Delincuencia asociada al uso de las TIC

Fernando Miró Llinares

PID_00195950

UOC
Universitat Oberta de Catalunya

Índice

Introducción

La delincuencia en el ámbito de las tecnologías de la información y la comunicación engloban toda una serie de conceptos y conductas que deben ser conocidos y manejados por los profesionales de la criminología. Los presentes materiales servirán al estudiante para que pueda familiarizarse con otro ámbito de la criminalidad, la cibercriminalidad.

Comenzaremos con el análisis de los diferentes conceptos relacionados con el fenómeno para pasar a estudiar su evolución y su estado actual.

Finalmente, se hará un análisis de los distintos tipos de cibercrímenes que existen y que permite establecer una visión general del problema, así como de sus dimensiones.

Objetivos

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

1. Familiarizarse con los conceptos básicos relacionados con la delincuencia y las TIC.

2. Conocer el origen y la evolución de la criminalidad en el ciberespacio.

3. Adquirir conocimientos sobre la realidad de la amenaza del cibercrimen.

4. Conocer los distintos tipos de ataques que se producen en el ciberespacio.

1. Delincuencia y TIC: cibercrimen y cibercriminalidad

El fenómeno de la criminalidad relacionada con el uso de las tecnologías de la información y comunicación sigue siendo totalmente novedoso, y por ello, parcialmente incomprendido por la sociedad en general, y en particular, por las instituciones que tienen que afrontar la prevención de esta amenaza, a pesar de que han pasado más de tres décadas desde comenzó a hablarse de criminalidad informática y más de dos desde que se acuñó en término *cybercrime*.

El cibercrimen forma parte ya de la realidad criminológica de nuestro mundo pero, como se verá posteriormente, en muchas ocasiones se exagera la amenaza que este supone y en otras no se percibe el riesgo real que el uso de las TIC conlleva. La revolución de las TIC, como concepto amplio, abierto y dinámico que engloba todos los elementos y sistemas utilizados en la actualidad para el tratamiento de la información, su intercambio y comunicación en la sociedad actual, en la que se enmarca el fenómeno del cibercrimen, no ha terminado todavía ni lo hará en mucho tiempo, lo que supone que la cibercriminalidad o delincuencia asociada al ciberespacio seguirá expandiéndose y evolucionando en las próximas décadas.

William Gibson

Novelista de ciencia ficción creador del término *cyberspace* en su obra *Neuromancer*, Ace-Books, Nueva York, 1984.

Pese a que el desarrollo de las tecnologías informáticas empezó en los años sesenta y setenta, tuvo su empuje definitivo con la creación de Internet y su posterior universalización, pero en los últimos años la rapidez con la que aparecen las nuevas tecnologías se ha ido incrementando exponencialmente y todo apunta a que seguirá haciéndolo. También son evidentes los efectos sociales que han marcado la revolución de las TIC: gracias a la aparición de Internet y a su popularización a escala planetaria, nos hemos acercado enormemente a la creación del ciberespacio virtual tal y como lo concibiera el que acuñó este término, William Gibson, al haberse configurado de forma paralela al mundo físico un espacio comunicativo e interactivo que, especialmente en la primera década del siglo XXI, ha modificado las relaciones económicas, políticas, sociales y muy especialmente, las personales. Hoy, la utilización de los servicios de Internet o las redes de la telefonía móvil constituyen la forma más común de comunicarse personalmente con familiares, amigos o personas del entorno laboral, y no solo para adultos sino también para los menores de una generación que no entenderá la comunicación entre iguales sin la Red; también es Internet el vehículo por el que fluye ya la mayor parte del dinero en el mundo: todos los bancos y entidades financieras actúan por medio del ciberespacio, y cada vez son más las transacciones económicas y los negocios a pequeña, mediana y gran escala que se llevan a cabo directamente a través de este medio de comunicación global.

Además, todo parece indicar que la incidencia del ciberespacio en todos los aspectos de la vida social no va a ir disminuyendo, sino que seguirá creciendo. Conforme lideren el mundo los denominados "nativos digitales" o nacidos en la era de la Web 2.0 popularizada, con los sistemas informáticos como forma de trabajo y también de diversión, con las redes sociales como forma de interactuación social, con las tecnologías móviles totalmente conectadas y con toda la información a la palma de su propósito, el ciberespacio, como lugar de encuentro por el uso de las TIC, irá expandiéndose, y la novedad del cibercrimen, como de cualquier otro elemento concatenado a ese espacio virtual, que es para muchas personas aún más real que el otro, irá desapareciendo y lo único que cambiará será la concreta manifestación de este a raíz del nuevo aspecto social digno de protección o la nueva tecnología que facilitará o modificará la forma de la comisión del delito.

Nativos digitales

Término acuñado por Marc Prensky en su obra "Digital Natives, Digital Immigrants" para referirse a la generación nacida con la implantación global de Internet.

Lo que también es innegable es que todos esos cambios sociales que estamos viviendo a raíz de los cambios tecnológicos que se están sucediendo tienen su reflejo en la criminalidad como fenómeno social que es. Lo tienen, concretamente, en la aparición de un nuevo tipo de delincuencia asociado al nuevo espacio de comunicación interpersonal que es Internet. De hecho, la evolución del cibercrimen como fenómeno criminológico ha transcurrido de forma paralela, como se verá posteriormente con más profundidad, a la evolución de los intereses sociales relacionados con las TIC: cuando el protagonismo lo tuvieron las terminales informáticas y la información personal que ellas podían contener, aparecieron nuevas formas de afectar a la intimidad de las personas; cuando dichas terminales y la información en ellas contenida comenzaron a tener valor económico y a servir para la realización de transacciones económicas, surgieron las distintas formas de criminalidad económica relacionadas con los ordenadores y muy especialmente el fraude informático, que, a su vez, evolucionó hacia el *scam*, el *phishing* y el *pharming* cuando apareció Internet; finalmente, con la universalización de la Red y la constitución del ciberespacio, comenzaron a surgir nuevas formas de criminalidad que aprovechaban la transnacionalidad de Internet para atacar intereses patrimoniales y personales de usuarios concretos, pero también para afectar a intereses colectivos por medio del ciberracismo o del ciberterrorismo.

Hoy, que el protagonismo empiezan a adquirirlo las redes sociales y otras formas de comunicación personal en las que se ceden voluntariamente esferas de intimidad y en las que se crean relaciones personales a través del ciberespacio, y que a la vez, no disminuye sino que aumenta la actividad económica en Internet, asistimos a un momento álgido de la criminalidad en el ciberespacio, tanto en sentido cuantitativo dado el creciente uso de Internet en todo el mundo y por todo el mundo, como cualitativo al aparecer nuevas formas de delincuencia relacionadas con los nuevos servicios y usos surgidos en el entorno digital.

La evolución del cibercrimen también conlleva una **evolución en sus protagonistas** esenciales, los **criminales** y las víctimas: del ya mítico ***hacker*** estereotipado en el **adolescente introvertido** y con problemas de sociabilidad encerrado en su casa y convertido en el primer ciberespacio en un **genio informático** capaz de lograr la guerra entre dos superpotencias solo desde su ordenador, hemos pasado a las mafias organizadas de cibercriminales, que aprovechan el nuevo ámbito para aumentar sus actividades ilícitas y sus recursos. Y al no ser los cibercrímenes únicamente los realizados con ánimo económico, también varían los perfiles de cibercriminales que cometen delitos, que no son más que réplicas en el ciberespacio de los que ejecutarían en el espacio físico.

Y lo mismo sucede con las **víctimas**. Las **empresas** siguen siendo objeto de victimización debido tanto al uso generalizado de las TIC en ellas, como a sus recursos económicos objeto de deseo por los cibercriminales. Pero la aparición de los cibercrímenes sociales convierten a **cualquier ciudadano que se relacione en Internet**, que contacte con otros, envíe mensajes, charle en foros o comparta sus fotos, en objeto de un ciberataque personal a su honor, intimidad, libertad sexual o similares bienes jurídicos. Y lo mismo sucede con otras **instituciones supranacionales** en relación con los cibercrímenes políticos o ideológicos cometidos con intención de desestabilizar un Estado o de difundir un determinado mensaje político aprovechando las posibilidades de comunicación masiva que ofrece el ciberespacio: la ciberguerra, el hacktivismo o el ciberterrorismo han convertido a los Estados, a los recursos públicos que ofrecen a los ciudadanos a través de Internet, en objetivo de ataques de denegación de servicios, de infecciones de *malware* u otros que pueden llegar, como ha sucedido, a paralizar la actividad de importantes instituciones de un país.

Aunque hay múltiples definiciones de cibercrimen, el aspecto esencial de todas y cada una de ellas se reduce a la cuestión de si con la definición se está adoptando una concepción amplia o restringida de la cibercriminalidad, dando cobertura en la categoría a todos o tan solo a algunos de los comportamientos criminales realizados en el ciberespacio.

Si utilizamos el término de forma amplia, podremos definir como *cibercrimen* cualquier comportamiento delictivo realizado en el ciberespacio, entendiendo además por el mismo el ámbito virtual de interacción y comunicación personal definido por el uso de las TIC, y dando cabida, por tanto, a conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio, así como también a comportamientos tradicionalmente ilícitos en los que únicamente cambia que ahora se llevan a cabo por medio de Internet.

Si, por el contrario, utilizamos el término de forma restringida, y si bien se pueden utilizar variados criterios para restringir la categoría, lo usual será acudir a la propia idea de la realización del delito por medio de las TIC.

Conforme a esto, estaremos ante un cibercrimen únicamente cuando se trate de un comportamiento delictivo realizado en el ciberespacio, cuya esencia de injusto no podría haberse dado de ninguna otra manera fuera de él.

El comportamiento de quien acosa sexualmente a un menor por Internet sería un cibercrimen bajo una concepción amplia, dado que ha sido llevado a cabo en el ciberespacio, pero podría haberse ejecutado en el "espacio real"; pero no lo sería si utilizamos un concepto restringido de cibercrimen, ya que tiene su referente fuera de él. Por el contrario, el ataque denominado "de denegación de servicios" sería un cibercrimen tanto siguiendo una concepción amplia como una restringida, puesto que tal conducta lesiva de los intereses económicos de la víctima solo puede realizarse por medio de Internet.

Desde una concepción amplia, debe entenderse por cibercrimen cualquier delito en el que las tecnologías de la información juegan un papel determinante en su concreta comisión, que es lo mismo que afirmar que lo será cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que se derivan de ello. El cibercrimen, pues, generalmente se utilizará aquí en sentido tipológico, bien como comportamiento criminal en el ciberespacio, bien como categoría que incluye a todos (o algunos de) ellos. Eso sí, para que estemos ante un cibercrimen no bastará con que se utilicen las TIC para realizar el comportamiento criminal, sino que tal uso tenga que ver con algún elemento esencial del delito.

No estamos ante un cibercrimen si, por ejemplo, se envía una carta que ha sido impresa utilizando la terminal informática e incluyendo contenidos copiados de recursos de Internet, pero sí cuando se amenaza a otro por medio del correo electrónico, o cuando el engaño constitutivo de la estafa se lleva a cabo utilizando este medio.

Por otra parte, es necesario aclarar que el término *cibercrimen* tiene una relación directa con el otro término generalmente utilizando en este ámbito, el de *cibercriminalidad*. Este no tiene sentido normativo, sino únicamente tipológico, como categoría criminológica que englobaría a todos los cibercrímenes. Se utiliza generalmente el término *cibercriminalidad* para referirse, por tanto, al fenómeno de la criminalidad en el ciberespacio, y en muchos casos, el término *cibercrimen* para situar dentro de este fenómeno a un tipo de comportamiento concreto.

Como acabamos de ver, sin embargo, hay ocasiones en que el término *cibercrimen* también se utiliza para hacer referencia a todos los comportamientos que reúnen las características tipológicas que conforman el fenómeno, esto es, como sinónimo de *cibercriminalidad*. Esto es lo que ocurre con el uso del término *cybercrime* en inglés, y también en castellano cuando se afirma, por

ejemplo, que “el cibercrimen es una amenaza para la seguridad de los Estados en la actualidad”. En ambos casos el uso es correcto y el contexto permite diferenciar uno de otro sentido.

2. Pasado y presente de la criminalidad en el ciberespacio

2.1. Evolución de la delincuencia en las TIC

Con el desarrollo de las tecnologías informáticas y la aparición de infracciones asociadas a estas se creó la categoría de delitos informáticos hacia los años setenta y que a día de hoy se sigue usando. De esta categoría formaban parte tanto los comportamientos delictivos realizados a través de procesos electrónicos, como aquellos otros delitos tradicionales que recaían bien sobre bienes que presentaban una configuración específica en la actividad informática o bien sobre nuevos objetos como el hardware y el software.

En realidad, la delincuencia informática definía un ámbito de riesgo que derivaba de la expansión social de la tecnología informática, común a muchos bienes jurídicos, cuya tutela completa por parte del legislador parecía requerir de una modificación de los tipos penales existentes para su adaptación a las nuevas realidades informáticas o de una creación de tipos distintos que respondiese a las nuevas necesidades de protección. El riesgo de la actividad informática, podría decirse, como ámbito en el que aparecían nuevos intereses, nuevas formas de comunicación social y, por todo ello, nuevos peligros para los bienes más importantes, era y es, por tanto, lo común a infracciones penales, como el fraude informático, el sabotaje o daños informáticos, el *hacking* o acceso ilícito a sistemas informáticos, la sustracción de servicios informáticos, el espionaje informático, o la piratería informática de obras del ingenio. Tipologías de conducta específica que la doctrina penal considera merecedoras de respuesta penal y sobre las que se analizaba su posible incardinación en los tipos penales tradicionales o la reforma de los mismos, e incluso la creación de tipos nuevos, para una mejor protección de los intereses dignos de tutela. Frente a otras categorías, pues, la de los delitos informáticos, incluía tipologías de conductas, y no tipos penales.

En los últimos tiempos se ha venido sustituyendo la denominación de delitos informáticos por la de cibercrimen y cibercriminalidad en referencia esta vez al término anglosajón *cybercrime*, procedente de la unión entre el prefijo *cyber-*, derivado del término *cyberspace*, y el término *crime*, como concepto que sirve para englobar la delincuencia en el espacio de comunicación abierta universal que es el ciberespacio. En inglés, parece estar imponiéndose este término frente a otros, como *computercrime*, u otros en los que se utilizan prefijos como *virtual*, *online*, *high-tech*, *digital*, *computer-related*, *Internet-related*, *electronic*, y *e-*. En la raíz de este cambio de denominación está la evolución, desde una perspectiva criminológica, de los comportamientos ilícitos en la Red y la preocupación legal en relación con ellos, concretamente, el hecho de que pasara de

ser el centro del riesgo la información del sistema informático, a serlo las redes telemáticas a las que los sistemas empezaron a estar conectados y los intereses personales y sociales que se ponen en juego en las mismas.

Así, a la primera generación de la cibercriminalidad en la que lo característico era el uso de ordenadores para la comisión de delitos, le ha sucedido una segunda época, en la que la característica central es que el delito se comete a través de Internet y una tercera en la que los delitos están absolutamente determinados por el uso de Internet y las TIC. Esto ha tenido su correlato en el ámbito legal: a partir del nuevo siglo empezaron a preocupar ya no solo la información que pudieran contener los sistemas informáticos y la afectación a la intimidad o el patrimonio que pudiera derivarse del acceso a ella, sino el ciberespacio en el que los mismos interactuaban y los crímenes que allí se producían y que podían afectar a muchos otros nuevos bienes jurídicos, como la indemnidad sexual, la dignidad personal o la propia seguridad nacional. Y todo ello ha llevado a la utilización de un término, el de *cibercrimen* que logra englobar todas las tipologías de comportamientos que deben estar y además enfatizar aquello que une a todo aquello que la conforma, que en este caso es Internet y las TIC como medio de comisión delictiva.

Al fin y al cabo, si bien Internet, la red más popular y a través de la cual se realizarán prácticamente todas estas infracciones, es en sí misma un medio informático y, por tanto, todos los ciberdelitos podrían entrar dentro de la categoría de los delitos informáticos, con la utilización del término *cibercriminalidad* se pone de manifiesto que sus implicaciones de riesgo van más allá de la utilización de tecnologías informáticas y se relacionan mucho más con el hecho de que las mismas están unidas en la actualidad a redes telemáticas, con los particulares problemas político-criminales que ello plantea en la actualidad. Además, al tener en cuenta no solo el aspecto "informacional" sino también el comunicativo de las TIC, se hace referencia a un catálogo más amplio de infracciones que incluye las que se relacionan con el (mal) uso de las comunicaciones personales entre particulares a través de redes telemáticas o con la introducción y mala utilización, de contenidos introducidos en ellas.

2.2. El cibercrimen en la actualidad ¿realidad o ficción?

Es necesario determinar las dimensiones actuales que alcanza la cibercriminalidad y al mismo tiempo conocer la amenaza real del cibercrimen, ya que se puede observar cómo los discursos frente a estos fenómenos suelen ser contradictorios.

Ejemplo

Un ejemplo de ello son los informes de la Fiscalía General del Estado, que apenas hacen mención a la cibercriminalidad y, sin embargo, paralelamente se sigue afirmando, desde muchos ámbitos, que su amenaza es creciente.

En efecto, el hecho de que comunicativamente sea muy poderosa la suma de la imagen de un ciberespacio universal y transnacional englobador de millones de conductas en un único punto, con la del crimen en sus múltiples manifes-

taciones y todo ello bajo el prisma de una sociedad del riesgo insegura como esta en la que vivimos, ha hecho que exista un temor a la cibercriminalidad que, en muchos aspectos, podría tildarse de exagerado.

Hay muchos que señalan que la amenaza de una ciberguerra es totalmente remota, pese a que existe un temor social sobre ella. En el caso del ciberterrorismo, entendido en el sentido más estricto de la utilización del ciberespacio para la realización de ataques terroristas, también ha habido una significativa exageración del alcance del fenómeno que conlleva un temor social más allá de la realidad de la amenaza. Y ese mismo temor se extiende al cibercrimen, al que se sobredimensiona no tanto en lo cuantitativo sino en lo cualitativo, como una amenaza desconocida y más allá de lo real. Así, puede sorprender que en algunas encuestas poblacionales exista un 13% de personas que estén más preocupadas por ser víctima de un cibercrimen que por serlo de un delito en el espacio físico, especialmente si lo que se mide no es tanto la probabilidad como el temor, dada la mayor gravedad general que conlleva la victimización en el espacio físico.

En realidad, el discurso sobre las amenazas cibernéticas tiende a estar dominado por el exceso de publicidad dada a algunas amenazas en perjuicio de los demás, y por las afirmaciones exageradas sobre la frecuencia y magnitud de los ataques.

La exageración la llevan a cabo en ocasiones las propias empresas de software que colaboran con los organismos públicos para evaluar la amenaza del cibercrimen y que, como interesadas en la financiación de sistemas de protección, pueden exagerar las cifras del crimen. Pero especialmente significativa es la cobertura que realizan los medios de comunicación que se centra, por ejemplo, en la presentación de informes sobre ataques a gran escala, como si cuanto mayor sea el ataque, más grande es la amenaza. Sin embargo, los ciberincidentes pueden ser menos dramáticos comunicativamente pero muchísimo más problemáticos.

Por poner un ejemplo, la realización de ataques de denegación de servicios contra las webs de la SGAE y los principales partidos políticos españoles recibe una cobertura informativa impresionante, llegando incluso a ser portada de los principales periódicos nacionales, pese a que la consecuencia de los mismos sea simplemente que unas webs con poca afluencia de usuarios no pudieron ser visitadas durante algunas horas. Mucho más grave es, sin embargo, la pérdida de información para empresas o usuarios debido a las infecciones de *malware* o el aumento de las conductas de ciberacoso escolar a menores, tal y como certifica el análisis jurisprudencial, si bien ese tipo de comportamientos nunca recibirá tal cobertura informativa.

Lo cierto es que esta forma de relato distorsiona la percepción pública de las amenazas y, por tanto, enmascara la realidad pudiendo producir el efecto contrario. En efecto, la exageración, junto a la desinformación, puede llevarnos a la minusvaloración de la amenaza del cibercrimen a partir de la creencia de que se está sobrevalorando la misma dada la aparentemente válida constatación de que tal tipo de criminalidad no ha llegado a los tribunales de forma masiva en los últimos años.

En otros términos: si llevamos más de una década avisando del riesgo que va a suponer la cibercriminalidad, hablando de ciberguerra y demás, y, sin embargo, nuestros tribunales siguen ocupándose de delitos contra la seguridad vial, de violencia de género y de tráfico de drogas esencialmente, quizás haya que convenir que tal amenaza no lo era tanto. Esta argumentación resumiría el efecto contrapuesto, la "banalización" del cibercrimen, que también es manifiestamente peligroso y además erróneo.

Es peligroso dado que se minusvaloran los riesgos existentes y, con ello, se dejan de adoptar medidas de protección así como de obtención de información para el conocimiento de las dimensiones reales de la amenaza del cibercrimen. Lo cierto es que, pese a la completa implantación de las TIC en los ámbitos empresarial y comercial, y pese a la expansión de los mismos a otros contextos sociales en los que los bienes jurídicos en juego pueden ser incluso más importantes, como es todo lo relacionado con la intercomunicación personal, aún son muchos los sistemas informáticos que no tienen sistemas de protección básicos y, lo que es más importante, sigue sin existir una educación en las TIC que, aparte de lo técnico, centre la atención en los riesgos reales existentes y en las posibilidades para detectarlos y evitarlos. **Tampoco la prioridad en el mercado de las TIC es la seguridad**: se siguen vendiendo sistemas informáticos que van a acceder inmediatamente a redes telemáticas sin antivirus o con software que tiene que ser actualizado por el usuario, que tiene que ir pagando por su seguridad mientras que la velocidad o la memoria de alta capacidad vienen incorporadas de serie.

Es sorprendente que nosotros, ciudadanos privados, pero también instituciones privadas y públicas, toleremos múltiples vulnerabilidades técnicas y sus consecuencias, como el precio a pagar por la innovación y la competencia en un mercado libre, cuando nadie toleraría un coche con un sistema de frenado que tiene que ser activado y actualizado por el propio usuario. La cuestión es que se perciben como riesgos algunos que todavía están muy lejanos y no se perciben como riesgos otros que sí son reales pero que, de alguna forma, se mantienen ocultos, debido, esencialmente, al desconocimiento de las propias TIC y a, en ocasiones, **la voluntad de ocultar tales amenazas para el éxito de su implantación social**.

Riesgos muy lejanos

La ciberguerra y otros ciberataques que afecten a la población son riesgos muy lejanos y que solo podrán producirse cuando haya una mayor dependencia de la tecnología también relacionada con los servicios y atenciones básicas.

Ahora bien, **la banalización de la cibercriminalidad solo es realmente tal si dicha forma de delincuencia existe** o, más bien, si supone una problemática creciente y digna de estudio. Al fin y al cabo, todas las expectativas de crecimiento de la cibercriminalidad, todas las previsiones sobre el cibercrimen, parecen chocar violentamente con el escasísimo impacto del ciberdelito en los tribunales de justicia. En **España**, las estadísticas oficiales también constatan un **aumento del cibercrimen**: es cierto que todavía es tenue, pero qué duda cabe de que la tipificación de nuevas figuras delictivas y, en especial, la popu-

larización de la Web 2.0 conlleva la realización de conductas delictivas en el ciberespacio que están comenzando a ser denunciadas aunque aún no tienen gran reflejo en los procesos judiciales.

Lo que cabría preguntarse en este punto es si **esa escasez de procesos judiciales por cibercrímenes se debe a la ausencia de pruebas para la imputación de los mismos o más bien a la propia ausencia de cibercrímenes**, esto es, si en realidad hay una sobredimensión de la amenaza del cibercrimen o una pobre respuesta judicial al mismo debido a factores varios, todos más o menos directamente relacionados con la novedad del fenómeno y el anquilosamiento espacio-territorial del sistema de administración de justicia. En el primer caso no habría banalización sino valoración del cibercrimen en su justa medida, como mera anécdota en el océano de la delincuencia tradicional; en el segundo caso sí la habría, y sería necesario tanto una mejora de la observación criminológica de este fenómeno para la correcta mesura del mismo como una intervención decidida en aras a su prevención.

Pues bien, la mayoría de quienes han tratado el tema de la cibercriminalidad con profundidad son de la opinión de que existe una importante **cifra negra** en materia de cibercriminalidad, esto es, que los delitos que se cometen son muchos más que los que aparecen en las estadísticas oficiales al ser enjuiciados y condenados como tales, hasta el punto de que hay quien ha señalado que la cibercriminalidad es la forma de delincuencia más infradenunciada de toda la existente.

Lo entiende así la doctrina, que argumenta si en todo tipo de delincuencia hay una cifra negra, esta debe ser mayor en el caso de la cibercriminalidad. Pero además, hay datos, y no meras hipótesis, que certificarían que con la cibercriminalidad ocurriría algo similar a lo que sucede con los icebergs, que lo que se percibe o visualiza es tan solo un porcentaje ínfimo en comparación con lo que realmente existe.

Estudios sobre cibercrimen

Variados estudios insisten en que el cibercrimen está en crecimiento desde hace más de 10 años, siendo múltiples los ataques recibidos diariamente en nuestro país, algunos de los cuales no son propiamente delictivos (el caso del envío de *spam*) pero otros sí, como los daños, el acceso informático ilícito, las injurias y las calumnias, los ataques de DoS, etc. Así lo ponen de manifiesto numerosos informes independientes de algunas importantes empresas de seguridad, como Javelin, que en su estudio sobre fraude de identidad, detectó un incremento de un 12% de víctimas de esta modalidad de ciberdelito, o el informe encargado a PricewaterhouseCoopers, en el que pone de manifiesto que, mientras que en un estudio del 2008 sobre brechas de seguridad en las empresas, el 21% de los encuestados declararon haber sido infectados por virus u otro software malicioso, en el 2010 esta cifra ascendió al 61%.

Este mismo informe destaca otro dato llamativo: únicamente el 16% de las empresas encuestadas esperan un número menor de ataques en el año próximo. Otros informes publicados por instituciones gubernamentales o auspiciadas por los gobiernos, como el Internet CrimeComplaintCenter (IC3), constatan que las denuncias por cibercrímenes pasaron de 16.838 en el 2000 a 303.809 en el 2010. También parecen certificar esta tendencia de incremento del cibercrimen otro tipo de estudios contra los que no podrá argumentarse, como se hace con los realizados por empresas de software, la falta de imparcia-

lidad. Me refiero a las investigaciones sobre victimización en el ciberespacio que abarcan muchos tipos de ciberdelitos, si bien se ocupan más especialmente de las infecciones de *malware*, el *phishing*, el *cyberbullying*, el *online grooming* o el *cyberstalking*. Todas las investigaciones reflejan un aumento de la criminalidad, si bien debe reprocharse a las mismas que ninguna de ellas cuestiona las razones por la falta de denuncia de estos delitos.

La criminalidad en el ciberespacio, por tanto, estaría aumentando y seguirá haciéndolo mientras vayan ampliándose los ámbitos de comunicación entre personas en Internet. No debe exagerarse la amenaza, pues si bien es cierto que los ataques han ido aumentando a lo largo de los años, también lo es que los procedimientos en seguridad también han ido mejorando, y conforme vayan surgiendo ámbitos de criminalidad, irán desarrollándose estrategias preventivas que limitarán los efectos de los mismos. Tampoco estamos en condiciones de cuantificar la cifra negra sin ningún tipo de apoyo empírico. Por el contrario, sería recomendable la realización de investigaciones criminológicas empíricas profundas que sirvieran para reflejar las dimensiones reales del fenómeno bien a través del estudio de las denuncias archivadas o bien a través de estudios de victimización entre la población. Sería una forma de salvar los problemas que conlleva el análisis de únicamente los datos oficiales y su imposibilidad para cuantificar el alcance real del fenómeno.

Cuantificar cualquier tipo de delito es una tarea difícil y complicada, pero lo es especialmente en el ámbito de la cibercriminalidad por dos grandes motivos: por un lado, por la falta de denuncias de este tipo de delito y por otro lado, por las características que presenta que dificultan los procesos judiciales aun cuando haya existido denuncia.

Comenzando por estos últimos, no debe ser ningún descubrimiento la afirmación de que los procesos judiciales contra gran parte de los cibercrímenes pueden tener muchas más complicaciones generales que los que se inician contra crímenes en el espacio físico. La razón principal es que cuando existe una denuncia, generalmente en estos casos no dirigida contra alguien en concreto sino reflejando una concreta victimización, los primeros pasos de la investigación policial se dirigen hacia la determinación de los autores y hay varios motivos por los que esta puede ser especialmente complicada para estos delitos:

Ejemplos

Ejemplos de denuncias sin determinación de autor son: un dinero defraudado por un usuario indeterminado, un daño en el sistema por un virus, una calumnia en una página web, etc.

- **Anonimato en la red**. En primer lugar por las propias características, favorecedoras del anonimato, del ciberespacio: aunque el ciberdelito es cometido por alguien en concreto, en Internet solo se muestra una representación virtual del autor (la dirección IP) que puede ser concretada, pero a la que después hay que atribuir la concreta persona física que está detrás de la acción; y eso ya es más complicado, pues exige, primero, la colaboración de las empresas proveedoras de servicios y, después, la investigación del titular del sistema informático desde el que se ha realizado el ataque y la concreción, de entre todos los usuarios del mismo, del que en particular lo ha ejecutado.

- **Transnacionalidad del delito**. En segundo lugar, y relacionado con lo primero, la determinación judicial de las personas autoras del cibercrimen suele complicarse debido a la transnacionalidad del delito. Ya no se trata, como en la criminalidad física, de que el delincuente haya podido trasladarse a otro país tras cometer el delito y haya que solicitar su entrega a las autoridades judiciales españolas, sino de que el delito haya sido directamente cometido desde el extranjero, con lo que los procesos para la identificación del cibercriminal requieren de la no siempre sencilla tarea de lograr colaboración de otros Estados.

Colaboración de Estados contra el cibercrimen

Al fin y al cabo no es lo mismo solicitar la extradición de una persona concreta por la comisión de un determinado delito, que solicitar a un Estado extranjero que investigue quién puede ser el sujeto que se halla detrás de una concreta IP, que presuntamente puede haber perpetrado una infracción penal. La práctica judicial demuestra que la fiscalía suele cesar en el intento de identificación cuando la IP se encuentra en Rusia o países similares relacionados con mafias de cibercriminales.

El segundo grupo de motivos tiene que ver con la falta de denuncia de la víctima del cibercrimen. Las razones son diversas y, probablemente, deban ser valoradas de distinta manera para según qué delitos. Al fin y al cabo la cibercriminalidad no viene a ser más que toda la criminalidad en el ciberespacio y la cifra negra no será idéntica para todas y cada una de las tipologías de delitos. Pero veamos estas razones:

1) Conducta criminal inadvertida. En primer lugar, en muchas ocasiones la conducta criminal pasa directamente inadvertida, de modo que no es denunciada aunque haya sido consumada e incluso se hayan logrado los efectos criminales con la misma. Esto puede ocurrir con otros delitos cometidos en el espacio físico, pero de forma muy excepcional, dado que en él la visualidad de los efectos y consecuencias de las acciones es mayor.

Así puede ocurrir, por ejemplo, con las infecciones de virus maliciosos que produzcan daños en los sistemas informáticos, también con injurias y calumnias colgadas en sitios web y que sean percibidas por otros sujetos pero no por la víctima de las mismas, pero especialmente sucederá en el caso del *hacking* o acceso informático ilícito, conducta consistente en la mera intromisión en el sistema informático ajeno, considerada como delictiva a partir de la reforma del CP del 2010, y que en muchos casos, prácticamente en la mayoría, no será percibida por el titular del sistema. Incluso puede suceder que la víctima no perciba el ataque en el caso de las defraudaciones en el ciberespacio. Así, el intento de descubrir la comisión de fraudes informáticos puede implicar enormes costes debido a las comprobaciones minuciosas, etc., que pueden suponer mayores pérdidas que el propio perjuicio causado.

2) Percepción tardía del ataque. En otros casos lo que sucede es que la víctima sí se percibe del ataque pero lo hace tarde, cuando el mismo ha prescrito o cuando ya valora como absurdo el presentar demanda judicial dado que habrá pocas posibilidades de que la policía vaya a identificar, detener y procesar a los

delincuentes. Esto será habitual en los ciberfraudes, especialmente en relación con los bancarios, dado que puede suceder que la víctima se aperciba de que le falta dinero en su cuenta o de que le han imputado un gasto que no es propio después de que suceda. Desde luego esto es lo que ocurrirá en el *hacking* en aquellos casos en los que la víctima lo perciba, pues es prácticamente imposible que esta conducta delictiva sea visualizada por la víctima en el mismo momento en que acontece. También ocurrirá en las infecciones de virus con resultado de daños, que a veces son percibidas por el sujeto pero no en otros casos, teniendo en cuenta, además, que el efecto del virus puede tener lugar en un determinado momento pero la infección puede haberse producido en otro muy anterior.

3) Falta de percepción como conducta delictiva. Otro factor a tener en cuenta como motivo de la cifra negra de la cibercriminalidad es que la propia víctima, que sí se percibe del ciberataque, ni siquiera valora el mismo como una conducta delictiva, por lo que no procede a denunciarlo. Esto ocurre especialmente en el caso de las infecciones de virus, de las que muchos desconocen que generalmente podría ser constitutiva de delito conforme a nuestro Código penal; pero también ocurre con gran parte del envío de *spam* que contiene mensajes de *scam* o *phishing*, que puede ser considerado como tentativa de estafa en algunos casos si no es utilización ilícita fraudulenta de la imagen de una empresa o estafa punible en el caso de que se cree una web para el *pharming* y aunque no haya pérdida patrimonial; desde luego sucede con el *hacking* o acceso informático ilícito que todavía no tiene la valoración social de comportamiento delictivo; e incluso puede ocurrir con los pequeños fraudes, con aquellos que producen una pérdida patrimonial tan ínfima para la víctima que puede pensar que ni siquiera resultan delictivos. Sin embargo, los criminales cibernéticos aprovechan esa subestimación crónica de los delitos cibernéticos, puesto que una pérdida de 30 libras o euros para una persona puede significar una ganancia mínima de 3.000 al infractor, ya que las estafas se dirigen a cientos de miles de personas en línea.

4) Falta de confianza en la justicia. En otras ocasiones la razón de la denuncia es precisamente la falta de confianza en las autoridades judiciales para la averiguación de los hechos, generalmente por la convicción de la dificultad que conllevará la identificación de los responsables. Esto ocurriría especialmente en los cibercrímenes económicos, particularmente en aquellos en los que las pérdidas no sean dramáticas, y en los que la víctima preferirá la pérdida al propio gasto judicial debido a las dudas que le plantea el éxito del mismo. Al fin y al cabo todos los problemas de identificación y la cuestión de la transnacionalidad del ataque no son ajenos a la víctima, que los tendrá en cuenta a la hora de iniciar un proceso judicial incierto. Por el contrario, cuando la víctima constate que el ciberataque sea realizado por alguien conocido (aunque no esté identificado) o de nacionalidad propia, es más posible entonces que se denuncie con la esperanza de que se pueda identificar al agresor. Y lo mismo

Cifra negra de empresas

Es conveniente hacer mención a la cifra negra que generan algunas empresas, especialmente en el caso de los bancos, que prefieren asumir las pérdidas provocadas por ciberataques e indemnizar a sus clientes que hacer pública la vulnerabilidad de sus sistemas mediante la denuncia, dado que el coste provocado por la pérdida de clientes por su desconfianza puede ser superior al generado por la conducta criminal.

sucederá cuando la denuncia trate de borrar los efectos visibles del delito (en el caso de las injurias, calumnias o atentados a la dignidad de una persona por medio de una publicación en una página web o similar).

3. Fenomenología de los ataques en el ciberespacio

La realidad criminológica nos enseña, en primer lugar, que el ciberespacio se ha convertido en algunos casos en un ámbito auténticamente generador de nuevas conductas delictivas cuando las TIC son la única forma de realización de la infracción; en otros, en cambio, lo que ha supuesto la irrupción del "nuevo espacio" ha sido la aparición no de nuevas formas puras de delincuencia, sino de réplicas de otras ya existentes que cambian sus caracteres básicos al llevarse a cabo en el nuevo ámbito virtual; y, por último, el ciberespacio de sistemas conectados en redes también ha potenciado la importancia de los contenidos al facilitar enormemente su difusión global y ha generado, con ello, todo un conjunto de conductas en las que la ilicitud no estriba más que en la difusión o acceso a determinadas formas de información ilícita o socialmente considerada peligrosa.

Así, podemos distinguir tres bloques de conductas delictivas en el ciberespacio atendiendo al papel que desempeñan las TIC en su desarrollo denominados: ciberataques puros, ciberataques réplica y ciberataques de contenido.

3.1. Ciberataques puros

Son categorizados como **ciberataques puros** aquellos que únicamente pueden ocurrir en el ciberespacio.

Se trata de un nuevo conjunto de infracciones completamente nuevas que surgen del desarrollo de las TIC.

3.1.1. El *hacking*

Se puede definir ***hacking*** como 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.

El *hacking*, en este sentido amplio, es la actividad de los *hackers* consistente en la superación de cualquier barrera informática, bien sea para el acceso a un sistema, o bien para la configuración de una determinada programación funcional, etc. En sentido estricto, en cambio, es equivalente a otro término generalmente utilizado, el *intrusismo informático*, que pone el acento en que tal conducta conlleva la violación de una esfera de exclusividad reservada al titular del sistema, haya o no haya en ella información privada o confidencial.

Hacking y cracking

Hay que distinguir entre el *hacking* blanco, en el que el propósito del *hacker* es simplemente el de acceder al sistema o a sus datos e información, pero sin ningún propósito de sabotaje o utilización posterior de la información, y el *cracking*, en la que el *cracker* accede al sistema para realizar cualquier tipo de daño al sistema, a los elementos que este contiene o a su titular al adquirir, eliminar o modificar información del mismo.

El *hacking* se puede llevar a cabo de muy distintas formas, si bien, generalmente, el modo de proceder consiste en la búsqueda de vulnerabilidades en los sistemas informáticos derivadas de una deficiente programación, de un cambio tecnológico que hace obsoleta la formulación binaria existente, o incluso, aprovechando las puertas que involuntariamente el propio titular del sistema informático o cualquiera de los múltiples sujetos que interaccionan con él pueden haber dejado abiertas. En todo caso, el *hacking* es siempre, por su propia naturaleza, un acceso remoto, esto es, realizado a distancia por el sujeto que, normalmente a través de Internet, se entromete en un sistema sin tener contacto físico con él.

No es *hacking* propiamente dicho el acceso directo en la propia terminal y no autorizado a un sistema informático. Este comportamiento, usual en el ámbito familiar o laboral y generalmente realizado para obtener información sensible que puede estar contenida en el sistema, no puede considerarse *hacking* a efectos criminológicos, dado que modifica el ámbito de riesgo que caracteriza al más usual, que es el que se ejecuta en el ciberespacio; aunque es evidente que tal forma de *hacking* que no nos interesa aquí sí que constituirá un acceso ilícito a un sistema informático, tal y como describen la conducta la mayor parte de los códigos penales.

Tampoco se puede considera *hacking* cuando el sujeto utiliza determinados programas informáticos para extraer información del sistema, pero sin que pueda decirse que el *hacker* ha tenido ningún tipo de acceso real al sistema.

Es decir, que independientemente de que haya habido o no acceso a los datos, lo relevante para que podamos decir que el tipo de ciberataque que se ha cometido es *hacking*, es que haya existido una entrada no autorizada en el sistema ajeno, no bastando con que debido a la introducción de algún *malware* u otro tipo de rutina, sea el propio sistema el que envíe información al *hacker*.

3.1.2. Infecciones de *malware* y otras formas de sabotaje cibernético

Uno de los principales riesgos, muchos de ellos asumidos, que sufren tanto empresas como particulares a la hora de adentrase en el ciberespacio es sufrir el denominado "sabotaje informático", que incluye tanto el envío de virus informático que aprovecha la inmensidad del ciberespacio para multiplicarse y acceder a miles de terminales, como cualesquiera otras formas de destrucción de archivos o datos de terminales concretos y determinados, con fines industriales o de daño individual.

Relacionado con el sabotaje informático encontramos el "sabotaje cibernético", denominado por otros autores como cibervandalismo, como son ataques a los sistemas informáticos, a su información, a las redes de comunicación o a los servicios de Internet. El sabotaje cibernético puede afectar bien a los propios sistemas informáticos y demás elementos de hardware que lo conforman y que son evaluables económicamente; bien a la información contenida en los citado sistemas y que puede tener un valor económico o personal, en el sentido de sentimental y relacionado con su propia dignidad, para el sujeto pasivo; o bien a la propia funcionalidad del sistema informático en el marco de la actividad económica de que se trate.

La forma más popular de sabotaje es el envío de virus destructivos que debe ser considerado como una forma de distribución de *malware* o software malicioso destinado a dañar, controlar o modificar un sistema informático.

Desde su aparición en los años setenta, los virus se han acabado convirtiendo en un fenómeno casi natural en el ciberespacio, si bien en los últimos años, conforme la interconexión de sistemas en red se ha ido popularizando, ha habido un crecimiento exponencial, pasando de los más de 2.000 virus que se calculaban en el 2000 hasta los 137.000 en el 2003 y calculándose en la actualidad que son millones los ordenadores infectados por todo tipo de *malware*.

Tipos de *malware*

Dentro del *malware* hay distintas modalidades de software con objetivos muy distintos, desde los que tratan de destruir el sistema o su información como los virus y algunos tipos de gusanos (*worms*) o troyanos (*trojans*), pasando por los que permiten el acceso remoto del sistema informático a través de la Red, como los *botnets* o los *rootkits*, que esconden el software malicioso o permiten el control del sistema, hasta los *keystrokeloggers* o *spyware*, que capturan información de los sistemas informáticos.

Hoy el envío de *malware* para la infección de un sistema suele ser un paso rutinario más dentro de una dinámica compleja definida para lograr objetivos generalmente consistentes en la defraudación económica. En otras palabras, el envío de *malware* en la actualidad no es más que un comportamiento inicial necesario para la realización del ataque final consistente en un ataque al patrimonio o a la intimidad de los usuarios.

De hecho, los últimos estudios demuestran que ese es ya el principal tipo de virus existente: troyanos, gusanos, *backdoors* y demás, todos los cuales tratan de permitir la posterior entrada en el ordenador o su control futuro, creando

vulnerabilidades que sean aprovechadas posteriormente por los *hackers*. Los usos que se le dan al sistema infectado luego pueden ser variados: desde constituir el propio objeto del ataque al abrir el *malware* una puerta para el *hacking*, pasando por su utilización para que el sistema envíe información para su propia victimización, hasta su uso como terminal desde la que realizar futuros envíos de *malware* para la infección de otras terminales.

Ataques de *botnet*

Esto ocurre especialmente en el caso de los ataques de *botnet*, en los que se infecta con *backdoors* un conjunto de sistemas (*bots*) que pasan a ser controlados por un único usuario (*botmaster*). Un *botnet* puede ser instruido por su controlador para realizar funciones de muy diverso tipo, entre las que destacan los ataques de denegación de servicios que después analizaremos, situar en el sistema el *hosting* o alojamiento de webs maliciosas dedicadas al blanqueo de dinero, la realización de fraudes por medio de *phishing* o la distribución de pornografía infantil, la realización de actividades de escaneo de sistemas y webs vulnerables para la realización de otras conductas delictivas, o el envío de gran número de correos electrónicos no solicitados (*spam*).

Otra forma de sabotaje pero que no se incluiría en el denominado grupo de cibernéticos sería el sabotaje de *insiders*, que se trata de la conducta que lleva a cabo un trabajador o extrabajador pero que sigue teniendo acceso a la empresa o institución y se aprovecha de su posición para dañar, destruir o distribuir el mayor número posible de información.

Los ataques de denegación de servicios o DoS (*denial of services*) es otra forma de sabotaje que consiste en utilizar técnicas para cargar los recursos del ordenador objetivo y producir la negación de acceso del servidor a otros sistemas informáticos.

Se suele llevar a cabo mediante la saturación del sistema por medio de envío masivo de información que produce una sobrecarga de los recursos del sistema y la consiguiente inutilización del servicio con los daños económicos que eso conlleva, y se convierte en Distributed DoS (DDoS) cuando se lleva a cabo por medio de muchas terminales, bien gracias una infección *botnet* o bien a la colaboración de múltiples usuarios que realizan a la vez el ataque.

Ataques DoS

Este tipo de ataques se popularizaron en el año 2000 cuando se produjeron los ataques a páginas web comerciales muy conocidas (Yahoo, Ebay, Etrade, etc.), cuyo objetivo era dañar la reputación de las empresas que ofrecen servicios en Internet impidiendo el correcto funcionamiento de sus actividades, pero en los últimos años, también se ha utilizado este tipo de ataques con finalidades de hacktivismo político, esto es, de difusión de mensajes de protesta en Internet generalmente dirigidos contra organismos o Estados.

El *spam* sería el siguiente ataque destacable a las terminales, en este caso, a los sistemas informáticos consistentes en ordenadores y llevado a cabo a través del correo electrónico.

El *spam* es un *e-mail* no solicitado que suele enviarse a un gran número de direcciones electrónicas bien a través de una dirección electrónica de las ofrecidas por los servicios de correo gratuito, como por ejemplo Hotmail, o bien desde un sistema informático infectado, convertido en *botnet* y utilizado por el *spammer*, que adquiere las direcciones de correo bien "hackeando" sistemas informáticos o bien utilizando *spyware* u otros sistemas de búsqueda de direcciones electrónicas a través de la Red.

El *spam* tiene diversas finalidades, que van desde el envío ilícito de publicidad hasta el intento de infección del sistema por medio de *malware*, pasando por el intento de *phishing*. En todo caso, el envío de *spam*, así como la previa recopilación de la dirección electrónica, puede considerarse ya un ataque a la terminal informática.

Pese a que el principal riesgo que conlleva la recepción de correos *spam* estriba en la posibilidad de ser infectado por algún tipo de *malware* que sea posteriormente utilizado para defraudar a la víctima, tampoco debe despreciarse la enorme gravedad que supone el mero hecho de recibir correos indeseados, aun en el caso de no ser infectado por ellos.

Costes económicos del *spam*

Según un estudio sobre los costes económicos del *spam*, este presenta un coste para las empresas de EE. UU. de casi 9 millones de dólares por año, 2,5 billones para las de Europa y 500 millones para los prestadores de servicios. Estas macrocifras aún llaman más la atención cuando se concretan en el coste para las empresas que supone la limpieza de *spam*: de unos 600 a unos 1.000 $ de pérdidas por año en productividad por usuario, con una media de 874 $ de pérdida de rendimiento por persona debido a los 10 correos de *spam* diarios recibidos por cuenta de correo en el ámbito de la empresa.

3.1.3. Ocupación o uso de redes sin autorización

También consideramos como ciberataque puro el ataque directo a las redes, de forma concreta, a la utilización de un terminal de comunicación titularidad de otro sujeto, y que comienza a ser común ya no solo en redes de comunicación de televisión por cable, sino también en las propias redes telemáticas, como Internet, debido a la popularización del sistema *Wifi* y a la facilidad de la conexión a estas redes. Por último, el otro elemento de las TIC, los servicios, concretamente aquellos generales de comunicación y difusión de contenidos de telecomunicación, también se ven en la actualidad gravemente afectados por toda una serie de comportamientos de piratería de señales de emisión radiofónica, televisiva y de Internet, que bien mediante la creación de software específico que se instala en un sistema informático para que con la conexión a la antena ya se pueda "piratear la señal digital de que se trate", o bien mediante otros sistemas más arcaicos, como la duplicación de claves o similares, ponen en serio peligro los intereses comerciales de quienes han aprovechado la mundialización de Internet para crear un nuevo modelo de negocio basado en la comunicación digital de contenidos.

3.1.4. *Antisocial networks*

Para finalizar con los ciberataques puros, hay que hacer referencia a una de las formas más novedosas de conducta criminal en el ciberespacio que algunos autores han bautizado con el nombre de *antisocial networks* o redes sociales antisociales.

El ***antisocial networks*** es un comportamiento preparatorio de las posteriores conductas criminales, que trata de asegurarlas y facilitarlas, y consiste en la manipulación de redes sociales o de grupos de ellas con finalidad de utilizarlas posteriormente para el fraude o para cualquier otro tipo de ciberdelitos.

Al fin y al cabo, y como han señalado algunos autores, las redes sociales tienen algunas propiedades intrínsecas que las hacen ideales para ser aprovechadas por adversarios o por quienes quieren utilizarlas para defraudar a otros: en primer lugar, tienen una gran, y ampliamente distribuida, base de usuarios; en segundo lugar, está formada por grupos de usuarios que comparten similares intereses sociales, lo cual conlleva un desarrollo de la confianza entre ellos y el uso de recursos compartidos; en tercer lugar, la plataforma permite a los usuarios la instalación de aplicaciones pensadas contra el fraude y similares cibercrímenes. Todas estas características dan la oportunidad a los cibercriminales de manipular las cuentas de Internet de los usuarios o a ellos mismos directamente y llevarlos a ejecutar conductas antisociales contra el resto de personas en el ciberespacio sin el consentimiento de que lo están llevando a cabo.

3.2. Ciberataques réplica

En esta categoría se incluyen todos aquellos delitos en los que el ciberespacio se ha convertido en un nuevo medio desde el que realizar delitos tradicionales.

En el caso de los **ciberataques réplica**, el ataque no se realiza a un terminal informático, ni tampoco es el contenido el objeto de la ilicitud, sino que la Red es el nuevo medio a través del cual se comete una infracción que utilizaba anteriormente otros medios para llevarse a cabo. Se trata, por tanto, de réplicas, llevadas a cabo en el ciberespacio, de crímenes que ya se realizaban, de otro modo, en el espacio físico.

Los especiales caracteres de este nuevo ámbito de realización criminal que es el ciberespacio confieren a la conducta una singularidad tal, que la hacen aparecer prácticamente como una conducta nueva.

3.2.1. Los ciberfraudes

En los **ciberfraudes** entrarían, en primer lugar, los fraudes de Internet, en los que las redes telemáticas se convierten en el instrumento mediante el cual lograr un beneficio patrimonial derivado de un perjuicio patrimonial a una víctima.

Son muchas las formas en las que se puede lograr acceder al patrimonio de terceros, utilizando las múltiples modalidades de relación comercial existentes en el ciberespacio, así como las propias debilidades de seguridad de los sistemas informáticos que dan directamente acceso al patrimonio o indirectamente a él, al contener las claves o datos bancarios de los usuarios.

Ejemplos de ciberfraudes

Así, algunas de las más conocidas son los distintos fraudes de tarjetas de crédito, los fraudes de cheques, las estafas de inversión, las estafas piramidales realizadas a través de Internet, las conocidas estafas de la lotería, las ventas *online* defraudadoras en las que no se envía el producto comprado (o se envía con otras características, como en la acción fraude) o no se paga el recibido o se cobran servicios no establecidos previamente, las estafas de inversión en las que se cobran gastos no previstos o no se explican pérdidas inesperadas, así como los ataques de *scam* en los que se prometen cantidades importantes de dinero a cambio de pequeñas transferencias relacionadas con ofertas de trabajo, loterías, premios u otros, entre una variedad de fraudes que van transformándose (o adaptándose, conforme a la terminología que utilizaremos más tarde) constantemente.

Fraude en las subastas

Uno de los fraudes más comunes y que se mantiene como usual en los últimos años es el denominado *auction fraud*, o fraude en las subastas, consistente en la tergiversación de un producto o su no entrega conforme a lo pactado en los sistemas de subasta *online* tipo eBay.

Dentro de este grupo también quedarían incluidos el envío de correos electrónicos denominados *scam*, que no son más que las tradicionales estafas en las que, en este caso, la forma de comunicación entre las personas para la realización del engaño es Internet, bien el correo electrónico o bien el uso de las redes sociales. Es esta más bien una categoría genérica que podría englobar a casi todos los fraudes, si bien se suele utilizar como referencia de los más burdos de ellos, aquellos en los que el engaño es poco elaborado y en los que el error de la víctima puede ir más allá de lo común.

Cartas nigerianas

En este caso podríamos integrar el conocido caso de las "cartas nigerianas", estafa clásica semejante al famoso "timo de la estampita", en el que el engaño se logra explotando el ánimo de lucro de la víctima, así como muchas otras que han surgido posteriormente, como la de la lotería, la del trabajo desde casa, etc., siempre caracterizadas por tratar de interesar a la víctima o ganarse su confianza para que sea él quien finalmente realice el acto de disposición patrimonial que le perjudica. En este tipo de estafas, el factor humano, más concretamente su vulnerabilidad, constituye el elemento esencial para que el engaño tenga éxito.

El ***phishing*** es otra modalidad de ciberfraude definido como el 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.

El uso de la ingeniería social se produce cuando se utiliza la identidad personal de otro (*spoofing*) mediante la falsificación de sitios web, para conducir a los consumidores a que confíen en la veracidad del mensaje y divulguen los datos objetivo. Cuando se utilizan otros artificios técnicos, como por ejemplo, redireccionar un nombre de dominio de una página web verdadera situada en la memoria caché del sujeto o bien a una página web falsa, o se monitoriza la intervención del sujeto en la verdadera, se utiliza el término de *pharming*.

3.2.2. *Identity theft* y cibersuplantación de identidad

El robo de identidad o *identity theft* sería el siguiente grupo de conductas a tratar que, no siendo nuevas, adquieren una nueva dimensión en el ciberespacio.

El **robo de identidad** podría definirse como la adquisición por parte de un sujeto, global o parcialmente, de los datos de otro sujeto para su posterior uso como si le pertenecieran a él, aunque generalmente cuando se habla de *identity theft* se utiliza ya presuponiendo el futuro uso delictivo de la suplantación; esto es, como la utilización o explicación de los datos de identificación personal u otro tipo de información de la persona como el nombre, el número de DNI, etc., para cometer fraude o participar en otras actividades ilegales.

Aunque la suplantación de personalidades también se produce fuera del mundo virtual, en el ciberespacio resulta más sencillo de ejecutar y potencialmente mucho más peligroso porque, en primer lugar, la eliminación de la inmediatez física y las posibilidades técnicas para la obtención de información personal y para la simulación hacen que sea posible tanto obtener datos privados necesarios para suplantar a la persona como actuar directamente haciéndose pasar por ella y, en segundo lugar, son múltiples las personas conectadas en el ciberespacio que realizan operaciones financieras y de cualquier otro tipo. En definitiva, que Internet no solo es el medio a través del cual se puede realizar el *identity theft*, sino que es la razón del gran riesgo que conlleva el mismo en la actualidad, al haber aumentado significativamente en el ciberespacio la necesidad de utilizar los datos personales para realizar transacciones, operaciones o acciones, no siempre comerciales, por parte de los titulares de esa identidad.

Hay que tener en cuenta además, que si bien el robo de identidad suele realizarse generalmente como primer paso para la ejecución posterior de algún tipo de fraude informático, generalmente el *phishing*, dada la importancia actual de la denominada identidad digital, tal suplantación no solo encierra un riesgo para el patrimonio de las personas, sino también para muchos otros bienes jurídicos. El robo de identidad en Internet se puede llevar a cabo de muchas formas, desde las más sencillas en las que se acude a la ingeniería social para la suplantación de la personalidad, hasta las más complejas en las que **se utiliza la ingeniería informática para lograr con los distintos mecanismos exis-**

tentes la identificación de los sistemas que actúan en el ciberespacio. En estas últimas, es donde debe situarse el *spoofing* que, a su vez, también puede ser poco o muy elaborado.

En la actualidad, se diferencian por lo menos **cinco formas de *spoofing***:

- **IP *spoofing***, en el que mediante la utilización de programas específicamente destinados a ello, se sustituye la dirección IP original por otra.

- **ARP *spoofing***, en el que se falsean las denominadas tablas ARP de una víctima para llevar a su sistema MAC a que envíe los paquetes al *host* atacante en vez de a su destino.

- **DNS *spoofing***, en el que lo que se modifica es el nombre de dominio-IP de un servidor DNS, aprovechando alguna vulnerabilidad, lo cual se suele utilizar para el *pharming*, en el que el sujeto pone la dirección web de una entidad bancaria oficial y se le remite a una web falsa.

- **Web *spoofing***, quizás el más común de todos estos ataques, en el que a través de un link u otras formas de engaño, se hace pasar una página web, imitada y albergada en otro servidor, por la real, por medio de un código que solicita la información requerida por el sistema víctima a cada servidor original y remite a la web falsa.

- ***Mail spoofing,*** consistente en la suplantación de la dirección de correo electrónico de otras personas o entidades, utilizada generalmente para enviar *spam* o como comienzo de la dinámica de ataque del *phishing*.

3.2.3. El ciberespionaje

El espionaje informático o *snooping* es otra modalidad de cibercriminalidad en la que las redes son el nuevo instrumento desde el que se debe interceptar la comunicación. Se puede realizar por un *insider* que aprovecha su situación en la empresa o con la persona de confianza para dañarla, por un *hacker* que accede directamente al sistema informático, o bien por medio de todo un conjunto de software cuya finalidad primera es la obtención de datos de muy diverso tipo y con diferentes objetivos últimos. Este es el software que se denomina *spyware* y que bien puede ser enviado por correo electrónico por el atacante, o bien puede ser descargado inconscientemente por la víctima al descargar algún otro tipo de software.

El ***spyware*** es un software que se instala en un sistema informático y que recopila determinada información de este, que después envía a otro sistema. Por medio del *spyware* se puede acceder a información personal o a secretos de empresa obtenidos en correos electrónicos y otro tipo de mensajes, pero generalmente este tipo de software lo que recaba es un conjunto de datos, que son necesarios para realizar posteriores ataques a la intimidad o al patrimonio del sujeto, como sus claves informáticas o bancarias, la dirección IP, los números de teléfono, etc.

Especial importancia tiene dentro del *spyware* el uso de programas *sniffers* y *keylogger*, que pretenden, en última instancia, la captación de información bien para el espionaje industrial, bien para su posterior uso en ataques de *spam*, *phishing*, *botnet*, etc.

Los ***sniffer*** son programas de captura de tramas de información que no están destinadas a él.

En realidad, lo que hacen los *packet sniffer* es capturar todo el tráfico que viaja de una determinada forma o con unas determinadas características por la Red, y eso puede ser utilizado con la finalidad de detectar fallos en redes o sistemas o incluso *hackers*, o bien con finalidad maliciosa, bien para capturar de forma automática contraseñas de sistemas informáticos o nombres de usuario de la Red para el posterior acceso informático o envío de *spam*, respectivamente, bien para tratar de interceptar mensajes de correo electrónico o espiar conversaciones de chat, etc.

En cuanto a los ***keylogger***, se trata de un tipo de hardware o software, el que más interesará aquí, que se dedica a registrar las pulsaciones que se realizan en el teclado con la finalidad de memorizarlas y posteriormente enviarlas al sujeto, que posteriormente las utilizará para acceder a la información o al patrimonio de la víctima.

Aunque en el ámbito de la empresa o incluso en las relaciones personales, en la misma familia, puede comenzar a darse el uso de hardware *keylogger*, lo que aquí nos interesa más son aquellos casos en los que, a través de un troyano o una *backdoor*, se instala en un sistema informático ajeno un software que, gracias al registro de pulsaciones, consigue que el cibercriminal acceda a contraseñas del sistema o a claves bancarias entre otras informaciones.

Por último, también se podrían citar aquí cualesquiera otras formas de*DNS snooping* o captación de datos de otro sistema sin modificación de los mismos y sin autorización, como por ejemplo el denominado *DNS snooping*, en el que se obtienen nombres de dominio resueltos por un servidor DNS.

Cookies

Finalmente, algunos autores sitúan dentro del *spyware*, aunque como conductas invasoras de la intimidad con menor lesividad, las denominadas *cookies*, archivos que almacenan información del usuario en su propio sistema y que sirven para que los sitios web identifiquen al visitante. La tecnología de las *cookies* permite que una página web, por defecto, inserte con disimulo su propio identificador en el terminal de forma permanente, para poder rastrear así el comportamiento del individuo en Internet.

3.2.4. Ciberblanqueo de capitales y ciberextorsión

En otro orden, la anteriormente comentada relación entre el crimen organizado y la cibercriminalidad hace que en la actualidad se utilice el ciberespacio y sus diferentes servicios para el blanqueo de capitales, derivados, generalmente, de las actividades cibercriminales de dichos grupos. Aunque existen muy diversas técnicas para el blanqueo del dinero virtual, las más comunes son en la actualidad el **uso de mulas** para el envío de dinero y el logro de divisas por medio de los juegos *online*. Cuando se habla de las mulas, especialmente en el ámbito del *phishing*, se hace referencia a los **usuarios de Internet que tienen (o abren) cuentas bancarias**, y que son reclutados vía web bajo la apariencia de un contrato de trabajo realizado desde casa, y que consiste en la recepción en sus cuentas bancarias de dinero y su envío, por medio, generalmente, de sistemas como el de Western Union, o también por **transferencia bancaria,** a las cuentas corrientes de los **cibercriminales** a cambio de una pequeña **comisión**. En cuanto a las webs de juego *online*, las mismas suponen la creación de una economía virtual en las que se intercambia el dinero real por dinero virtual para participar en los juegos. Esto es aprovechado por las organizaciones criminales para, primero, intercambiar el dinero real por dinero virtual y después, volverlo a recuperar como real, complicando la perseguibilidad de los bienes ilícitos.

También en relación con las bandas organizadas tiene que ver el siguiente comportamiento criminal que únicamente cambia en cuanto a que el ciberespacio es el nuevo medio utilizado, en este caso, aquello con lo que se amenaza. Me refiero a la extorsión realizada por cibercriminales, generalmente por bandas organizadas, consistente en la solicitud de importantes cantidades económicas a cambio de cesar en la realización de algún tipo de ciberataque o incluso de empezar a ejecutarlo. Al igual que en los casos de extorsión normal, el criminal aprovecha el hecho de que para la víctima puede resultar más sencillo, e incluso beneficioso, atender a la solicitud del criminal y no recibir el ataque que ser víctima de él y tratar de defenderse posteriormente. En el caso de los comportamientos cibercriminales, estas conductas parecen proliferar en relación con las páginas web dedicadas a las apuestas y a los juegos de azar *online*, a las que les interesa pagar cantidades no demasiado grandes a las mafias a cambio de no sufrir un ataque de denegación de servicios o similares en fechas concretas que les puede paralizar la página web y hacerles perder cantidades significativamente superiores.

3.2.5. El ciberacoso

Finalmente, el ciberespacio también es un medio de intercomunicación personal, por lo que dentro de esta categoría de infracciones tradicionales en las que lo que cambia es el medio de realización de las mismas, entrarían las conductas de ataque a bienes personalísimos, como las amenazas, coacciones, injurias, calumnias y otras agresiones al honor o a la libertad. Destacan algunas de ellas por su especial trascendencia al afectar a menores de edad como el *cyberbullying* y el *child grooming*.

El ***cyberbullying*** ha sido definido como la conducta consistente en "infligir daño de forma voluntaria y repetida a través de texto electrónico", y es un comportamiento que, si no sustituir, si que va a complementar muchas conductas de *bullying* entre menores, debido a la popularización, también en ese espectro de la población, del uso de las TIC en general, y de las redes sociales en particular.

En este caso, y frente al *bullying* tradicional, el poder que se ejerce sobre la víctima ya no es físico ni (tan solo, pues también puede serlo) social, sino que se trata de un poder en línea que se deriva de la unión entre la crueldad asociada a este tipo de intimidación y la habilidad: es el joven capaz de navegar y dominar el mundo electrónico el que está en una posición de poder en relación con una víctima y puede utilizar las TIC para acosar a sus víctimas.

Se incluye también dentro de la modalidad de acoso en el ciberespacio el ciberacoso sexual, tanto a menores como a mayores, en el que se aprovecha el uso de distintos instrumentos de comunicación como el Messenger, el correo electrónico, el sistema de comunicación oral Skype o las redes sociales como Twitter o Facebook para realizar el atentado contra la libertad sexual de otra persona. Hay que tener en cuenta que el atentado puede ser de todo tipo, puesto que la popularización del uso de las webcam amplía profundamente el catálogo de comportamientos relacionados con la libertad sexual que pueden ser realizados a través de Internet: ya no se trata únicamente de la posibilidad de realizar un acoso sexual por medio de palabras, sino que es posible la difusión directa de contenido sexual a un menor o, incluso, la visualización de una actitud sexual de la víctima coaccionada por una amenaza.

El comportamiento más conocido de ataque relacionado con la indemnidad y la libertad sexual en el ciberespacio es el denominado ***child grooming***, que consiste en contactar con menores por medio de las redes sociales o de otras formas de comunicación, como las salas de chat, canales de Messenger o similares, para acercarse a ellos e intentar posteriormente un acoso sexual.

Otro de los comportamientos de moda relacionados con este ámbito es el denominado ***sexting***, que consiste en la realización, por parte de menores, de fotografías propias de desnudos completos o de partes desnudas y su envío, generalmente por medio del teléfono móvil, a otros, junto con textos obscenos y con la finalidad de conocer personas, de enviar mensajes de amor o de odio.

Por último, destacar otra de las conductas de acoso a través de la Red, el ***cyberstalking*** entendido este como el uso de Internet u otra tecnología de la comunicación para hostigar, perseguir o amenazar a alguien. Se sustituyen las llamadas de teléfono a horas en que el sujeto no está en casa, o las visitas al trabajo y a la casa, así como los seguimientos no deseados, por otras conductas como el envío de decenas de correos o de mensajes a través de las redes sociales, la puesta a disposición del público de fotos, mensajes o correo de la víctima en páginas web, etc. Lo habitual es que el *cyberstalker* seleccione a su víctima a través de chats, foros, etc. y una vez seleccionada realiza una o distintas formas de persecución como intentar contactar en repetidas ocasiones con ella, amenazarle con violencia física, solicitarle sexo de forma explícita, enviarle imágenes obscenas entre otras, siempre teniendo en cuenta el carácter repetitivo de la acción. El medio más común empleado por los *cyberstalkers* es el correo electrónico para enviar mensajes de acoso, amenaza, odio, obscenos o incluir imágenes hirientes. Otras formas de *cyberstalking*, aunque menos usadas, son instar a otros usuarios de Internet a acosar o amenazar a la víctima mediante foros o chat, enviar archivos infectados con la intención de dañar el sistema informático de la víctima y el robo de identidad, siendo estos dos últimos considerados como *cyberstalking* únicamente cuando el objetivo del agresor sea intimidar a la víctima.

3.3. Ciberataques de contenido

Conforman el último grupo de conductas denominadas de contenido que hacen referencia a una forma concreta de los ataques denominados réplica, pero con una singularidad tal y con problemáticas jurídicas tan especiales que merecen ser tratadas por separado.

Los **ciberataques de contenidos** aglutinan a todas aquellas conductas en las que el centro de la infracción lo constituye el contenido que se comunica o se transmite a través de Internet.

La facilidad con la que hoy se puede digitalizar cualquier tipo de información y con la que se puede comunicar la misma a múltiples receptores simultáneamente y situados en lugares diversos de todo el mundo, convierte a la Red en un medio abierto en el que los contenidos ilícitos, al igual que los lícitos, también pueden viajar con facilidad. Hay que tener en cuenta, además, que frente al resto de medios de comunicación, Internet funciona simultáneamente como un medio de edición y como un medio de comunicación, en el sentido

de que la dicotomía entre emisor y receptor se difumina en el ciberespacio, donde un usuario puede pasar de ser receptor a ser también comunicador y productor de contenidos. Si a ello se suma la popularización de Internet y la facilidad para el acceso y el envío de información a través del mismo, y la progresiva utilización por los menores de este sistema de comunicación, se puede entender entonces que desde hace ya más de una década surgiera una preocupación por los contenidos, ante la aparición de todo un conjunto de conductas a las que les une que la ilegalidad proviene, no del medio utilizado, sino del contenido distribuido por Internet.

3.3.1. Pornografía infantil en Internet

Uno de los problemas clásicos con carácter internacional es la difusión de pornografía infantil, en el que se aprovecha la capacidad de comunicación transnacional y la anonimidad que aporta Internet para difundir material pornográfico. En este, o bien se ha usado niños para su realización, o bien se utilizan imágenes figuradas representativas de menores de edad manteniendo relaciones sexuales.

> El Grupo Interpol, especializado en crímenes contra los niños, ha definido pornografía infantil como "toda forma de representación o promoción de la explotación sexual de los niños, incluidos los materiales escritos y de audio, que se concentren en la conducta sexual o los órganos genitales de los niños".

Este fenómeno está cada vez más vinculado al uso de las nuevas tecnologías de la información, hasta el punto de que, en la actualidad, desde una perspectiva criminológica, puede decirse que la mayoría de estos comportamientos se perpetran básicamente a través de Internet.

La **pornografía infantil** ha pasado por varias **fases** a lo largo de los años:

1) En una primera fase, se empleaban **páginas web alojadas en servidores de Internet**, en las que el traficante comerciaba con el material pornográfico que ponía a disposición de los usuarios, que previamente accedían a pagar una contraprestación que se satisfacía por medio de un cargo en la tarjeta de crédito del adquiriente.

Dentro de esta primera fase se pueden diferenciar dos modalidades, por un lado, la del usuario que decide navegar con el objeto de acceder a una página web concreta cuyo contenido sabe con certeza que contiene material pornográfico infantil, y por otro lado, la de aquel que crea la página web misma. Sin embargo, como este sistema era de fácil detección, se abandonó y se pasó a usar otras modalidades.

2) La segunda fase se desarrolla en los **chats a tiempo real**, en los que los pedófilos dialogan entre sí y acuerdan intercambiarse a través del correo electrónico el referido material, la compra directa de este elemento por medio de alguna página web o la simple descarga de archivos, en los que el intercambio de fotografías de pornografía infantil es cuestión de segundos. Otra de estas nuevas modalidades conductuales que surgieron fueron los **grupos de noticias y foros** como medio de comunicación, así como el **camuflaje de las páginas web** de pornografía infantil, no accesibles a través de buscadores y localizables solamente para iniciados. Posteriormente, debido a que los *chat rooms* son evitados por los pedófilos al darse cuenta de que pueden estar infiltrados por agentes encubiertos, la figura del traficante de pornografía infantil es sustituida en gran medida por la de los consumidores que informalmente se asocian sin ánimo de lucro. Estos **socios**, actuando coordinadamente, pueden descargarse en su ordenador multitud de fotografías en poco tiempo a través de técnicas de intercambio por medio de correo electrónico o de fórmulas como ***send to receive***.

En esta acelerada evolución, los programas de globalización de archivos individuales han habilitado nuevas vías comisivas, en tanto que permiten al usuario la posibilidad de compartir parte del contenido de su ordenador con las personas que se encuentren conectadas a la Red utilizando ese mismo programa (programas tipo Napster), de forma que los usuarios de los programas de archivos compartidos ponen en común su material pornográfico, sin necesidad de entablar contacto directo, realizar adquisiciones individualizadas o mantener conversación alguna. Así, **el intercambio mutuo de material sustituye a la compra al traficante**. Dentro de esta modalidad, debemos hacer referencia a dos tipos de protocolos, el **FTP** y el **p2p**, que dan lugar a dos tipos de comportamientos muy distintos.

3.3.2. La ciberpiratería intelectual

La ciberpiratería intelectual es otra forma de ciberataque de contenido que abarca desde la de obras digitalizadas, pasando por la comunicación pública de las obras vía *streaming* a cambio de una cantidad de dinero, entre otras muchas. Internet ha dado lugar a variadas conductas caracterizadas por la infracción de derechos de propiedad intelectual y que englobarían lo que se viene denominando **ciberpiratería**. La mayor parte de ellas, sin embargo, han acabado desapareciendo debido al impacto del comportamiento que, sin lugar a dudas, más daño ha hecho a la industria del entretenimiento, pero sobre el que más podría discutirse su consideración como piratería digital, el intercambio gratuito de archivos.

El uso compartido de archivos se inició con el protocolo IRC[1] a mediados de la década de los noventa, alcanzando en el cambio de milenio su apogeo con Napster primero, y luego con un nuevo sistema de intercambio de archivos con un protocolo p2p[2]. Este sistema permaneció en auge con programas como

(1)Sigla que corresponde a *internet relay chat*.

(2)Sigla que corresponde a *peer-to-peer.*

eMule o Ares, que compartió con los sistemas de *streaming*, hasta que se ha puesto en boga el **sistema de descarga directa**, surgiendo programas como Megaupload, RapidShare o MediaFire, que si bien servían en apariencia para guardar archivos y codificarlos, se relacionaban con múltiples blogs y páginas que enlazaban los nombres de los contenidos protegidos con los de los códigos de descarga en webs de este tipo.

Megaupload

Y si bien el cierre de Megaupload por parte del FBI pudo suponer un aparente ataque al sistema de descargas en Internet, su sustitución inmediata por otras webs y otros sistemas de intercambio gratuito de archivos conlleva que difícilmente sea una opción real para el consumidor de bienes culturales en el ciberespacio el pagar por ello. De hecho, además de la proliferación de sitios de descarga gratuita de archivos y de nuevas formas de explotación, en ocasiones lícitas, pero contrarias a la configuración tradicional de la propiedad intelectual, se une el hecho de que en los motores de búsqueda como Google, Yahoo! y Bing, muchos de los principales resultados que brindan sus páginas proporcionan enlaces a contenidos no autorizados o a sitios que infringen los derechos de autor. Estas empresas, sin embargo, tratan de responder inmediatamente a las demandas y solicitudes de los titulares de los derechos.

3.3.3. Difusión de otros contenidos ilícitos

La posibilidad de introducir información en la Red con contenidos ilícitos diversos y de difundirlos a través de ella ha convertido a la Red en un medio potente para la comisión de delitos, como la apología y otros actos preparatorios del terrorismo.

Dentro de esta última categoría encontramos el denominado ***cyberhate speech*** o **incitación al odio racial**. El ciberespacio incrementa el riesgo que tal actividad supone: como ámbito transnacional y mundial, es un peligroso lugar para la difusión de mensajes racistas y violentos, que se vierten con más facilidad en Internet ante la dificultad de persecución de la cibercriminalidad y las mayores facilidades para el anonimato que da el medio. Internet permitía sustituir prospectos y folletos racistas que eran difundidos localmente, por webs y blogs fáciles de hacer y que resultaban mucho más eficaces para transmitir ideas odiosas a millones de personas en todo el mundo. Aunque no hay cifras fiables, se calculan que son miles las webs que, mayoritariamente provenientes de EE.UU., fomentan y difunden ideas racistas, generalmente relacionadas con la supremacía blanca, aunque también las hay que difunden similares mensajes fascistas bajo otras apariencias ideológicas.

También podríamos integrar dentro de este tipo de cibercriminalidad otras páginas web en las que el mensaje de odio y de incitación a la violencia y de difusión de ideas racistas es menos abstracto y mucho más localizado contra partidos políticos, gobernantes o asociaciones concretas y determinadas. Es cierto, sin embargo, que estas conductas apenas se pueden deslindar de la incitación que suponen algunas formas de terrorismo:

Ejemplos de difusión de contenidos ilícitos

Dos ejemplos bien conocidos serían la campaña, focalizada en Internet, de amenazas e incitación a la violencia, realizada desde sectores islamistas radicales contra Dinamarca y el dibujante de un periódico que identificaba en sus viñetas a Mahoma y a los musulmanes, con los terroristas; y por otra parte, la campaña llevada a cabo por medio de vídeos en YouTube en la que se promocionaba la quema de ejemplares de *El Corán* como forma de protesta ante la decisión de construir en Nueva York, en la denominada Zona Cero, una mezquita.

Ambos comportamientos comparten no solo que se trata de mensajes de incitación al odio y a la violencia, sino que, pese a realizarse en un ámbito localizado muy concreto (un humorista en Dinamarca y frente a él varios estudiantes musulmanes desde sus universidades en Siria o Irán, o un sacerdote de una pequeña iglesia de un diminuto pueblo de EE. UU.), al utilizarse Internet para la difusión del mensaje, el mismo acaba llegando a muchísimas personas y generando un clima de odio con consecuencias difíciles de medir.

Resumen

El fenómeno de la delincuencia asociada a las TIC es una realidad que está adquiriendo protagonismo en los últimos años. Sin embargo, en muchas ocasiones se exagera la amenaza que conlleva el mismo y en otros no se percibe el riesgo real y en parte derivado por la altísima cifra negra de este tipo delincuencia.

Hay que tener en cuenta que el uso de Internet ha evolucionado desde su creación, pasando de ser un medio usado por unos pocos hasta convertirse en el medio más usado para realizar operaciones económicas y establecer relaciones sociales. Del mismo modo que ha evolucionado Internet, paralelamente también lo ha hecho la cibercriminalidad, y con estos, sus actores principales, pasando desde los primeros ataques destinados a los terminales a los que tienen como objetivo otros bienes personalísimos, como la integridad, la indemnidad sexual, la dignidad personal, etc. Así, durante la primera época de la cibercriminalidad lo característico era el uso de ordenadores para la comisión de delito, precedido por otra época en la que la característica central es que el delito se comete a través de Internet hasta una tercera en la que los delitos están absolutamente determinados por el uso de Internet y las TIC.

En definitiva, esta evolución nos ha permitido establecer una clasificación de los delitos en función de la incidencia que tienen las TIC en su comisión. Así, hemos visto cómo el ciberespacio se ha convertido en algunos casos en un generador de nuevas conductas que solo se pueden realizar a través de las TIC y que hemos venido a denominar ciberataques puros. En otros casos, la evolución de las TIC ha servido para realizar delitos que ya se venían cometiendo en el mundo físico, por lo que han sido denominados ciberataques réplica, pero que los caracteres especiales de este nuevo ámbito les confiere una singularidad tal que les hace parecer conductas nuevas. Y finalmente, hemos estudiado los llamados ciberataques de contenido y que vienen a englobar todos los delitos en los que la infracción viene determinada por la información ilícita que se transmite y que, teniendo en cuenta la difusión que puede ofrecer Internet, suponen un gran peligro.

Ejercicios de autoevaluación

1. La infección por *malware* es...

a) un ciberataque puro.
b) un ciberataque réplica.
c) un ciberataque de contenido.
d) Ninguna de las anteriores es correcta.

2. El ciberataque que consiste en adaptar al mundo virtual comportamientos delictivos que ya se hacía por otros medios es un...

a) ciberataque económico.
b) ciberataque réplica.
c) ciberataque puro.
d) ciberataque de contenido.

3. 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) *child grooming*.
b) *grooming*.
c) *cyberstalking*.
d) *cyberbullying*.

4. El que roba información de una empresa aprovechándose de su situación dentro de ella es un...

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

5. El concepto de cibercrimen entendido desde un sentido amplio abarca...

a) cualquier comportamiento delictivo realizado en el ciberespacio.
b) solamente comportamientos tradicionalmente ilícitos, en lo que únicamente cambia que ahora se llevan a cabo en Internet.
c) conductas cuyo contenido ilícito se relaciona directamente con bienes existentes en el ciberespacio.
d) Ninguna de las opciones es correcta.

6. El tipo de ciberfraude que consiste en propuestas de negocio engañosas es...

a) *pharming*.
b) *phishing*.
c) *spoofing*.
d) *scam.*

7. El *cyberhate* es...

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

8. Desde un concepto empleado en sentido restringido para el cibercrimen, solo se englobaría dentro de él un comportamiento delictivo en el que...

a) se utilicen medios tecnológicos.
b) se aprovecha el ciberespacio para poderlo ejecutar.
c) la esencia del injusto no se puede dar fuera de él.
d) Ninguna de las anteriores es cierta.

9. ¿Cuál de los siguientes cibercrímenes sería categorizado como un ciberataque de contenido?

a) Acosar a alguien a través de las redes sociales.
b) Introducirse sin permiso a través de Internet en el terminal de otro sujeto.
c) Robar los datos de acceso a las cuentas bancarias.
d) Crear una página web con mensajes que incitan a la violencia.

10. El motivo por el que la cifra negra de la cibercriminalidad es superior a otras formas de delincuencia se debe a...

a) que es muy difícil la determinación del autor.
b) la falta de denuncia por parte de los afectados.
c) que la conducta pasa inadvertida.
d) Todas las opciones anteriores son correctas.

Solucionario

Ejercicios de autoevaluación

1. a

2. b

3. a

4. c

5. a

6. d

7. b

8. c

9. d

10. d

Glosario

cibercrimen *m* Cualquier delito llevado a cabo en el ciberespacio.

ciberespacio *m* Término que indica el lugar de intercomunicación social transnacional, universal, popularizado y en permanente evolución derivado del uso de las TIC.

cyberbullying *m* Daño repetido e intencionado a través de medios electrónicos como teléfonos móviles o Internet realizado por un grupo o individuo contra el que la víctima no puede defenderse de si misma.

cybergrooming *m* Ciberacoso sexual a menores.

cyberhate *m* Difusión de mensajes de odio racial en el ciberespacio.

cyberstalking *m* Uso de Internet u otra tecnología de la comunicación para hostigar, perseguir o amenazar a alguien de forma repetida.

***denial of services* (DoS)** *m* Denegación de servicios. Ciberataque consistente en saturar el servidor del sistema logrando que el mismo se centre en la petición que realiza el atacante sin que pueda atender a ninguna más.

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.

hardware *m* Conjunto de los componentes que integran la parte material de una computadora.

insider *m y f* Cibercriminal que pertenece o trabaja para la institución o empresa víctima de la infracción.

Internet *m* Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

keylogger *m* Tipo de hardware o software, que se dedica a registrar las pulsaciones que se realizan en el teclado con la finalidad de memorizarlas y posteriormente enviarlas al sujeto que las utilizará para acceder a la información o al patrimonio de la víctima.

malware *m* Software malicioso destinado a dañar, controlar o modificar un sistema informático.

nativos digitales *m y f* Término acuñado para referirse a la generación nacida con la implantación total de Internet.

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 FTP *m* Protocolo de transferencia de ficheros.

protocolo IP *m* Protocolo de Internet. Es un protocolo para el envío y recepción de datos a través de una red de paquetes conmutados.

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

scam *m* Concepto que podría englobar a casi todos los fraudes en el ciberespacio, si bien se suele utilizar como referencia de los más burdos de ellos, aquellos en los que el engaño es poco elaborado y en los que el error de la víctima puede ir más allá de lo común.

sexting *m* Realización, por parte de menores, de fotografías propias de desnudos completos o de partes desnudas y su envío, generalmente por medio del teléfono móvil, a otros, junto

con textos obscenos y con la finalidad de conocer a personas o de enviar mensajes de amor o de odio.

snooping *m* Acceso no autorizado a datos de otros.

software *m* Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

spam *m* *E-mail* no solicitado que suele enviarse a un gran número de direcciones electrónicas bien a través de una dirección electrónica de las ofrecidas por los servicios de correo gratuitos estilo Hotmail, o bien desde un sistema informático infectado, convertido en *botnet* y utilizado por el *spammer*, que adquiere las direcciones de correo bien *hackeando* sistemas informáticos o bien utilizando *spyware* u otros sistemas de búsqueda de direcciones electrónicas a través de la Red.

spoofing *m* Suplantación de identidad.

spyware *m* Software que se instala en un sistema informático y que recopila determinada información de este, que después envía a otro sistema.

TIC *f pl* Tecnologías de la información y la comunicación.

troyano *m* Programa malicioso que mediante ventanas emergentes recoge claves; y en general cualquier otra técnica que, utilizando software permite perfeccionar el engaño haciendo creer a la víctima que está fuera de peligro.

Wifi *m* Tecnología de comunicación inalámbrica.

Bibliografía

Agustina Sanllehí, J. R. (2010). "¿Menores infractores o víctimas de pornografía infantil? Respuestas legales e hipótesis criminológicas ante el Sexting". *RECPC* (núm. 12-11).

Agustina Sanllehí, J. R. (2009). "La arquitectura digital de Internet como factor criminógeno". *IeJCS* (art. 4, núm. 3).

Álvarez Vizcaya, M. (2001). "Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la Red". *CDJ* (núm. 10). Madrid.

Bocij, P. (2003). "Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet". *FMPRJI* (vol. 8, núm. 10).

Chawki, M.; Abdel Wahab, M. (primavera, verano, 2006). "Identity Theft in Cyberspace: Issues and Solutions". *LE* (vol.11, núm. 1).

Chiu, C.; Ku, Y.; Lie, T.; Chen, Y. (2011). "Internet Auction Fraud Detection Using Social Network Analysis and Classification Tree Approaches". *IJEC* (vol. 15, núm. 3).

Choo, K. K. R. (2007). "Zombies and Botnets". *TICCJ* (núm. 233). Canberra.

Chua, C. E. H.; Wareham, J. (2004). "Fighting Internet Auction Fraud: An Assessment and Proposal". *IEEE Computer* (núm. 10).

Cilli, C. (2005). "Identity Theft: A New Frontier for Hackers and Cybercrime". *Information Systems Control Journal* (vol. 6).

Marco Marco, J. J. (coord.) (2010). "Menores, ciberacoso y derechos de la personalidad". En: J. García González. *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet*. Valencia: Tirant lo Blanch.

Morillas Fernández, D. L. (2005). *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comisivas relacionadas con Internet* (Colección Monografías de Derecho penal, 4). Madrid: Dykinson.

Patchin, J. W.; Hinduja, S. (2006). "Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying". *YVJJ* (vol. 4).

Pathé, M.; Mullen, P. E. (1997). "The impact of stalkers on their victims". *BJP*.

Pérez Martínez, A.; Ortigosa Blanch, A. (coord.) (2010). "Una aproximación al ciberbullying". En: J. García González. *Ciberacoso: La tutela penal de la intimidad, la integridad y la libertad sexual en Internet*. Valencia: Tirant lo Blanch.

Pinguelo, F. M. ; Muller, B. W. (primavera, 2011). "Virtual Crimes, Real Damages: A Primer On Cybercrimes In The United States and Efforts to Combat Cybercriminals". *VJLT* (vol. 16, núm. 1).

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

Pollock, E. T. (2010). "Understanding and Contextualising Racial Hatred on the Internet: A Study of Newsgroups and Websites". *Internet Journal of Criminology*.

Poullet, Y. (2007). "Hacia nuevos principios de protección de datos en un nuevo entorno TIC". *IDP* (núm. 5).

Prensky, M. (octubre, 2001). "Digital Natives, Digital Immigrants". *On the Horizon* (vol. 9, núm. 5). Lincoln: NCB University Press.

Romeo Casabona, C. M. (coord.) (2006). *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Granada: Comares.

Sommer, P.; Brown I. (2011). "Reducing Systemic Cybersecurity Risk". *Contribution to the OECD project Future Global Shocks*. Oxford University Press.

Thomas, D.; Loader, B. (eds.) (2000). *Cybercrime: Law enforcement, security and surveillance in the information age*. Londres: Routledge.

Villacampa Estiarte, C. (2010). "La respuesta jurídico-penal frente al stalking en España: presente y futuro". *Revista del Instituto Universitario de Investigación en Criminología y Ciencias Penales de la UV*. Disponible en http://www.uv.es/recrim/recrim10/recrim10a03.pdf.

Wall, D. S. (2005). "What are Cybercrimes?". *CJR*.

Wall, D. (2007). *Cybercrime: the transformation of crime in the information age*. Cambridge: Polity Press.

Williams, P. (agosto, 2001). "Organized Crime and Cybercrime: Synergies, Trends, and Responses". *ATC* (vol. 6).

Yar, M. (2005). "The novelty of 'cybercrime': an assessment in light of routine activity theory". *EJC* (núm. 2).

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