FERNANDO MIRÓ LLINARES

# EL CIBERCRIMEN

## Fenomenología y criminología de la delincuencia en el ciberespacio

Prólogo de
Marcus Felson

Marcial Pons

MADRID | BARCELONA | BUENOS AIRES | SÃO PAULO

2012

# ÍNDICE

Pág.

## SEGUNDA PARTE
## CRIMINOLOGÍA DEL CIBERCRIMEN

### CAPÍTULO III
### CIBERESPACIO Y OPORTUNIDAD DELICTIVA



### CAPÍTULO IV
### EL CIBERCRIMINAL. PERFILES DE DELINCUENTES EN EL CIBERESPACIO

# PRÓLOGO

El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio *es el libro más importante publicado hasta la fecha acerca de la relación entre el cibercrimen y el amplio mundo de la actividad social y empresarial. Este libro no trata sobre tecnología ni sobre Derecho en sí, ni siquiera es un libro sobre problemas sociales generales. Por el contrario, esta obra pone de manifiesto la forma en que la cibercriminalidad se nutre de las actividades legales y de la extensa estructura de la vida cotidiana. Es cierto que ha habido otras personas que han abordado esta vinculación y planteado los conceptos básicos, pero estas páginas reflejan como nunca antes la medida en que la vida diaria genera la oportunidad de abusar de la tecnología para obtener un beneficio personal ilícito.*

*Para llegar a comprender el cibercrimen, para prevenirlo, es muy importante entender la forma en que las personas interactúan con el ciberespacio cada día e incluso cada hora, dónde lo hacen y el modo en que trabajan. Debemos pensar asimismo en la relación que guarda el uso del ciberespacio con los extensos patrones de la vida diaria. De hecho, una persona que trabaje en horario nocturno podría intentar hacerse con contraseñas o utilizar los ordenadores de empresas que no estén bajo vigilancia. Un padre que no supervise a su hijo adolescente durante el día o durante un viaje de fin de semana podría desconocer que se ha iniciado en el cibercrimen o que es víctima de éste. Una persona que haga uso de una cantidad considerable de pornografía legal puede ser extremadamente susceptible de convertirse en una víctima de, entre otros, usurpación de identidad o de diversos tipos de ataques informáticos o códigos maliciosos. La gente de negocios que viaja constantemente puede ser especialmente vulnerable al hacer uso del acceso a Internet que facilitan hoteles o lugares públicos, como es el caso de las cafeterías Starbucks y otros establecimientos. Las personas que realizan compras en línea de manera desmedida son asimismo especialmente vulnerables. Los usuarios de Internet que siguen un patrón de uso complejo o que descargan grandes volúmenes de datos se exponen a sí mismos a un mayor y más diverso número de riesgos que aquéllos que utilizan estos servicios con menos frecuencia. Muchos usuarios realizan un control menos exhaustivo de sus ordenadores y, por este motivo, pueden poner a otros usuarios en riesgo. De hecho, el riesgo global puede ser muy superior al riesgo que asume cualquier persona que haga un uso individual de los servicios informáticos. Por otro lado,*

*la supervisión de los ordenadores por parte de otros miembros de la familia puede contribuir a evitar conductas de riesgo.*

*En muchos aspectos, el ordenador tan sólo aumenta y multiplica los fallos cometidos por los humanos y las limitaciones que deben afrontar durante el resto de sus vidas. La estrategia más extendida y antigua consiste en explotar el instinto sexual de las víctimas, llevándolas a una posición vulnerable para robarles o coaccionarles. El ciberespacio ofrece la posibilidad de automatizar esta conocida estrategia. El fraude es un arte antiguo, pero el ciberespacio proporciona un número mucho más elevado de víctimas, incluso para un solo delincuente. P. T. Barnum dijo que cada minuto nace un tonto nuevo e Internet los conecta entre sí y con quienes pueden convertirlos en víctimas, sin necesidad de interactuar en persona. Además, el ordenador facilita la explotación personal, ya sea en casos en los que un adulto contacta con un menor de edad con fines sexuales o cuando un estafador engaña a personas con quienes no tiene un trato directo. Es incluso útil para encontrar a víctimas inocentes con quienes sí se guarde una relación interpersonal. Consecuentemente, el ciberespacio hace posible tanto los ataques electrónicos como los abusos cara a cara.*

*No resulta nada sencillo modificar la estructura del ciberespacio, pero no debemos descartar ciertos cambios. Actualmente existen técnicas optimizadas para el seguimiento de mensajes y destinadas al cumplimiento de la legislación, a lo que se suman universidades y organizaciones con ingentes cantidades de usuarios que están cada vez más dispuestas a bloquear los ciberataques dirigidos a esos usuarios y a impedirles que hagan uso de los procesos informáticos de estas organizaciones con fines criminales. La protección contra* software *maligno y virus ha ganado terreno a lo largo de los años y la carrera se debate entre los progresos conquistados por los delincuentes y los alcanzados por las víctimas, con cierta ventaja, para ganar esta pugna, de las víctimas o de quienes éstas contratan. Es probable que haya mejorado la supervisión de los adolescentes por parte de los adultos en lo que respecta a su uso de Internet, pero en este caso los adolescentes han ganado terreno en esa particular batalla al haber aprendido a eludir el control de sus padres. Una vez más, la interacción de las relaciones interpersonales y las relaciones cibernéticas es un factor de suma importancia. Los adolescentes que están sometidos a un control mayor pueden encontrar sin problemas a otros adolescentes con limitaciones inferiores y aprovechan la estructura social para vencer los obstáculos impuestos por sus padres.*

*Normalmente, resulta más usual concebir el delito y la ausencia de éste como una dicotomía. Las cuatro categorías de actividades siguientes pueden ayudarnos a comprenderlo mejor: 1) actividades delictivas contra las que trata de luchar el sistema judicial; 2) actividades delictivas que, a pesar de ser ilícitas, gozan de una cierta tolerancia; 3) actividades no delictivas que la sociedad condena tajantemente por norma general; y 4) actividades no delictivas que también están permitidas por la normativa. Podríamos reducir esta clasificación a tres puntos si combinamos las categorías 2) y 3) en una sola: «actividades*

*marginales». Se trata de actividades que bien no son punibles o son legales, pero que la gente sigue tratando de ocultar de los demás. Probablemente, las actividades marginales son mucho más comunes en la sociedad que las de la primera categoría, tanto en la vida personal como en el ciberespacio. De hecho, las actividades marginales son normalmente la antesala de las actividades puramente delictivas englobadas en la última categoría. De este modo, el consumo legal de pornografía expone a las personas al riesgo de cometer actividades delictivas o ser víctimas de ellas. En países en los que la prostitución es legal para personas mayores de edad, Internet puede hacer uso de la prostitución legal fácilmente para hallar clientes de prostitución infantil, y por lo tanto, de prostitución ilegal. Las actividades legales sospechosas pueden encontrar participantes sin problemas hasta en las circunstancias más adversas. Así pues, la vinculación del cibercrimen con un extenso grupo de actividades que podrían no ser más que actividades delictivas marginales o incluso actividades no delictivas en ningún sentido, nos permite hacer grandes avances en esta materia. Este libro proporciona un medio para reflexionar sobre muchas de estas relaciones que, en ocasiones, no son tan evidentes.*

*Una de las características más importantes de esta obra es, por tanto, la asociación de la teoría de la oportunidad del delito con el cibercrimen pero muy especialmente, con la particular arquitectura del ciberespacio (véase capítulo 3). Este análisis estudia la forma en que el tiempo y el espacio funcionan en el ciberespacio y cómo derivan en el crimen transnacional, así como en el uso de redes transnacionales para cometer delitos locales. El autor tiene en cuenta la universalidad y la capacidad de divulgación del ciberespacio y sus múltiples funciones de carácter anónimo. Hace asimismo referencia a la medida en que estos cambios se encuentran abiertos a posibles modificaciones, ya sea de forma permanente u ocasional. A este respecto, el profesor Miró Llinares sugiere ciertos enfoques para la reducción del cibercrimen, teniendo en cuenta la estructura de las actividades cotidianas en la Red. Podríamos concluir que lo más importante de este libro radica en que nos ayuda a* reflexionar *sobre el cibercrimen, al permitirnos conectar ideas sobre la teoría de la oportunidad del delito, incluido el enfoque de las actividades cotidianas, con el uso diario y el abuso de Internet y de los programas de* software *y el* hardware *asociados a éste. El autor vincula la cultura cibernética con lo que sabemos hoy en día sobre el crimen en general y ayuda así a ampliar la criminología, además de responder a una serie de preguntas que los expertos en cibernética se formularán en el futuro.*

*En este libro se presta especial atenció asimismo, a la necesidad de enumerar y clasificar los tipos de cibercrimen, teniendo en cuenta siempre los fenómenos técnicos y sociales. Entre los tipos existentes podemos citar la piratería informática, el uso de código malicioso, el sabotaje interno, el correo basura, el uso no autorizado de redes, los fraudes cibernéticos, la suplantación o usurpación de identidad, el* spoofing*, el ciberespionaje, la ciberextorsión, la ciberin-*

*timidación, el ciberacoso o acoso en línea, el* sexting*, la pornografía infantil y el contenido ilícito, entre otros muchos que son profundamente analizados por el autor.*

*En conclusión, con este libro del profesor Fernando Miró, podremos profundizar significativamente en nuestros conocimientos sobre la vinculación entre el cibercrimen y el amplio mundo de las interacciones interpersonales, comprender la manera en que el cibercrimen se relaciona con la vasta estructura de la vida cotidiana y, así, ayudar a prevenirlo.*

Marcus FELSON
Texas State University
Noviembre de 2012

# PREÁMBULO Y AGRADECIMIENTOS

No sólo los hombres, sino también sus obras, están condicionados por las circunstancias. El presente libro no nació como *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* sino como un trabajo de investigación iniciado en 2008 sobre las reformas penales en relación con la criminalidad en Internet; pero múltiples acontecimientos, así como la vida propia de la obra, desviaron la primera ambición hacia objetivos mayores. Lo que empezó como un proyecto de artículo doctrinal, continuó, como el libro de arena de Borges, extendiéndose hacia el infinito por varios motivos: lo amplio, variado y novedoso que es el fenómeno, lo cambiante que resulta el ciberdelito y la consiguiente actualización permanente de investigaciones o resoluciones jurídicas sobre el mismo, y también debido a la voluntad, adquirida al poco de empezar el trabajo, de adoptar para la consecución de los objetivos de la investigación, no sólo la perspectiva jurídica sino también la criminológica. Por todo ello, la investigación dejó de consistir en el análisis dogmático, con vocación de apoyo hermenéutico, de los delitos que se denominaban «informáticos», y pasó, antes de ello, a ocuparse de la propia comprensión del fenómeno desde la criminología, el saber científico que mejor podía acercarnos a tal entendimiento y que, curiosamente, apenas se había ocupado de este tipo de cibercriminalidad que hoy comparte tiempo, que no espacio, con la delincuencia tradicional.

Las circunstancias, pues, anticipaban una obra de excesivo tamaño y con dos partes claramente separables que, pese a conformar conjuntamente la visión deseada de la problemática de la delincuencia realizada en el nuevo ámbito de intercomunicación social que es el ciberespacio, merecían un tratamiento individualizado propio de cada saber para evitar restricciones y limitaciones de descripciones y argumentos logrando, así, cumplir el objetivo final de comprender esta nueva forma de delincuencia y valorar la eficacia de las técnicas de prevención actual de la misma, entre ellas, la derivada de la propia tipificación de nuevos delitos o de la adaptación interpretativa de los existentes a las nuevas modalidades comisivas en el ciberespacio.

El presente libro, pues, constituye el primero de los dos con los que trataré de abarcar los objetivos reseñados, y se centra en el análisis del fenó-

meno del ciberdelito y en la comprensión, a través del saber criminológico, de sus caracteres diferenciadores de la delincuencia cometida en el espacio físico en aras a la mejor prevención del mismo. Se trata, por consiguiente, de una obra autocomprensiva en la que se abarca el estudio de una delincuencia cuyo rasgo definitorio y diferenciador es el de realizarse en otro espacio/ámbito distinto a aquél en el que siempre se habían ejecutado las infracciones penales. Como acontecimiento social que es el crimen, el lugar en el que el mismo se comete incide claramente en tal evento y, por ello, lo hace en el sujeto que comete el delito, en las personas victimizadas, y por todo, en las posibilidades de prevención de tal forma de delincuencia. Comprender todo ello, o acercarnos, al menos, a tal logro, es el objetivo esencial de esta obra.

Especialmente relevantes para el desarrollo de esta obra fueron las estancias de investigación que durante cuatro años pude ir haciendo en dos universidades que, alternativamente, fueron brindándome la posibilidad de acceder a las fuentes así como centrarme en la investigación con la comodidad que da el trabajar en una universidad extraña pero amiga. Las universidades de Texas at San Antonio y Navarra se han convertido durante los últimos cuatro años en refugios para la investigación a los que acudía no tanto como deseaba. Quiero agradecer a Roger Enríquez, director del Departamento de Criminal Justice de la UTSA, y a Pablo Sánchez Ostiz y a Elena Íñigo del Área de Derecho penal de la Unav, no sólo las invitaciones a sus universidades sino su amistad y la dedicación y el cariño con el que siempre me acogieron, así como las facilidades que me prestaron para acceder a los recursos bibliográficos. También debo mencionar que las últimas estancias en la UTSA, donde cerré definitivamente el trabajo, fueron posibles gracias a la concesión de un proyecto de investigación sobre la cibercriminalidad financiado por el Ministerio de Educación y Ciencia[1].

Al fin y al cabo, es indudable que entre las circunstancias que condicionan un libro tienen siempre especial valor las personas que lo han hecho posible. A ellas dedico unas últimas líneas para agradecerles su ayuda. Junto a los citados tiene un papel destacado Miguel Olmedo, amigo y compañero cuyo cariño y consejo me acompañan siempre que los necesito; Íñigo Ortiz de Urbina y Ramon Ragués que, especialmente el primero, me animaron a publicar en esta brillante colección de la editorial Marcial Pons a la que también agradezco su trabajo editorial; también las personas que conforman conmigo el equipo decanal de la Facultad de Ciencias Sociales y Jurídicas de Elche al que entré a finales de 2011, que, con su trabajo, hicieron más fácil el mío y me permitieron finalizar al fin esta tarea; y por supuesto los integrantes del Centro de Investigación Crímina, entre otros, Rebeca, Natalia, Zora, Mar, Araceli, etc., que con su día a día han compensado para el proyecto

[1] Proyecto de investigación «Cibercriminalidad: Detección de déficits en su prevención jurídica y determinación de los riesgos» (DER2011-26054).

común las ausencias debidas a mi dedicación a este libro. Debo destacar además las lecciones individualizadas de criminología avanzada (además de los primeros libros que, años atrás, comenzaron a marcar mi inclinación hacia tal saber) que me dio Paco Bernabeu, el apoyo incansable plagado de aportes materiales e inmateriales de José Eugenio Medina, y el enorme y excelente trabajo de revisión final del libro que realizó Elena B. Fernández Castejón. Y por supuesto debo agradecer a Marcus Felson su prólogo, todo un honor para mí, así como nuestras conversaciones sobre mi particular visión del cibercrimen y de las actividades cotidianas que fueron el punto de partida de este libro.

Finalmente, y por encima de todo, Esther (y con ella siempre María y Alicia). De nuevo, y después de comprender y afirmar «te has vuelto a meter en un berenjenal», pensó más en mí que en ella y volvió a cargar con el peso de mis repetidas y largas ausencias.

# INTRODUCCIÓN

Aunque han pasado ya más de treinta años desde que comenzó a hablarse de la criminalidad informática, y más de veinte desde que se acuñó el término *cybercrime*, parece que el fenómeno de la criminalidad relacionada con el uso de las Tecnologías de la Información y la Comunicación (en adelante TIC)[1] 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. 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 el mismo supone y en otras no se percibe el riesgo real que el uso de las TIC conlleva. Creo que a nadie escapa la lógica de que esta «novedad» dure tanto: 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.

---

[1] El término TIC es en realidad un acrónimo de Tecnologías de la Información y la Comunicación (o de las comunicaciones, según las variantes). Aunque en ocasiones se usa en plural (TICs), parece más recomendable, siguiendo la regla que recomienda no añadir una «s» a las siglas, realizar el acrónimo como TIC y referirse con los determinantes al carácter plural de las mismas. En la actualidad también se utiliza el acrónimo NTIC, para incluir en el mismo la letra referida a «nuevas» tecnologías, si bien resulta más recomendable usar el término TIC, generalizado ya en muchos ámbitos. En inglés el acrónimo utilizado es ICT, correspondiente a las siglas de «*Information and Communications Technology*». No existe una lista cerrada de elementos que configuran las TIC, sino que más bien con tal categoría se incluyen no sólo los que conforman los modos actuales de sistematización y transmisión de la información, sino también los futuros. En todo caso, se viene admitiendo que se incluyen dentro de las TIC, tanto las redes (entre las cuales destaca Internet pero también se incluyen las de telefonía móvil y otras redes telemáticas), como las terminales (entre las que destacan los sistemas informáticos consistentes en ordenadores personales, pero también comienzan a ser gran vehículo de comunicación las consolas) y los servicios, entre los que destacan todavía la descarga de archivos en sitios de intercambio gratuito y en webs de pago, pero también el comercio electrónico, la banca electrónica, la realización electrónica de actividades relacionadas con la Administración Pública y, cada vez más, las redes sociales. En todo caso, los datos personales y el patrimonio son especialmente, los principales objetos de los servicios en la Red.

En efecto, el desarrollo de todo el conjunto de tecnologías informáticas que empezó en los sesenta y setenta y que tuvo su espaldarazo definitivo con la creación de Internet y su posterior universalización hasta su conversión en el medio de intercomunicación social más importante de la actualidad, no tiene visos de haber firmado sus últimos avances, sino que, más bien al contrario, parece que la rapidez con la que aparecen nuevas tecnologías se ha ido incrementando exponencialmente. Desde luego, lo han hecho los efectos sociales que han acompañado a 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 tal 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 sólo 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[2]. 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»[3] 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 en la palma de su mano, 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 éste a raíz del nuevo aspecto social digno de

---

[2] Resulta reveladora de la implantación de Internet en la sociedad actual, la lectura del informe eEspaña 2011. GIMENO, M. (dir.), «eEspaña, Informe anual sobre el desarrollo de la sociedad de la información en España, Fundación Orange». En Internet, en *http://www.informeeespana.es/docs/eE2011.pdf* (última visita el 11 de junio de 2012).

[3] Aunque el término *Digital natives* fue usado por primera vez por Marc PRENSKY en su obra de 2001 *Digital Natives, Digital Immigrants,* ha sido recientemente cuando más ha comenzado a acuñarse el término para referirse a la generación nacida con la implantación global de Internet. Véase al respecto, MANAFY, M., y GAUTSCHI, H., *Dancing with digital Natives: Staying in step with the generation that's transforming the way business is done,* Medford, New Jersey, Cyberage Books, 2011.

protección o la nueva tecnología que facilitará o modificará la forma de la comisión del delito.

Porque 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, cuando 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.

Obviamente esta 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 usando sólo 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 ge-

neralizado 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 servicio, de infecciones de *malware* u otros que pueden llegar, como ha sucedido, a paralizar la actividad de importantes instituciones de un país.

Con lo afirmado hasta el momento estoy resaltando ya una idea importante que pretende defenderse en este libro: la del carácter omnicomprensivo, a todo lo ejecutado en el ciberespacio, del cibercrimen. Es decir, que, frente a la primera visión que ofrecía la criminalidad informática de ser una modalidad de delincuencia muy específica, relacionada con concretas tecnologías y con reducidos usos de la misma, hoy la única visión posible, por funcional, sobre la cibercriminalidad es la de una delincuencia amplia, variada y cambiante que ni puede asociarse a una concreta tecnología o a un específico grupo de sujetos, ni limitarse a un concreto sector de la actividad social. Por el contrario la cibercriminalidad es hoy toda la criminalidad cometida en el nuevo espacio, al igual que la delincuencia tradicional es toda la ejecutada en el viejo. Es el lugar, en este caso el «no lugar», el que define y marca los eventos sociales en él realizados y el que, por tanto, configura también como distinta la delincuencia en él ejecutada. Y es ese ámbito y su carácter novedoso y cambiante lo que puede explicar la anteriormente comentada sensación de «novedad perpetua» que parece asociada al cibercrimen y puede ayudar a comprender, además, el reto político criminal al que nos enfrentamos: el de adaptar todas las estructuras políticas, jurídicas y sociales a la necesidad de protección de nuevos y viejos intereses frente a nuevas formas delictivas que son cambiantes porque lo sigue siendo el ámbito social en el que las mismas se producen.

También puede servir esta idea de que el cibercrimen no es más, ni menos, que el delito cometido en «el otro lugar», en el ciberespacio, para argumentar la perspectiva que he querido adoptar para realizar este trabajo: frente a la visión de análisis (que se ha dado desde los teóricos de la seguridad informática) del fenómeno del cibercrimen desde una perspectiva técnica, esencialmente descriptiva de los efectos (en los sistemas y en las redes) y de las causas (en términos informáticos) de los distintos ciberataques, es esencial adoptar una visión criminológica de la ciberdelincuencia en la que se analice la misma como lo que es, un evento social ejecutado por personas, individual-

mente o en grupo, con efectos sobre otras personas o instituciones sociales y ejecutado en un nuevo ámbito de intercomunicación social que incide en las conductas, quienes las realizan, sus efectos y en quienes sufren éstos.

Convertir el cibercrimen, como en parte se ha pretendido, en un evento irremediable en el que no nos preguntamos por su origen, por las causas del mismo, por quién y por qué lo realiza, difícilmente nos ayudará a la prevención completa y real del fenómeno. Del mismo modo, y como se verá con especial significación, eliminar de la ecuación del ciberdelito a la víctima supone obviar que en las conductas que ella realice, en la incorporación a sus actividades cotidianas de usos seguros de interacción con ese nuevo mundo al igual que se tienen en el espacio físico, estará en gran parte la superación de este momento actual en el que el cibercrimen parece crecer irremediablemente.

El presente libro debe enmarcarse, por tanto, en el interés por afrontar ese reto, por comprender el fenómeno de la cibercriminalidad desde su consideración como eventos sociales definidos legalmente como delitos, por entender las implicaciones que el mismo conlleva para toda la sociedad, y, por supuesto, por tratar de aprender nuevas estrategias para la prevención de esa delincuencia en el ciberespacio. Por eso la división en dos partes de la presente obra es más una declaración de intenciones de incorporar el análisis criminológico a la visión del cibercrimen, que una separación real.

En los dos primeros capítulos, que conforman la parte titulada «Fenomenología del cibercrimen», se define la cibercriminalidad, configurando, primero, la categoría en su significado más amplio, y tratando de situar y clasificar después todas las modalidades de cibercrímenes existentes en la actualidad. En esa primera parte, sin embargo, ya se adopta la visión criminológica dado que frente a las sistematizaciones habituales de los ciberdelitos que o bien se basan en elementos fácticos de poca utilidad (ataques a sistemas frente a ataques a datos, o clasificaciones similares), o bien lo hacen a partir de consideraciones jurídicas sobre los intereses afectados por los comportamientos criminales, se realizan dos clasificaciones de los ciberdelitos, una más fenomenológica en la que se diferencia según la incidencia de las TIC en la conducta criminal, y otra ya criminológica en la que se atiende a la intención del ciberdelincuente para clasificar los distintos delitos en aras a una mejor identificación de las posibles estrategias de prevención.

La segunda parte del libro está dedicada ya íntegramente al análisis criminológico del ciberdelito, con la intención de identificar los caracteres del nuevo espacio de riesgo delictivo y de los sujetos de esta nueva forma de criminalidad. La hipótesis de partida, como ya se ha dicho, es que el ciberespacio constituye un nuevo, distinto, ámbito de riesgo delictivo, por lo que a partir de la propia identificación de los caracteres configuradores del ciberespacio se tratará de comprender ese nuevo evento que es el cibercrimen. A esto se dedica el tercer capítulo, esencial en la argumentación que supone la obra, que tra-

ta de definir el ciberespacio como un nuevo (en el sentido de distinto) ámbito de oportunidad criminal cuya comprensión resulta esencial para la prevención del ciberdelito. De hecho, el citado capítulo III termina con el intento de desarrollar las teorías de la prevención situacional, que tanto éxito han tenido en la prevención urbana de la delincuencia y que han dado lugar a la geografía criminal, al ámbito definido como el «no lugar», el ciberespacio. Y es que si bien se ha realizado una completa revisión de la literatura criminológica sobre la delincuencia en Internet, el estudio presta especial atención a todos aquellos trabajos que se aproximan al cibercrimen desde la óptica de la teoría de las actividades cotidianas en particular, y de las teorías de la oportunidad en general. La razón es la especial importancia que las teorías del crimen otorgan, para la explicación del delito, al ámbito en el que el mismo se produce, lo cual las habilita especialmente para valorar en qué medida el ciberdelito será distinto, por dónde se produce, al delito cometido en el espacio físico.

El estudio criminológico, como no podía ser de otra forma, integra también la revisión de los principales avances sobre el *profiling* de cibercriminal y cibervíctima, en aras a estar en disposición de comprender mejor el riesgo criminal en el ciberespacio. Pese a la dificultad que conlleva intentar hacer una perfilación criminal y victimal de la delincuencia en Internet (derivada tanto de la variedad de delitos de distinta naturaleza que abarca la macrocategoría, como de la numerosa cantidad de estudios al respecto, no todos ellos con el rigor metodológico que debiera exigirse), se intenta, en los dos capítulos finales del libro, discutir algunos de los tópicos comúnmente aceptados al respecto del ciberdelito, y retratar, en la medida de lo posible, la variedad de perfiles de cibercriminal y cibervíctima que están surgiendo a la luz de Internet.

En los tipos de criminales, de víctimas, y de comportamientos ilícitos en el ciberespacio, es obvia la imposibilidad de lograr la total sincronía de las descripciones y categorizaciones realizadas en este trabajo. Desde el mismo momento de su publicación el libro estará desactualizado, pues es tanta la velocidad de mutación del ciberespacio que durante el tiempo que tarda la edición ya habrán surgido nuevas formas de conducta criminal, nuevos intereses sociales dignos de tutela, así como variados artículos de investigación que intenten aportar luz sobre todo ello. Y esto pese a que he tratado de ser lo más exhaustivo posible en las fuentes y de incorporar todas las formas de comportamiento «desviado» en el ciberespacio existentes hasta el momento de finalización del libro.

En todo caso el que esto sea así demuestra, una vez más, la necesidad de un planteamiento más allá de la mera descripción de las conductas que surgen en Internet y justifica que se haga un análisis global del mismo pese a las evidentes diferencias existentes entre muchos de los delitos ejecutados en el ciberespacio. Sólo mediante una comprensión global del fenómeno que identifique los caracteres comunes del evento criminal cometido en Internet podremos mejorar la prevención de «la otra delincuencia del siglo XXI».

# CAPÍTULO I

# LA CRIMINALIDAD EN EL CIBERESPACIO: LA CIBERCRIMINALIDAD

## 1. ACERCA DE LOS CONCEPTOS CIBERCRIMEN Y CIBERCRIMINALIDAD

La utilización en el ámbito científico de neologismos procedentes de la traducción al castellano de términos de otras lenguas, resulta, en muchos casos, inevitable y, en múltiples ocasiones, arriesgada, dado que generalmente no es posible una identificación completa de sentidos mediante la traducción de términos procedentes de otros idiomas. Quienes en Estados Unidos, Inglaterra, Australia y muchos otros países han tratado, desde muy diversas ciencias sociales, el fenómeno que es objeto de este trabajo, no suelen hablar de *cybercriminality,* ni de *cyberdelinquency,* sino de *cybercrime* [1]*;* en castellano, en cambio, se vienen utilizando, indiscriminadamente, los términos cibercrimen, ciberdelito, cibercriminalidad, ciberdelincuencia [2], en muchos casos para referirse todos ellos a un mismo significado y en otras pretendiéndole otorgar sentidos distintos. A esto hay que unir que en el ámbito jurídico y criminológico se utilizan en España y en otros países de habla hispana otros conceptos, los de criminalidad informática, delito informático, etc.,

---

[1] Se atribuye el primer uso del término *cybercrime* a John Perry BARLOW, teórico de la Sociedad de la información, en general, y de Internet en particular, que en 1990 publica «A Not Terribly Brief History of the Electronic Frontier Foundation». En Internet en *http://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/not_too_brief_history.html* (última visita el 9 de septiembre de 2010); si bien, como señala Brenner, en aquel momento ya debía utilizarse fuera del ámbito académico. BRENNER, S. W., «Cybercrime Metrics: Old Wine, New Bottles?», en *VJOLT*, vol. 9, núm. 13, 2004, p. 2, nota 4. Ya en el ámbito académico son pioneros en la utilización de este término SUSSMAN, V., «Policing cyberspace», en *U.S. News and World Report,* enero, 1995, pp. 54 y ss.; y HEUSTON, G. Z., «Investigating the Information Superhighway: Global Views, local perspectives», en *JCJE*, vol. 2, núm. 6, 1995, pp. 311 y ss. Sobre el término véase más adelante.

[2] Hay autores que suelen redactar las palabras con el prefijo «ciber» añadiendo un guión, o bien en dos palabras, al estilo de cómo se suele hacer con el prefijo *«cyber»* en inglés. Según las normas de formación de palabras en español, a partir del prefijo ciber-, como elemento compositivo de numerosas voces relacionadas con la informática y la realidad virtual, se pueden utilizar como neologismos válidos términos como ciberataque, cibercrimen o cibercriminalidad, siempre que se escriban en una sola palabra y sin guión intermedio.

también procedentes de términos ingleses y alemanes como son respectivamente *computer crime* [3] y *Computerkriminalität* [4]*, para* referirse, en muchos casos, al mismo fenómeno al que pretende hacerse referencia cuando se habla de la cibercriminalidad o del cibercrimen.

Antes de analizar las claves criminológicas de un nuevo tipo de delincuencia ejecutada en el ciberespacio, que es el principal objetivo de este trabajo, resulta necesario, por tanto, precisar cuál va a ser el objeto de investigación y ello exige, por los motivos apuntados, la determinación del alcance real de los términos cibercrimen y cibercriminalidad. Se analizará así, el tránsito del primer uso de los conceptos relacionados con las tecnologías informáticas a los directamente concernientes a la evolución de las TIC hacia la configuración del ciberespacio, y se apuntarán los posibles sentidos en que se puede utilizar el término cibercrimen antes de decidirnos por el que se usa en este trabajo.

### 1.1. De la delincuencia informática a la cibercriminalidad: evolución de un término por la evolución del fenómeno

La categoría de los delitos informáticos, como constructo doctrinal que se usó por la doctrina penal alemana y española durante los años setenta, ochenta, noventa y al principio de este nuevo siglo, y que sigue usándose por parte de la doctrina, no se concibió por quienes lo utilizaban en el sentido de grupo autónomo de infracciones penales con caracteres sistemáticos, o de contenido material de protección, homogéneos que exigirían una metodología distinta al resto de grupos o de una valoración político-criminal común al tutelar intereses sociales de idéntica naturaleza [5]. De acuerdo con la caracterización de delitos informáticos, tanto por el medio utilizado, como por el objeto sobre el que recaía el ataque [6], que conllevaba que formasen parte de

---

[3] En el ámbito anglosajón, y como recuerda Brenner, es clásico el libro de PARKER, D. B., *Crime by Computer*, New York, Charles Scribner's Sons, 1976; véase, BRENNER, S. W., «Cybercrime...», *op. cit.*, p. 2, nota 4. Posteriormente, y con más repercusión en nuestro ámbito, también debe mencionarse PARKER, D. B., *Fighting Computer Crime,* New York, Charles Scribner's Sons, 1983.

[4] En Alemania, y para su ámbito de influencia, el pionero fue, sin lugar a dudas, SIEBER con sus primeras monografías *Computerkriminalität und Strafrecht,* Köln/Berlin/Bonn/München, Carl Heymanns, 1980 (2.ª ed.); y SIEBER, U., *The international handbook on Computer Crime*, Chichester, John Wiley and Sons, 1986. En España, pionero en la materia fue ROMEO CASABONA con *Poder informático y seguridad jurídica. La función tutelar del Derecho penal ante las nuevas tecnologías de la información,* quien, sin embargo, ya se mostraba en esa obra reacio a hablar de delito informático. ROMEO CASABONA, C. M., *Poder informático y seguridad jurídica. La función tutelar del Derecho penal ante las nuevas tecnologías de la información,* Madrid, Fundesco, 1988, p. 28.

[5] En este sentido, por todos, ROMEO CASABONA, C. M., *Poder informático..., op. cit.,* p. 41.

[6] La premisa de que hay delitos informáticos por razón del medio y delitos informáticos por razón del objeto, es aceptada de forma generalizada por la doctrina. Así véase MATA Y MARTÍN, R. M., *Delincuencia informática y Derecho penal,* Madrid, Edisofer, 2001, p. 23. Véase también en este sentido González Rus, quien distingue entre ilícitos patrimoniales contra elementos informá-

la misma tanto aquellos comportamientos delictivos realizados a través de procesos electrónicos [7], como aquellos otros delitos tradicionales que recaían sobre bienes que presentaban una configuración específica en la actividad informática, o bien sobre nuevos objetos como el *hardware* y el *software* [8], difícilmente podía decirse que los tipos que la conformaban tuvieran problemas dogmáticos idénticos o, cuanto menos, distintos a los de otras figuras delictivas. Tampoco la doctrina se empeñaba en buscar algún tipo de identidad de bienes jurídicos en todos los delitos económicos. Siguiendo la categorización de Sieber [9], el patrimonio y el orden económico [10], bienes personalísimos como la intimidad o la libertad sexual, y otros bienes supraindividuales o difusos, se consideraban protegidos por «los delitos informáticos».

La categoría de los delitos informáticos, o quizá mejor, de la criminalidad o delincuencia informática [11], no definía un bien jurídico protegido común a

---

ticos, bien sean físicos o *hardware*, o de naturaleza lógica o *software*, cuando éstos son el objeto material de la conducta, e ilícitos patrimoniales cometidos por medio del sistema informático, en los cuales el sistema informático es el medio a través del cual se lleva a cabo el comportamiento lesivo de lo patrimonial. González Rus, J. J., «Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», en *PJ, número especial IX,* 1989, p. 40.

[7] Corcoy Bidasolo, M., y Joshi, U., «Delitos contra el patrimonio cometidos por medios informáticos», en *RJC,* Barcelona, núm. 3, 1988, p. 134. Bueno Arús, F., «El delito informático», en *AIA,* núm. 11, abril de 1994, p. 2. Partiendo del medio utilizado, Tiedemann define la «criminalidad mediante computadoras», como «todos los actos, antijurídicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados con el empleo de un equipo automático de procesamiento de datos», Tiedemann, K., *Poder económico y delito,* Barcelona*,* Ariel, 1985, p. 122.

[8] Romeo Casabona, C. M., *Poder informático...*, *op. cit.,* p. 46.

[9] Distingue Sieber tres categorías: Una primera de contenido patrimonial, formada por el fraude informático, espionaje informático y sabotaje informático; una segunda de delitos cometidos por medio de sistemas informáticos contra derechos de la personalidad; y una tercera categoría de delitos informáticos que afectan a bienes supraindividuales o bienes sociales. Sieber, U., *Informationstechnologie und Strafrechtsreform,* Köln/Berlin/Bonn/München, Carl Heymanns, 1985, pp. 14 y 15.

[10] En un principio, la delincuencia informática fue categorizada como delincuencia económica por uno de los principales impulsores de ambas sistematizaciones, Tiedemann, K., *Wirtschaftsstrafrecht und Wirtschaftskriminalität,* vol. 2, Hamburg, 1976, p. 148. Pronto, sin embargo, reconoció el autor otro ámbito de la criminalidad informática, cuando ésta supone una amenaza a la esfera privada del ciudadano. Tiedemann, K., *Poder económico y delito, op. cit.,* p. 122. Lo mismo hizo el principal teórico alemán sobre la categoría, Sieber, quien comienza atribuyendo un esencial contenido económico a estas infracciones, *Computerkriminalität und..., op. cit.,* p. 188, pero pronto amplía los delitos informáticos a los lesivos de la privacidad, *The International Handbook..., op. cit.,* y acaba distinguiendo entre las tres categorías citadas. Algo similar le ocurre en España a Ruiz Vadillo, E., «Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica», en *PJ, número especial IX,* 1989, p. 56, para quien «si partimos por vía de hipótesis de que existe una delincuencia específica informática necesitada de una cierta autonomía, ésta ha de insertarse en el más amplio capítulo de la criminalidad de los negocios», si bien más adelante, el mismo autor considera tres las zonas hacia las que se dirige la delincuencia económica (suponemos que se refiere a la informática): la patrimonial, el espionaje y la intimidad de las personas. Ruiz Vadillo, E., «Tratamiento de la delincuencia informática...», *op. cit.,* p. 57.

[11] Véase, en general, y extensamente, sobre la «cuestión terminológica», Hernández Díaz, L., «Aproximación a un concepto de Derecho penal informático», en De la Cuesta Arzamendi, J. L. (dir.) *Derecho penal informático,* Cizur Menor, Civitas, 2010, pp. 35 y ss., especialmente 42 y ss.

todos ellos, sino más bien un ámbito de riesgo, el que derivaba de la expansión social de la tecnología informática, común a muchos bienes jurídicos cuya tutela completa por parte del legislador parecía requerir una modificación de los tipos penales existentes para su adaptación a las nuevas realidades informáticas o la creación de tipos distintos que respondiesen 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 [12], el sabotaje o daños informáticos, el *hacking* o acceso ilícito a sistemas informáticos, la sustracción de servicios informáticos, el espionaje informático [13], o la piratería informática de obras del ingenio [14]; tipologías de conducta específica que la doctrina penal considera merecedoras

---

[12] Indica GUTIÉRREZ FRANCÉS, M. L., «En torno a los fraudes informáticos en el derecho español», en *AIA,* núm. 11, abril, 1994, p. 7, que conviene no confundir el fraude informático con el delito informático, esto es, la parte con el todo, puesto que aquél no es más que un tipo de delincuencia informática.

[13] Señala Sieber que el espionaje informático (incluyente del hurto de *software*) constituye en el ámbito de la criminalidad por ordenador la segunda forma más frecuente de delito. SIEBER, U., «Criminalidad informática: peligro y prevención» (traducido por Elena FARRÉ TREPAT), en MIR PUIG, S. (comp.): *Delincuencia informática,* Barcelona, PPU, 1992, p. 22. También MÖHRENSCHLAGER, M. E., «El nuevo Derecho penal informático en Alemania» (traducido por Jesús-María SILVA SÁNCHEZ), en MIR PUIG, S. (comp.), *Delincuencia informática*, *op. cit.,* p. 126, incluye dentro del espionaje informático el hurto de *software* o copia no autorizada de programas informáticos.

[14] Recuerda ROMEO CASABONA, C. M., *Poder informático y seguridad..., op. cit.,* p. 45, que la clasificación de SIEBER, U., *Computerkriminalität und Strafrecht, op. cit.,* pp. 39 y ss., había sido utilizada anteriormente por Lampe. Sistematización similar es la de TIEDEMANN, al diferenciar entre manipulaciones, hurto de tiempo, hurto de *software* y espionaje y sabotaje (*Poder económico y delito..., op. cit.,* pp. 122 y ss.). También GUTIÉRREZ FRANCÉS, M. L., «Delincuencia económica e informática en el nuevo Código Penal», en *CDJ,* núm. 11, 1996, pp. 252 y ss., distingue entre infracciones patrimoniales por medios informáticos (incluye la estafa informática y la utilización ilícita de tarjetas electromagnéticas a los efectos del delito de robo con fuerza) y atentados contra la información como bien de contenido económico, entre los que incluye el espionaje informático, el sabotaje informático y el intrusismo informático, y los delitos relativos a la propiedad intelectual, si bien no entra en su estudio porque, a su parecer, estos delitos «no sufren modificaciones de interés en el nuevo Código». Romeo Casabona, aceptando las bases de la clasificación de Sieber, distingue en su estudio entre el fraude informático, las manipulaciones en cajeros automáticos mediante tarjetas provistas de banda magnética, y las agresiones a los sistemas o elementos informáticos, dentro de las cuales incluye el sabotaje informático y las agresiones al soporte material, y la sustracción o copia de bases de datos o de programas, cuyos principales tipos son el espionaje informático y la piratería de programas. ROMEO CASABONA, C. M., *Poder informático y seguridad..., op. cit.,* pp. 46 y ss., y CORCOY BIDASOLO, M., y JOSHI, U., «Delitos contra el patrimonio cometidos...», *op. cit.,* p. 684, incluyen entre la delincuencia económica patrimonial la falsificación de datos, las estafas por computador, el descubrimiento y revelación de secretos, el hurto de *software*, la destrucción de datos y la utilización de sistemas informáticos sin costo. Véanse también enumeraciones similares de ALONSO ROYANO, F., «¿Estado de Derecho o derecho del Estado? El delito informático», en *RGD,* núm. 498, marzo, 1986, pp. 602 y ss., y GONZÁLEZ RUS, J. J., «Tratamiento penal de los ilícitos patrimoniales...», *op. cit.,* p. 40. Sobre las clasificaciones de delitos informáticos llevadas a cabo por los principales autores del ámbito anglosajón y continental, nos remitimos al completo estudio de ROMEO CASABONA, C. M., *Poder informático y seguridad..., op. cit.,* pp. 43 y ss.

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, aunque no por todos [15], la denominación de delitos informáticos por la de cibercrimen y cibercriminalidad en referencia esta vez al término anglosajón *cybercrime* [16], procedente de la unión entre el prefijo *cyber*, derivado del término *cyberspace* [17], 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-* [18]. 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 según Wall, una tercera en la que los delitos están absolutamente determinados por el uso de Internet y las TIC [19]. Esto ha tenido su correlato en el ámbito legal: a

---

[15] Véase, por ejemplo, DE LA CUESTA ARZAMENDI, J. L. (dir.), *Derecho penal informático, op. cit*. En España institucionalmente se prefiere esa denominación para, por ejemplo, la fiscalía delegada en materia de delitos informáticos.

[16] Entre otros, THOMAS, D., y LOADER, B., «Introduction - Cybercrime: Law enforcement, security and surveillance in the information age», en THOMAS, D., y LOADER, B. (eds.), *Cybercrime: Law enforcement, security and surveillance in the information age*, London, Routledge, 2000; y FURNELL, S., «Cybercrime: vandalizing the information society», en *LNCS,* vol. 2722, 2003, p. 333, donde señala que el crimen informático no anticipaba el riesgo que conllevaría la generalización del uso de estas tecnologías que ha supuesto Internet.

[17] Conviene recordar que el prefijo *cyber* proviene a su vez del término *cyberspace* creado por el novelista de ciencia ficción William GIBSON y su obra *Neuromancer,* Ace Books, New York, 1984 (en España, traducida *Neuromante),* en la que el autor describía una sociedad tecnológicamente avanzada en la que las personas accedían a un mundo virtual separado del mundo real.

[18] SMITH, R. G.; GRABOSKY, P., y URBAS, G., *Cyber criminals on trial,* Cambridge, Cambridge University Press, 2004, p. 5.

[19] WALL, D., *Cybercrime: the transformation of crime in the information age*, Cambridge, Polity Press, 2007, pp. 44 y ss. La diferencia entre la segunda y la tercera generación de cibercrímenes estaría en que en la primera, Internet se convierte en una oportunidad para la comisión de infracciones tradicionales, mientras que la tercera englobaría a aquellas infracciones que no se pueden cometer sin la existencia de Internet. A mi parecer es una diferencia de matiz interesante, y desde luego, creo que es fácilmente reconocible la distinción entre la primera y la segunda generación al existir un antes y un después de la aparición de Internet como forma de división,

partir del nuevo siglo empezaron a preocupar ya no sólo 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 [20]. Y todo ello ha llevado a la utilización de un término, el de cibercrimen que, a mi parecer, logra englobar todas las tipologías de comportamientos que deben estar, y además alcanza mejor que otros el que debe ser un propósito esencial de cualquier concepto que sirve para nombrar a una categoría [21]: enfatizar aquello que une a todo lo que la conforma que, en este caso, es Internet y las TIC como medio de comisión delictiva [22].

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 [23], 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 estos comportamientos están unidos en la actualidad a redes telemáticas, con los particulares problemas político-criminales que ello plantea en la actualidad. Además, al tener en cuenta no sólo 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

---

criminológica, entre la criminalidad informática y la cibercriminalidad que ha acabado por abarcar la primera.

[20] Clough, J., *Principles of Cybercrime,* Cambridge, Cambridge University Press, 2010, p. 4.

[21] Yar, M., «The novelty of "cybercrime": an assessment in light of routine activity theory», en *EJC,* núm. 2, 2005, p. 409.

[22] Clough, J., *Principles of Cybercrime, op. cit.,* p. 9.

[23] Hernández Díaz, L., «Aproximación a un concepto de Derecho penal informático», *op. cit.,* p. 44. Señala además la autora que mientras que todo lo que es cibernético o telemático es también informático, no ocurre lo mismo en sentido inverso, siendo por tanto mucho más omnicomprensiva esta última categoría. Tal afirmación es algo interesada: podría discutirse la veracidad de la afirmación de que no todo lo que es cibernético es informático, pero ¿quién ha dicho que tenga que serlo? Lo importante es si el término cibercrimen, o cibercriminalidad, abarca todas las infracciones en las que hay una misma problemática penal, y lo mismo ocurre con el término delito informático o delincuencia informática. En ese sentido, creo que ambos términos son prácticamente igual de «omnicomprensivos», pero que, en cambio, y como se dice en el texto, el de cibercrimen sirve para identificar socialmente de forma más adecuada todas las nuevas conductas criminales surgidas en Internet, así como las problemáticas que las mismas plantean para el sistema penal. Además, y como ha señalado Clough, J., *Principles of Cybercrime, op. cit.,* p. 9, tampoco es desdeñable el argumento de que el único convenio a nivel internacional que abordó de forma completa el fenómeno, utilizaba el término cibercriminalidad (Convenio de Budapest del Consejo de Europa de 2001). También parece preferir el término ciberdelincuencia, frente al de crimen informático, Quintero Olivares, G., «Internet y Derecho penal. Imputación de los delitos y determinación de la competencia», en *LL,* núm. 37, enero, año IV, abril de 2007, p. 6.

redes telemáticas o con la introducción y mala utilización de los contenidos introducidas en ellas. En todo caso, y derivando la relevancia de la «cuestión terminológica» de la importancia de los términos para la transmisión de significados, creo que no debe desdeñarse el hecho de que hoy en día es el término Internet, y en relación con él el término ciberespacio y el prefijo ciber- como castellanización de *cyber*, los que reflejan socialmente, mucho mejor que el término «informático», algunas conductas delictivas. Así, el acoso sexual por Internet, el acoso a menores realizado en la Red o por medio de los *smartphones*, y la instigación al delito terrorista en el entorno virtual entre otros, parecen encajar mucho más con la idea de «lo cibernético» que con la de «lo informático». Y lo mismo sucede con los problemas de anonimato, transnacionalidad y otros que derivan más que del hecho de que se utilice para la comisión de la infracción una terminal informática, de que todas las terminales interaccionan en un nuevo espacio virtual universal.

### 1.2. El cibercrimen: sentidos tipológico y normativo, concepciones amplia y restringida, y relación con el término cibercriminalidad

Explicada la preferencia por el término cibercrimen, resulta necesario afrontar el problema de su definición. Gran parte de la confusión que deriva del uso de este término se debe, sin embargo, a que no existe un único concepto de cibercrimen, ni un único sentido en el que se puede utilizar el mismo. A ello hay que unir que junto a él, aparece otro término, el de cibercriminalidad, que unas veces parece un sinónimo y otras un concepto distinto al de cibercrimen. Para tratar de comprender mejor el fenómeno de la cibercriminalidad y los caracteres del cibercrimen, es necesario precisar la relación entre ambos conceptos, lo cual exige, a su vez, distinguir los sentidos con que se pueden usar los mismos y las ventajas de uno u otro uso.

Pues bien, a nadie se le escapa el carácter polisémico del término delito. Cuando se utiliza el mismo, se puede hacer referencia bien a una figura delictiva incluida en una determinada ley y que permite sancionar todo un conjunto de comportamientos (el delito como hecho típico, antijurídico, culpable y punible), bien a un hecho personal concreto que merece tal calificación, generalmente, al entrar en el ámbito del primero. El delito en sentido normativo y el delito en sentido tipológico, como hecho concreto con relevancia social. A partir de aquí, pues, hay que reconocer que podemos utilizar el término cibercrimen para referirnos a un comportamiento concreto que reúne una serie de características criminológicas (también podrían ser legales) [24] relacionadas con el ciberespacio (sentido tipológico), o para tratar de

[24] Y aquí habría que hacer una nueva diferenciación a partir de si se está utilizando un concepto legal de delito o un concepto criminológico que vaya más allá del primero. No es el lugar para plantear estas cuestiones, bien resueltas, a mi parecer, por SERRANO MAÍLLO, A., *Introducción a la criminología*, 6.ª ed., Madrid, Dykinson, 2009, pp. 68 y ss., especialmente 76 y ss.; limitándome por

identificar un tipo penal concreto con un presupuesto y una sanción, que pretende prevenir la realización de conductas en el ciberespacio que afectan a bienes jurídicos dignos de protección (sentido normativo). En el primer caso, el término cibercrimen describiría conductas como la consistente en acceder ilícitamente a un sistema informático ajeno, o la del adulto que propone a través de Internet un contacto con un menor con la intención de consumar posteriormente un abuso sexual. En el segundo, el término cibercrimen describiría tipos penales como el del nuevo art. 197.3 que sanciona el acceso informático ilícito, o el del art. 183 bis que castiga el denominado *online child grooming*.

Evidentemente ambos sentidos, tipológico y normativo, son aceptables, y será el contexto el que nos determine que estamos utilizando uno u otro. Cuestión distinta es, en cambio, la de si tiene alguna utilidad la configuración del cibercrimen como una categoría en sentido normativo, como un conjunto de delitos del CP caracterizados por llevarse a cabo en el ciberespacio, o únicamente la tiene su construcción como una categoría tipológica (o criminológica) que incluya todas las modalidades (o algunas de ellas, según veremos) de comportamientos delictivos en el ciberespacio. Si bien ambas categorías podrían desempeñar su función, considero que, al igual que ocurría con la de los delitos informáticos, la categoría del cibercrimen, más que por dar nombre a un grupo de tipos penales [25], resulta útil como categoría de base criminológica que sirve como referencia de un ámbito de riesgo que incluiría a todas las tipologías de comportamientos que utilicen la Red para la realización de comportamientos que atenten contra bienes considerados esenciales [26] y que, en todo caso, puede posteriormente ser comparada con la categoría normativa en aras a descubrir si los tipos penales dan o no una respuesta adecuada al problema criminológico del delito en el ciberespacio. El cibercrimen (o la cibercriminalidad, como después precisaré), cumple su función principal, por tanto, con la descripción y sistematización de las nuevas formas de afectación de los bienes más importantes en el ámbito de las tecnologías de la información y la comunicación, y, a partir de ahí, la valoración de las soluciones político-criminales adoptadas frente a las mismas, partiendo de la revisión de los tipos penales existentes y de la necesidad (o

---

tanto a señalar que dentro de ese concepto débil de cibercrimen hay que tener en cuenta que se utiliza el término crimen también en sentido débil.

[25] El que el cibercrimen no corresponda a una categoría legalmente establecida no es propio sólo de España, sino de todo el mundo. YAR, M., *Cybercrime and society,* London, Sage, 2006, p. 9.

[26] En sentido similar Romeo Casabona, quien señala que el término cibercrimen no puede llegar a satisfacer plenamente una función dogmática de integración de estos delitos de nueva generación, pero sí descriptiva de identificación de un fenómeno criminal. ROMEO CASABONA, C. M., «De los delitos informáticos al cibercrimen: una aproximación conceptual y político criminal», en ROMEO CASABONA, C. M. (coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Granada, Comares, 2006, p. 8.

no) de modificación de los mismos. Las necesidades de intervención político-criminal frente al cibercrimen, sin embargo, no se agotan en la tipificación de nuevos preceptos penales, sino que las peculiaridades criminológicas y la incidencia de esa amenaza real en múltiples aspectos sociales es tal, que más importante que la correcta política legislativa sustantiva nacional, es la adaptación de las estructuras procesales y técnicas necesarias, especialmente a nivel internacional, para la prevención de su realización y la mejor investigación procesal de las mismas.

El cibercrimen, pues, se utilizará generalmente 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 se exigirá 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; 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 utilizado en este ámbito, el de cibercriminalidad. Éste no tiene sentido normativo, sino únicamente tipológico, como categoría criminológica que englobaría 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 ese 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». Creo que en ambos casos el uso es correcto y que el contexto permite diferenciar uno u otro sentido, por lo que esto es lo que sucederá en este libro que, de hecho, se titula «El cibercrimen» otorgando al término un sentido idéntico al que tendría el de «La cibercriminalidad».

Más relevante es, en cambio, la cuestión de la concepción amplia o restringida del cibercrimen (o de la cibercriminalidad) [27]. Estas dos concepcio-

[27] Que viene a corresponderse con la pretendida distinción entre *cybercrime,* como conjunto de conductas criminales nuevas surgidas en el ciberespacio, y *cyber crime,* que abarcaría las conductas criminales surgidas en el ciberespacio, incluyendo las nuevas formas de realización de conductas criminales digamos «convencionales», SMITH, R. G.; GRABOSKY, P., y URBAS, G., *Cyber criminals on trial, op. cit.,* p. 6.