELAND, P./REDONDO, S., *Principios de Criminología*, 2ª edic., Valencia, 2001; GÓMEZ NAVAJAS, J., *Protección de los datos personales. Un análisis desde la perspectiva del Derecho Penal*, Madrid, 2005; GRABOSKY, P., «Recent Trends in Cybercrime», en *11th. UN Congress on Crime Prevention and Criminal Justice. Workshop 6 –Measures to Combat Computer Related Crime*, Korean Institute of Criminology, 2005; HERRERA MORENO, M., «El fraude informático en el Derecho Penal español», en *Actualidd Penal*, 2001-3, 925-964; KATYAL, W. K., «Criminal law Cyberspace», en *University of Pennsylvania law Review*, 2001, 1003-1114; MATA Y MARTÍN, R., *Delincuencia informática y Derecho Penal*, Madrid, 2002; MCAFFE, *Informe de Criminología virtual de McAfee: estudio norteamericano sobre crimen organizado e Internet*, 2005; AFFE, *Informe McAfee sobre criminología virtual: la delincuencia organizada en Internet*, 2006; MEDINA ARIZA, J. J., «El control social del delito a través de la prevención situacional», en *Revista de Derecho Penal y Criminología*, 2, 1998, 281-323; MORÓN LERMA, E., *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la red*, Pamplona, 1999; REYNA ALFARO, L. M., «Aproximaciones victimológicas al delito informático», en *Capítulo Criminológico*, 31-4, 2003, 93-04; REYNA ALFARO, L. M., «La víctima en el delito informático», en http://www.ieid.org/congreso/po-

nencias/Reina%20Alfaro,%20Luis%20M.pdf; ROMEO CASABONA, C. M., *Poder Informático y Seguridad jurídica*, Madrid, 1988; ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos*, Granada, 2002; RUIZ RODRÍGUEZ, L. R., «Nuevos riesgos, nuevo lenguaje: la violencia virtual», en *Menores y Juventud: nuevos retos*, 2007, 102-108; RUIZ VADILLO, E. «El tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica», en *Poder Judicial*, 9, 1989, 53-84; SAZARNA, C. «Observaciones sobre la victimación informática», en Ágora, 2, 1986, 45-60; SIEBER, U., «Las medidas de seguridad de los usuarios de ordenador», en *Delincuencia informática*, compilado por MIR PUIG, Barcelona, 1992, 83-89; SINROD, E. J./REILLY, W., «Cyber-crimes: A practical approach to the application of Federal computer crime laws», en *Computer High Technology law Journal*, 16, 2000, 177-232; VELÁZQUEZ BAUTISTA, R., *Derecho de las tecnologías de la información y las comunicaciones (TIC)*, Madrid, 2002; YAR, M., *Cibercrime and Society*, California, 2006.