El cibercrimen en el ámbito económico y patrimonial

Prof. Dr. iur Dr. med. Carlos María Romeo Casabona
Prof. Dr. Iñigo de Miguel Beriain

Temario

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

Tema 1º

Aspectos generales sobre la cibercriminalidad y el cibercrimen

Las formas de aparición del cibercrimen. La vulnerabilidad de las TIC ¿Delitos informáticos o ciberdelitos?

1. LAS FORMAS ACTUALES DE APARICIÓN DEL CIBERCRIMEN

La fenomenología criminal vinculada con las Tecnologías de la Información y la Comunicación (TIC) es cada vez más abundante y variada, sin perjuicio de que algunas conductas continúen siendo las más relevantes por su frecuencia y en ocasiones también por su gravedad. Es asimismo cierto que sus formas de aparición concreta van cambiando con el paso del tiempo, al irse adaptando a las nuevas potencialidades que de forma constante ofrecen estas tecnologías. Así, habría que destacar en primer lugar que la extensión y el uso de redes telemáticas (en particular, Internet) es un fenómeno más de la globalización (probablemente, también sea cierto su contrario: las comunicaciones telemáticas por medio de sistemas informáticos han contribuido a su vez a desplegar este fenómeno), lo que ha originado al mismo tiempo encuentros o enfrentamientos entre culturas y sistemas jurídicos diferentes, esto es, entre cosmovisiones muy diversas.

Conductas principales

- ✓ ***Accesos no autorizados***
- ✓ ***Interceptaciones de las comunicaciones***
- ✓ ***Manipulaciones de datos o de sistemas informáticos***
- ✓ ***Interferencias dañosas o inutilizadoras de sistemas informáticos***
- ✓ ***Introducción y difusión en la red de contenidos ilícitos***
- ✓ ***Copia e intercambio de obras de creación intelectual***

Accesos no autorizados.

En cuanto a manifestaciones concretas, habría que recordar los accesos no autorizados o no consentidos en ficheros, bases de datos o sistemas informáticos ajenos (*hackering*), los cuales pueden perseguir los más variados objetivos y una dañosidad también de muy diversa entidad: desde las acciones destructivas (*crackering*),

pasando por lo que se conoce como "intromisión blanca", expresión con la que se designa el supuesto de hecho conforme al cual en realidad no se persigue un propósito diferente a lograr el mero acceso a un archivo o base de datos por lo general protegido por procedimientos lógicos –informáticos- concebidos para impedir accesos de terceros no autorizados.

Interceptaciones de las comunicaciones.

Son asimismo relevantes desde el punto de vista jurídico-penal las interceptaciones de las comunicaciones de carácter personal o de otra naturaleza (financiera, comercial, etc.), como pueden ser los mensajes de correo electrónico, conversaciones orales o escritas a tiempo real (teléfonos por cable, celulares o móviles, foros restringidos, *chat*), remisión o intercambio de documentos, etc.

Manipulaciones de datos o de sistemas informáticos.

Por otro lado, también pueden realizarse modificaciones, incluso meramente transitorias, mediante manipulaciones de datos o de sistemas informáticos con el fin de obtener un beneficio, por lo general económico.

Interferencias dañosas o inutilizadoras de sistemas informáticos.

Son igualmente demasiado conocidas las difusiones de virus informáticos y la perpetración de otras conductas dañosas o inutilizadoras de los sistemas informáticos y de ficheros a través de la red (daños sabotaje informático, ciberterrorismo), los cuales suelen expandirse con gran rapidez y amplitud en todo tipo de terminales, incluidos los de uso doméstico o personal, para cuyo propósito se utiliza con frecuencia el correo electrónico o las descargas de contenidos de la red como medios transmisores y de acceso al sistema del terminal, pudiendo alcanzar sus daños globales en ocasiones cuantías económicas muy elevadas.

Introducción y difusión en la red de contenidos ilícitos.

La posibilidad de introducir información (datos, imágenes, voz y sonido) de en la red con contenidos ilícitos muy diversos y de difundirlos a través de aquélla, han convertido a la red en un medio muy potente para la comisión de otros delitos: apología del terrorismo y de otros actos preparatorios relacionados con él, incitación a la xenofobia, al odio racial y a la discriminación, escarnio religioso, difusión y posesión de pornografía infantil.

Copia e intercambio de obras de creación intelectual (programas de ordenador y productos multimedia).

Finalmente, la capacidad de reproducción e intercambio de **obras de creación intelectual** de todo tipo, infringiendo los derechos de autor con fines comerciales, o destinando su copia a usos exclusivamente personales, ha adquirido un desarrollo extraordinario, en particular de programas de ordenador, obras musicales y producciones cinematográficas. El recurso a las TIC en este sector ha puesto en evidencia más que en cualquier otro la insolvencia de las construcciones jurídicas creadas en su entorno, puesto que el sistema jurídico actual de regulación y protección de los derechos vinculados con las obras de creación intelectual apenas puede satisfacer las exigencias y los diferentes intereses presentes actualmente en el mercado.

2. LA VULNERABILIDAD DE LAS TIC FRENTE AL HECHO DELICTIVO

Esta otra cara de la moneda de, por lo demás, tan potentes y versátiles tecnologías nos muestra, por consiguiente, su extraordinaria vulnerabilidad ante su utilización abusiva y con ello la aparición de un nuevo factor criminógeno de primera magnitud. En resumen, el ciberespacio presenta unos perfiles de gran interés para el Derecho Penal, pues en gran parte en ellos radica su propia vulnerabilidad:

Vulnerabilidad de las TIC

1. ***La capacidad para procesar, albergar y circular, de forma automatizada y a tiempo real, ingentes cantidades de información.***
2. ***Las dimensiones colosales del número de usuarios.***
3. ***Las propias características físicas, técnicas y lógicas de las TIC.***
4. ***La extraordinaria potencialidad multiplicadora de las acciones ilícitas y de sus efectos lesivos para los bienes jurídicos afectados.***

a) **La capacidad para procesar, albergar y circular, de forma automatizada y a tiempo real, ingentes cantidades de información** bajo las formas (digitales) más variadas, gracias a la disponibilidad de protocolos universales de transmisión y acceso: texto, sonido, imagen y voz, sin más límites de volumen, espaciales y temporales que los de la propia red. Por otro lado, la estructura descentralizada y no jerarquizada de la red es incompatible con la existencia de órganos o instituciones de control de la información circulante, incluido el establecimiento de una censura sistemática, lo que comporta la imposibilidad o la extraordinaria dificultad de filtrar, supervisar o controlar semejante volumen de información.

b) **Las dimensiones colosales del número de usuarios**, las frecuencias de acceso y uso por parte de los mismos, así como la libre circulación y navegación, tanto para emitir, transferir y difundir información como para acceder a ella por medio de la red. De este modo, los cibernautas han pasado a ser al mismo tiempo tanto potenciales víctimas como perpetradores de los hechos ilícitos. Unos y otros pueden introducirse en la red de forma anónima (o, tal vez mejor, pseudoanónima, pues en buen número de casos podrán ser identificados, al menos el punto desde el que accedieron a la red, tras las investigaciones oportunas), o simulando una identidad diferente de la verdadera. Estas posibilidades pueden facilitar la comisión del delito, dificultando al mismo tiempo su investigación y persecución judicial, pues aun siendo factible seguir el rastro digital dejado al iniciar la comunicación y proseguir la navegación y accesos correspondientes, pudiendo establecer así desde qué terminal y a través de qué servidor se accedió y actuó criminalmente en la red, no lo es tanto identificar quién fue el individuo concreto que realmente lo perpetró.

c) **Las propias características físicas, técnicas y lógicas de las TIC**, que pueden ser intervenidas y alteradas –aunque sea momentáneamente, lo que suscita el interrogante jurídico-penal de si realmente se alteró un dato, fichero o software. De este modo puede conseguirse el acceso a ficheros y archivos de muy variada naturaleza y trascendencia sin la autorización o el consentimiento de sus titulares o responsables, la manipulación de sus contenidos por diversos procedimientos, incluida la alteración del software conforme a las necesidades o propósitos del intruso. Además, la capacidad material de controlar la información circulante en las redes por parte de las autoridades u otros responsables (p. ej., los proveedores de acceso o de servicios en la red) es limitada, a la vista de la complejidad de éstas y de sus estructuras organizativas, del número de sus usuarios, de la posibilidad de acceder a las redes desde cualquier punto geográfico y de la cantidad de información depositada o circulante o meramente accesible.

d) **La extraordinaria potencialidad multiplicadora de las acciones ilícitas y de sus efectos lesivos para los bienes jurídicos afectados**. En efecto, otra de las gran des preocupaciones respecto a la vulnerabilidad criminógena de la red se refiere a que ésta y la creación de sitios, foros de debate, y otros procedimientos similares en aquélla pueden facilitar o magnificar la comisión de algunos delitos cuyo injusto viene fundamentado en los contenidos de la información, como son los casos de la apología

del terrorismo, la discriminación de determinados grupos de personas, la xenofobia, la comisión de injurias en contra de terceros, la difusión de pornografía infantil, basada tanto en imágenes reales como virtuales, la distribución e intercambio no autorizados de obras de creación intelectual, etc. A diferencia de otros procedimientos de difusión de estos contenidos, la red no sólo facilita dicha difusión gracias a sus características más destacables, sino también debido a que abarata considerablemente estos costes y favorece al mismo tiempo la comunicación e intercambio con personas afines (p. ej., en relación con la pornografía infantil). Las TIC se han convertido asimismo en un útil y sofisticado instrumento para el desarrollo de las actividades delictivas vinculadas con el crimen organizado.

Significa esto que el Derecho Penal se enfrenta a una criminalidad progresivamente más poderosa y peligrosa desde muchos puntos de vista, a la que aquél no debe renunciar a darle la respuesta que sea necesaria. Al mismo tiempo se acrecienta su complejidad técnica y jurídica, con el efecto subsiguiente de que las construcciones jurídico-penales (pero asimismo, las de otras disciplinas jurídicas) elaboradas a lo largo de las últimas décadas no siempre pueden adaptarse a las características de estas tecnologías ni a las manifestaciones criminales que propicia.

Es previsible, asimismo, que las TIC provoquen ya a corto plazo una profunda modificación y reelaboración de muchas categorías jurídicas de diversos sectores del ordenamiento jurídico. En todo caso, estas nuevas construcciones jurídicas vinculadas a las TIC habrán de ser creativas y adecuadas a las nuevas demandas jurídicas de aquéllas, pero al mismo tiempo habrán de aspirar a ser sólidas, creíbles y estables.

En resumen, se requiere un atento examen de tan diversos aspectos previamente a la adopción de las políticas legislativas oportunas en materia penal.

3. ¿DELITOS INFORMÁTICOS *VERSUS* CIBERDELITOS?

3.1. La evolución de los delitos relacionados con las TIC

La caracterización, tanto criminológica como dogmática, de los delitos informáticos no es sencilla, pues éstos mismos han experimentado una evolución y, hasta cierto punto, transformación. Como efecto, son también diversos los problemas jurídico-penales que se han ido planteando. Con la expresión

"delitos informáticos" suele aludirse a una pluralidad de conductas:

a) Aquéllas que atentan de forma grave a determinados bienes de titularidad individual –de personas físicas, pero también de personas jurídicas-, que presentan una configuración específica y exclusiva de la actividad informática y telemática y han sido sometidos a una 'tipología' técnico-criminológica: acceso, alteración, ocultación o destrucción no autorizados o no consentidos de los datos almacenados en un sistema informático; reproducción completa o parcial de datos contenidos en un sistema informático, así como la distribución o comercialización de los mismos. Asimismo, suelen incluirse otras conductas, como la sustracción del 'tiempo' o utilización ilegítima de equipos, sistemas, y redes informáticos o telemáticos, etc.

   En estos casos el equipo, sus elementos, sus productos o los sistemas de telecomunicación al servicio de éstos son el objeto del delito, esto es, el objeto material sobre el que recae la acción delictiva.

b) En otros supuestos, todos estos elementos y sistemas son un mero instrumento para cometer hechos por lo general ya castigados en el CP, pero lo que configura la originalidad del delito es precisamente la peculiaridad comisiva que ofrece ese instrumento o medio de ataque, que consiste en su elevada capacidad agresiva o multiplicadora de sus efectos lesivos. En este grupo se encontrarían los delitos contra la intimidad y contra los datos de carácter personal y el patrimonio (así, los delitos de descubrimiento y revelación de secretos, el llamado fraude informático, o los daños en las cosas), contra la libertad sexual (difusión de pornografía, particularmente infantil), contra los derechos de propiedad intelectual, contra la seguridad del Estado (informaciones secretas), principalmente.

c) Por último, existen otras conductas en las que es agredido el medio o instrumental informático (*software, hardware*) como objeto del tráfico mercantil y jurídico: derechos de propiedad intelectual e industrial, pacífica posesión o integridad del medio informático (delitos de daños), etc.

En resumen, tan variada manifestación delictiva puede diferenciarse de algún modo, teniendo en cuenta, por un lado, aquellos hechos delictivos que se valen principalmente de las

características de los sistemas informáticos y de ellos mismos. En esta primera generación delictiva la utilización de sistemas telemáticos y redes de comunicación para la comisión de la infracción delictiva tenía un alcance muy limitado y meramente operativo.

Estos ilícitos constituirían, según algunos autores, el llamado delito o delitos informáticos, que habría que distinguir en la actualidad del cibercrimen o de los ciberdelitos. A comprobar si es acertada o no esta clasificación en dos bloques delictivos, con base en qué criterios se sostiene y qué consecuencias jurídicas pueden aprovecharse de ella, voy a dedicar brevemente mi atención.

3.2. ¿Existe el llamado delito informático?

A la vista de las anteriores observaciones es cuestionable que, en sentido estricto, sea aceptable la denominación, en ocasiones generalizada, de "delito informático". La simple comprobación empírica de que estos nuevos 'delitos' (o hechos merecedores de respuesta penal) pueden ser cometidos en conexión con las TIC no es un argumento o razón suficiente para tratar, por lo menos en singular, de ellos como un fenómeno criminal autónomo ("delito informático"). Para un análisis acertado de la cuestión debemos retener tanto que caben multitud de formas de agresión como que son variados los bienes jurídicos susceptibles de dichos ataques. En efecto, la comprobación de la pluralidad de los componentes 'agresión' y 'bien jurídico' nos conduce a preferir aludir a una pluralidad de "delitos informáticos" o, incluso, según se ha indicado más arriba, "ciberdelitos", si son cometidos en una relación más estrecha con las redes telemáticas.

La incorporación de las TIC al mundo empresarial, financiero y económico ha abierto un nuevo campo a la delincuencia de índole patrimonial y socioeconómica, con profundas repercusiones en dichas actividades. Las conductas más significativas desde esta perspectiva se han venido agrupando en estas cinco modalidades principales: a) manipulaciones de datos y/o programas, o 'fraude informático'; b) copia ilegal de programas, 'piratería informática'; c) obtención y utilización ilícita de datos, o 'espionaje informático', que en este contexto económico quiere aludir a la afectación de la capacidad competitiva de la empresa (espionaje industrial, de mercado o financiero); d) destrucción o inutilización de datos y/o sistemas informáticos, o daños o 'sabotaje informático'; e) agresiones en el *hardware* o soporte material informático, principalmente 'hurto de tiempo de un sistema informático'.

La precedente clasificación continúa siendo muy sugestiva, si bien el paso del tiempo, la terminología utilizada, que en la actualidad puede parecer pintoresca, y la diversificación y evolución criminal han puesto en evidencia sus carencias actuales. Los problemas técnico-jurídicos y político-criminales de estas formas de delincuencia se han resuelto en un buen número de sistemas jurídicos con la incorporación de nuevos delitos al derecho positivo respectivo, para lo que se ha recurrido con tal propósito a diversas técnicas legislativas, a las que me referiré más abajo. En efecto, hasta que se produjo la intervención del legislador penal con relativa frecuencia resultaba problemático en el derecho comparado encuadrar estas conductas en los delitos tradicionales contra el patrimonio sin infringir al mismo tiempo las garantías derivadas de la observancia del principio de legalidad.

En conclusión, la pluralidad y diversidad de bienes jurídicos que pueden verse comprometidos, así como de medios comisivos, han impuesto la configuración en el derecho comparado de una pluralidad de 'delitos informáticos' y no de uno solo. En cualquier caso, ni la denominación de ‘delito informático’, ni la de ‘delitos informáticos’ (en todo caso preferible) apenas aportan en la actualidad una mínima precisión desde el punto de vista criminológico, político-criminal y de política legislativa.

3.3. El cibercrimen o ciberdelito

Los perfiles de los delitos informáticos han de ser sometidos a las peculiaridades jurídicas que pueden ofrecer nuevos recursos técnicos o de uso más extendido, como ha sucedido con las comunicaciones telemáticas abiertas, en particular con Internet. Como se indicó más arriba, estos medios permiten una ilimitada posibilidad de transferencia, flujo y comunicación de la información, así como el ofrecimiento de servicios de cualquier tipo, desde cualquier origen geográfico y hacia cualquier destino, prácticamente con una absoluta libertad de acceso y de puesta en circulación de cualquier información, así como de tratarla y manipularla. Al haberse extendido el uso de las redes de comunicación, convertidas en un instrumento de trabajo en numerosas actividades y en un punto de encuentro de las personas, su instrumentación criminal ha ido adquiriendo o acentuando otros perfiles que eran meramente incipientes con anterioridad. Como se indicó más arriba, la posibilidad de difundir contenidos ilícitos de dispar significación y la reproducción e intercambio de obras musicales y cinematográficas, etc., aparte de facilitar el acceso no autorizado o

no consentido a ficheros, archivos y documentos confidenciales situados en cualquier lugar del planeta, permiten calificar las TIC como instrumentos muy potentes para la comisión de delitos de muy diversa naturaleza.

De esta constelación de presupuestos fácticos surge la necesidad de distinguir una ulterior generación de delincuencia vinculada con las TIC y llevan a plantearse si expresiones nuevas o cuyo uso se está extendiendo podrían aglutinar todos los diversos aspectos que presenta la criminalidad vinculada con la combinación de los sistemas informáticos y telemáticos actuales. A este planteamiento responde, por ejemplo, la adopción y preferencia por el término "cibercrimen" (o "ciberdelito"), el cual se ha incorporado incluso a la legislación internacional, como ocurre con el Convenio Internacional del Consejo de Europa sobre Cibercrimen, hecho en Budapest el 23 de noviembre de 2001.

Por cibercrimen podemos entender el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos, individuales o supraindividuales.

Por consiguiente, y a la vista de los componentes fácticos someramente descritos más arriba, podrían incluirse como más característicos de esta ulterior generación delictiva vinculada al cibercrimen: a) la difusión de contenidos ilícitos; b) el acceso, alteración u obstrucción de sistemas y bases de datos ajenos, cualquiera que sea su estructura y contenido; c) los ataques a diversos objetos de la propiedad intelectual; y, d) delitos convencionales en los que la red constituye el factor más relevante para facilitar la comisión y la reiteración instantánea o sucesiva del hecho.

Desde un punto de vista técnico-jurídico tampoco parece, sin embargo, que el término cibercrimen pueda llegar a satisfacer plenamente una función dogmática de integración de estos delitos de nueva generación, sin perjuicio de que desde planteamientos criminológicos pueda ser adecuado para cumplir una función descriptiva o de identificación de un fenómeno criminal singular, pues presenta unos perfiles diferentes respecto a lo que se venía entendiendo por delito o delitos informáticos y, desde luego, respecto a cualesquiera otros delitos.

3.4. De los delitos informáticos a los cibecrimenes

En puridad, y sin perjuicio de las definiciones propuestas más arriba, no existe un concepto dogmático de delito o delitos informáticos ni de cibercrimen o ciberdelitos, ni tampoco puede construirse *de lege lata* en el Derecho español. No obstante, ambos términos pueden servir para identificar, respectivamente, sendos conjuntos de delitos, según se adelantaba más arriba. Los primeros estarían caracterizados por ser perpetrados en torno a sistemas informáticos, en los que la red, de ser utilizada, tiene por lo general una relevancia limitada o secundaria para las características de la conducta delictiva (es más frecuente que se trate entonces de redes cerradas o de acceso restringido). Mientras que los segundos girarían en torno a redes telemáticas (abiertas, cerradas o de acceso restringido), siendo en estos casos los sistemas informáticos más instrumentales o secundarios para la comisión del delito.

Por consiguiente, podría sostenerse que los ciberdelitos, aunque coexistan en el tiempo con los delitos informáticos, configuran una generación posterior de esta clase de delincuencia en relación con estos últimos, si nos fijamos en la diversificación y expansión que han alcanzado los ciberdelitos a lo largo de los últimos años. Por otro lado, como podrá comprobarse más adelante, los problemas jurídicos más específicos del cibercrimen están más relacionados con las insuficiencias de la aplicación de la ley penal en el ámbito espacial de su vigencia y con la necesidad de buscar otras fórmulas legales basadas en la extraterritorialidad y en la entreayuda judicial con el fin de superar los límites penales de dicho espacio, que con problemas de su adecuación típica, los cuales, no obstante, también pueden suscitarse en ciertos supuestos.

4. ALGUNAS DEFINICIONES LEGALES

En ocasiones la ley aporta alguna definición legal de conceptos o instituciones que guardan relación o están implicadas en los delitos correspondientes. A este respecto merece interés recordar aquí algunas definiciones aportadas por el Convenio sobre el Cibercrimen:

Definiciones del Convenio sobre el Cibercrimen de 2001 (Consejo de Europa)

"A los efectos del presente Convenio:

a) por 'sistema informático' se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;

b) por 'datos informáticos' se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;

c) por 'proveedor de servicios' se entenderá (véase más arriba);

d) por 'datos sobre el tráfico' se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente" (art. 1º).

En otro lugar veremos cómo el Código Penal (CP) proporciona otras definiciones, como la de documento, a los efectos penales (art. 26 CP).