El cibercrimen

Fenomenología y criminología de la delincuencia en el ciberespacio

Fernando Miró Llinares

Derecho penal & Criminología

Marcial Pons

Colección

Derecho penal y Criminología

Directores
Íñigo Ortiz de Urbina Gimeno
Ramon Ragués i Vallès
Luis Greco

EL CIBERCRIMEN

Fenomenología y criminología de la delincuencia en el ciberespacio

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

La colección *Derecho penal y Criminología* publica aquellos trabajos que han superado una evaluación anónima realizada por especialistas en la materia, con arreglo a los estándares usuales en la comunidad académica internacional.

Los autores interesados en publicar en esta colección deberán enviar sus manuscritos en documento *Word* a la dirección de correo electrónico *manuscritos@derechopenalycriminologia.es.* Los datos personales del autor deben ser aportados en documento aparte y el manuscrito no debe contener ninguna referencia, directa o indirecta, que permita identificar al autor.

Puede encontrarse más información sobre la colección en la página web *www.derechopenalycriminologia.es.*

© MARCIAL PONS
EDICIONES JURÍDICAS Y SOCIALES, S. A.
San Sotero, 6 - 28037 MADRID
☎ (91) 304 33 03
www.marcialpons.es

ISBN: 978-84-91233-87-9

A María Miró, Alicia Miró, Esther Sitges
y Cristina Llinares.
A quienes conforman Crímina.
A mis amigos de La Universidad.

«Tlön será un laberinto, pero es un laberinto urdido por hombres, un laberinto destinado a que lo descifren los hombres. El contacto y el hábito de Tlön han desintegrado este mundo. Encantada por su rigor, la humanidad olvida y torna a olvidar que es un rigor de ajedrecistas, no de ángeles [...]. Una dispersa dinastía de solitarios ha cambiado la faz del mundo. Su tarea prosigue. Si nuestras previsiones no erran, de aquí a cien años alguien descubrirá los cien tomos de la segunda enciclopedia de Tlön. Entonces desaparecerán del planeta el inglés y el francés y el mero español. El mundo será Tlön».

(Jorge Luis BORGES, *Tlön, Uqbar, Orbis Tertius*).

«Cuando se proclamó que la biblioteca abarcaba todos los libros, la primera impresión fue de extravagante felicidad. Todos los hombres se sintieron señores de un tesoro intacto y secreto. No había problema personal o mundial cuya elocuente solución no existiera en algún hexágono. El universo estaba justificado, el universo bruscamente usurpó las dimensiones ilimitadas de la esperanza».

(Jorge Luis BORGES, *La biblioteca de Babel*).

«Por lo demás, el problema central es irresoluble: la enumeración, siquiera parcial, de un conjunto infinito. En ese instante gigantesco, he visto millones de actos deleitables o atroces; ninguno me asombró como el hecho de que todos ocuparan el mismo punto, sin superposición y sin trasparencia».

(Jorge Luis BORGES, *El Aleph*).

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.

ABREVIATURAS

ABS	*American Behavioral Scientist*
ACM	*ACM Transactions on Computer Systems*
ACT	*Advances in Criminological Theory*
AERJ	*American Educational Research Journal*
AFD	*Anuario de Filosofía del Derecho*
AGP	*Archives of General Psychiatry*
AGUC	*Anales de Geografía de la Universidad Complutense*
AHR	*The American Historical Review*
AIA	*Actualidad Informática Aranzadi*
AIPPI	Asociación Internacional para la Protección de la Propiedad Industrial e Intelectual
AJC	*Asian Journal of Criminology*
AJPM	*American Journal of Preventive Medicine*
ANNALS	*The ANNALS of the American Academy of Political and Social Science*
APs	*American Psychologist*
APSACA	*American Professional Society on the Abuse of Children Advisor*
ART	*Argumentos de Razón Técnica*
ASR	*American Sociological Review*
AT	*Anthropological Theory*
ATC	*Arresting Transnational Crime*
BIR	*Business Information Review*
BJP	*British Journal of Psychiatry*
BJS	*Bureau of Justice Statistics*
BP	*Boletín de Psicología*
CDJ	*Cuadernos de Derecho judicial*
CFS	*Computer Fraud & Security*
CGPJ	Consejo General del Poder Judicial
CHTLJ	*Computer & High Technology Law Journal*
CICJ	*Current Issues in Criminal Justice*
CJB	*Criminal Justice and Behavior*
CJR	*Criminal Justice Review*
ClP	*Clinical Pediatrics*
CLSC	*Crime, Law and Social Change*
CLSR	*Computer Law & Security Review*
CP	Código Penal
CpB	*Cyberpsychology & Behavior*

CPC	*Cuadernos de Política Criminal*
CPS	*Crime Prevention Studies*
DB	*Deviant Behavior*
DLTR	*Duke Law & Technology Review*
DN	*Detroit News*
Eguzkilore	*Eguzkilore: Cuaderno del Instituto Vasco de Criminología*
EJC	*European Journal of Criminology*
EJMF	*Estudios Jurídicos. Ministerio Fiscal*
EREL	*Espéculo. Revista de estudios literarios*
ERS	*Ethnic and Racial Studies*
FMPRJI	*First Monday Peer-Reviewed Journal on the Internet*
FP	*Federal Probation*
FSULR	*Florida State University Law Review*
GC	*Global Crime*
GMC	*Global Media and Communication*
HCLQ	*Hastings Constitutional Law Quarterly*
IC3	*Internet Crime Complaint Center*
ICS	*Information Communications and Society*
ICT	*Information and Communications Technologies*
IDP	*Revista d'Internet, Dret i Política*
IeJCS	*International e-Journal of Criminal Science*
IJCC	*International Journal of Cyber Criminology*
IJCSIS	*International Journal of Computer Science and Information Security*
IJEC	*International Journal of Electronic Commerce*
IJLIT	*International Journal of Law and Information Technology*
IJPPT	*International Journal of Psychology and Psychological Therapy*
INTECO	Instituto Nacional de Tecnologías de la Comunicación
IP	Internet Protocol
IR	Internet Research
IS	The Information Society
JA	*Journal of Adolescence*
JADP	*Journal of Applied Developmental Psychology*
JAH	*Journal of Adolescent Health*
JBP	*Journal of Behavioral Profiling*
JCPP	*Journal of Child Psychology and Psychiatry*
JCCJ	*Journal of Contemporary Criminal Justice*
JCJE	*Journal of Criminal Justice Education*
JCLC	*Journal of Criminal Law & Criminology*
JCMC	*Journal of Computer-Mediated Communication*
JILT	*Journal of Information, Law and Tecnology,*
JRCD	*Journal of Research in Crime and Delinquency*
JRCR	*Journal of Retailing and Consumer Research,*
JECM	*Journal of Economic Crime Management*
JFCJ	*Juvenile and Family Court Journal*
JHTL	*Journal of High Technology Law*
JLSP	*Journal of Language and Social Psychology*
JMP	*Journal of Media Psychology*

JRDP	*Justicia. Revista de Derecho procesal*
JSeC	*Journal of Strategic E-Commerce*
JSC	*Journal of Strategic Security*
JSV	*Journal of School Violence*
JTLP	*Journal of Transnational Law & Policy*
LE	*Lex Electronica*
LNCS	*Lecture Notes in Computer Science*
LL	*La Ley Penal. Revista de Derecho Penal, Procesal y Penitenciario*
LQR	*Law Quarterly Review*
MCS	*Media, Culture & Society*
MUEJL	*Murdoch University Electronic Journal of Law*
NCJOLT	*North Carolina Journal of Law & Technology*
NMS	*New Media & Society*
NS	*Network Security*
OECD	Organisation for Economic Co-operation and Development
OJCMT	*Online Journal of Communication and Media Technologies*
ONG	Organización No Gubernamental
PCL	*Psychology, Crime & Law*
PIALP	Pew Internet & American Life Project
PHG	*Progress in Human Geography*
PPR	*Public Policy Research*
PRS	*Police Research Series*
PSJ	*Prison Service Journal*
RAT	Routine Activities Theory
RCVS	*Rivista di Criminologia, Vittimologia e Sicurezza*
RDPP	*Revista de Derecho y Proceso Penal*
RECPC	*Revista Electrónica de Ciencia Penal y Criminología*
RFDUCM	*Revista de la Facultad de Derecho de la Universidad Complutense de Madrid*
RGD	*Revista General de Derecho*
RIDP	*Revista de Internet, Derecho y Política*
RJC	*Revista Jurídica de Catalunya*
SA	*Sexual Abuse*
SJ	*Security Journal*
SJP	*Scandinavian Journal of Psychology*
SLS	*Social & Legal Studies*
SSCR	*Social Science Computer Review*
TAC	Teoría de las Actividades Cotidianas
TIC	*Tecnologías de la Información y la Comunicación*
TJMJCIL	*The John Marshall Journal of Computer & Information Law*
TC	*Tribunal Constitucional*
TCS	*Theory, Culture & Society*
TD	*Teoría y Derecho. Revista de Pensamiento Jurídico*
TICCJ	*Trends and Issues in Crime and Criminal Justice*
TOC	*Trends in Organised Crime*
TP	*Teaching of Psychology*
TRLPI	Texto Refundido de la Ley de Propiedad Intelectual
TS	Tribunal Supremo

TSoc.	*Time & Society*
TSR	*The Sociological Review*
VJOLT	*Virginia Journal of Law & Technology*
VJSPL	*Virginia Journal of Social Policy and the Law*
WM	*The Washington Monthly*
WFLR	*Wake Forest Law Review*
WLLR	*Washington and Lee Law Review*
WT	*Washington Times*
WUJLP	*Washington University Journal of Law & Policy*
YS	*Youth and Society*

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».

PRIMERA PARTE

FENOMENOLOGÍA DEL CIBERCRIMEN

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.

nes son aplicables tanto al sentido normativo [28] como al tipológico, pero es en relación con este último donde tal diferenciación adquiere más importancia, dado que sirve, ni más ni menos, para fijar el auténtico objeto de investigación de este trabajo.

Pues bien, si utilizamos el término de forma amplia, podremos definir como cibercrimen cualquier comportamiento delictivo realizado en el ciberespacio, entendiendo además por el mismo el ámbito virtual de interacción y comunicación personal definido por el uso de las TIC, y dando cabida, por tanto, a conductas cuyo contenido ilícito es nuevo y se relaciona directamente con los nuevos intereses o bienes sociales existentes en el ciberespacio, así como también a comportamientos tradicionalmente ilícitos en los que únicamente cambia que ahora se llevan a cabo por medio de Internet. Si, por el contrario, utilizamos el término de forma restringida, y si bien se pueden utilizar variados criterios para restringir la categoría [29], lo usual será acudir a la propia idea de la realización del delito por medio de las TIC. Conforme a esto, estaremos ante un cibercrimen únicamente cuando se trate de un comportamiento delictivo realizado en el ciberespacio cuya esencia de injusto no podría haberse dado de ninguna otra forma fuera de él [30]. El comportamiento de quien acosa sexualmente a un menor por Internet sería un cibercrimen

---

[28] En el sentido normativo podemos incluir dentro de la categoría del cibercrimen, bien cualquier tipo penal que permita ser realizado utilizando las TIC como medio u objetivo comisivo (concepto amplio), o bien sólo aquellos cuya única forma comisiva típica exija la utilización de las TIC (concepto restringido). El delito de acceso informático ilícito sería un cibercrimen, conforme a la concepción amplia, pero no lo sería conforme a la concepción restringida que, sin embargo, sí daría cabida al *child grooming,* puesto que el mismo no puede realizarse sino a través de Internet u otras TIC.

[29] Así ocurre, por ejemplo, con la definición de Romeo Casabona, quien define el cibercrimen como «el conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual», ROMEO CASABONA, C. M., «De los delitos informáticos al cibercrimen...», *op. cit.,* p. 9. La definición de Romeo Casabona no concuerda con una concepción totalmente restringida del cibercrimen, puesto que permite incluir en ella conductas como el espionaje informático, cuyo contenido esencial de injusto puede darse también en otros comportamientos de espionaje llevados a cabo, por ejemplo, por *insiders* que acceden al sistema sin usar las redes telemáticas. Sin embargo está más cerca de esa concepción restringida que de la concepción amplia, pues al utilizar una descripción de conductas tan estricta como «acceso, apropiación, intercambio y puesta a disposición de información», deja fuera un gran número de tipologías de conductas en las que lo esencial es la dimensión comunicativa y no la relativa a la información como el ciberacoso sexual a menores, el *cyberbullying*, o el *cyberstalking*.

[30] Los que Clough y Wall, en trabajos separados pero coincidentes en lo terminológico, denominan *«the true cybercrimes»,* aunque Clough acabe aceptando una categoría más amplia. CLOUGH, J., *Principles of Cybercrime, op. cit.,* p. 11. Por su parte Wall señala que los auténticos (*true*) cibercrímenes son únicamente aquellos que son producto de las oportunidades creadas por Internet y que sólo pueden ser perpetrados por medio del ciberespacio, refiriéndose a los robos de propiedad intelectual, el envío de *spam* y otras formas de ingeniería social. WALL, D. S., «What are Cybercrimes?», en *CJR,* 2005, p. 59. Aunque creo que coincidimos en la idea de que no cualquier utilización

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

Puede adelantarse aquí que la concepción de cibercrimen seguida en este trabajo es amplia. La explicación del porqué y la precisión final de qué tipologías de conductas en el ciberespacio se incluyen en la categoría ya corresponden al siguiente punto, dedicado al alcance del cibercrimen.

2. EL CIBERCRIMEN: FUNCIONES DE LA CATEGORÍA Y CONCEPCIÓN AMPLIA DEL CIBERCRIMEN

Aunque hay múltiples definiciones de cibercrimen, el aspecto esencial de todas y cada una de ellas se reduce, a mi parecer, y como ya se ha adelantado, a la cuestión de si con la definición se está adoptando una concepción amplia o restringida de la cibercriminalidad, dando cobertura en la categoría a todos o tan sólo a algunos de los comportamientos criminales realizados en el ciberespacio. Es éste, a mi parecer, el aspecto determinante que debe ser tomado en cuenta para valorar una definición (en términos de precisión del concepto en relación con su significado), aunque no siempre el mismo es afrontado explícitamente por los autores y tiene que ser descubierto en cada una de las definiciones. Así ocurre, por ejemplo, con la definición de Yar quien define el cibercrimen como «aquel delito cuya característica esencial es el rol central que las TIC juegan en su comisión»[31]. Aunque en principio, podría parecer que está tratando de restringir el alcance de la categoría, lo hace únicamente en el sentido antes afirmado de incluir sólo aquellas infracciones en las que la utilización de las TIC tiene que ver con el aspecto esencial del delito. En cambio, se trata de una concepción amplia que incluye cualquier comportamiento delictivo llevado a cabo en el ciberespacio, sea el mismo esencialmente nuevo o consista simplemente en la comisión de un injusto tradicional utilizando como nuevo medio comisivo el ciberespacio.

Esta concepción amplia es la que se sigue en esta monografía, y ello debido a la función que se pretende dar a la categoría de referencia como forma de criminalidad que plantea unas nuevas problemáticas, tanto desde una perspectiva criminológica como desde la perspectiva penal, y en aspectos tan importantes como la eficacia de los modelos preventivos, la aplicación

---

de Internet da lugar a un cibercrimen, también creo que con la definición que he aportado aquí se precisa esto de forma más clara.

[31] YAR, M., *Cybercrime and society, op. cit.,* p. 9.

de las normas jurídicas, o la identificación de los criminales, entre muchas otras derivadas de los especiales rasgos de la criminalidad realizada en el ciberespacio. Si es, pues, el mero hecho de que el delito se ejecute utilizando Internet, aquello que dota a la conducta de unos caracteres de riesgo delictivo y de riesgo penal distintos a los de las infracciones penales ejecutadas en el espacio físico-real, entonces debe entenderse, como aquí se hace, que la categoría debe abarcar a todas ellas: sean las infracciones nuevas en su esencia o tan sólo en los medios; sean las TIC el objetivo, el medio o el lugar de ejecución; y sean los bienes jurídicos afectados tan dispares como el patrimonio, la seguridad nacional o la indemnidad sexual de los menores. O en otros términos, si la cibercriminalidad pretende configurarse, en suma, como una categoría criminológica que englobe a todo un conjunto de infracciones con una misma problemática de riesgo y de respuesta penal, bastará con que la conducta, para que sea objeto de esta nueva categoría penal, se lleve a cabo en ese ámbito virtual con dimensiones espacio-temporales distintas, y caracterizado por la transnacionalidad, la universalización del medio y el estar sujeto a revolución permanente, que es el ciberespacio.

Por consiguiente, entiendo por cibercrimen, al objeto de este trabajo, cualquier delito en el que las TIC juegan un papel determinante en su concreta comisión, que es lo mismo que afirmar que lo será cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan [32]. Antes, sin embargo, de sistematizar las distintas tipologías de cibercrímenes que conforman la categoría, hay que hacer una última precisión.

Se trata de reconocer que no todos los comportamientos que vamos a integrar dentro de las diferentes tipologías de cibercrímenes pueden ser reputados delictivos conforme al sistema penal español [33]. Si en última instancia el objetivo es analizar la respuesta penal a las distintas tipologías de conductas que pueden poner en riesgo algunos de los intereses sociales más significativos, resulta lógico realizar un análisis tipológico amplio que se compare posteriormente con el normativo para señalar cuáles de los comportamientos son delictivos y cuáles no. En este libro, se está realizando, por tanto, un estudio criminológico del cibercrimen en el que no se analizan figuras delictivas, sino modalidades de comportamiento. Esto significa que vamos a re-

---

[32] De modo similar, Yvonne Jewkes define el cibercrimen como cualquier acto ilegal cometido por medio de (o con la asistencia de) sistemas informáticos, redes digitales, Internet y demás TIC. JEWKES, Y., «Cybercrime», en MCLAUGHLIN, E. U., y MUNCIE, J. (eds.)., *The Sage Dictionary of Criminology,* London-California, Sage, 2006, p. 106.

[33] Lo cual es general en la categoría que, en algunos casos, como señala JEWKES, Y., «Cybercrime», *op. cit.,* p. 106, llega incluso a incluir comportamientos legales como la lotería en Internet. A mi parecer, la de la ilicitud sí es, como se explicará, una barrera clara que no se puede saltar, aunque en ocasiones haya que plantearse los problemas político-criminales que plantean comportamientos lícitos como algunas formas de envío de *spam* o concretas conductas de distribución de archivos en Internet.

ferirnos a conductas como el envío de *spam* o a algunas concretas formas de *cyberstalking* utilizando el concepto de cibercrimen y, todo ello, pese a que gran parte de las mismas no serían delictivas. Las razones de hacerlo así son varias: la primera es que muchos de los ciberataques, y esto se verá posteriormente, conllevan dinámicas comisivas complejas repletas de pasos previos que en algunos casos podrán ser reputados como tentativas delictivas y en otros no. Es lo que sucede con el *spam*, o con algunas infecciones de *malware* que no causando ningún daño se realizan, en última instancia, como pasos necesarios para el posterior acceso ilícito al sistema o la futura defraudación. En segundo lugar, la presente obra analiza un fenómeno transnacional regulado de forma distinta por muchos Estados que no siempre seleccionan las mismas conductas para su sanción penal, por lo que resulta más adecuada una visión omnicomprensiva de los ciberataques que los incluya a todos sean o no penados. Por último, y desde una perspectiva criminológica, nos interesa el cibercrimen como una categoría amplia en aras a la prevención del mismo, de modo que limitarnos a las conductas que están presentes en el Código Penal actual, resultaría contradictorio con estos objetivos.

CAPÍTULO II

TIPOS DE CIBERCRIMEN Y CLASIFICACIÓN DE LOS MISMOS

1. INTRODUCCIÓN: EL CIBERCRIMEN (LOS CIBERCRÍMENES)

Aceptada la denominación de cibercriminalidad como preferible en la actualidad a la de delincuencia informática, reconocido que la misma sirve esencialmente para definir un ámbito de riesgo particular y específico, el derivado del uso de las TIC, para bienes jurídicos esenciales, y admitido, por último, que tal categoría engloba no tipos penales sino tipologías de conductas peligrosas para dichos bienes y caracterizadas por la utilización de redes telemáticas y demás sistemas, terminales y servicios de las TIC con los riesgos que ello conlleva, es el momento de tratar de sistematizar, sobre la base de los distintos criterios existentes, estas tipologías incardinadas en la cibercriminalidad. La historia del cibercrimen, que evolucionó de los primeros ataques a sistemas informáticos a las últimas formas de ciberterrorismo [1], ha sido tan rápida que nos demuestra que probablemente en esta misma relación estemos obviando algún nuevo comportamiento ilícito ya existente en Internet. Lo relevante ahora es tratar de sistematizar los que hasta el momento conocemos.

La doctrina ha tratado de sistematizar de muy diferentes formas los numerosos comportamientos ilícitos surgidos en el ciberespacio transnacional, popular y en permanente revolución [2]. Esto ya ocurría cuando se utilizaba

---

[1] Véase desde los *white hat hackers* hasta el ciberterrorismo, el análisis de SCHELL, B. H., y MARTIN, C., *Handbook on cybercrime,* Santa Bárbara, ABC-CLIO, 2004, pp. 4 y ss.

[2] Así, una clasificación clásica, entre lo tipológico y lo legal, es la de Wall que diferencia entre *cyber-tresspass; cyber-deceptions and thefts; cyber-pornography;* y *cyber-violence.* El *cyber-tresspass* abarcaría el *hacking/cracking*, y consiste en la intromisión del sujeto en un ámbito del sistema informático donde imperan los derechos establecidos por su propio titular; el término *cyber-deception/thefts* describiría los diferentes tipos de ataque codicioso y englobaría las diferentes formas de fraude en el ciberespacio; *cyper-pornography* abarcaría, evidentemente, todas las infracciones penales relacionadas con la transmisión por Internet de contenidos ilícitos; y, por último, dentro de la categoría de *cyber-violence* se situarían todas las conductas como el *cyberbullying,* el *cyberstalking* o el *hate speech* en las que se causa un daño psicológico, o se incita al mismo, sobre una persona.

la denominación clásica de delitos informáticos. Entonces, la doctrina solía generalmente distinguir entre *computer* (después, Internet) *assisted crimes*, en los que las TIC son el medio que se utiliza para llevar a cabo el ataque, y *computer* (o Internet) *focused crimes*, aquellos en los que se ataca al sistema o a la red informática [3]. Esta sistematización sería equiparable a la que hoy en día se viene aceptando por la mayoría de los teóricos del cibercrimen, y que diferencia entre si el sistema informático es el *«target»* (objetivo), o más bien es la *«tool»* (herramienta) del ataque delictivo [4]. Con ella, en realidad, lo que se pone de manifiesto es que el cibercrimen lo es tanto cuando Internet, sus servicios o las terminales informáticas a él conectadas, constituye el objeto sobre el que se realiza el ataque, como cuando es el medio a través del cual se ejecuta la agresión. Se trata, por tanto, de una mera sistematización inclusiva y simbólica, más que de una clasificación que diferencie entre las tipologías de conductas por algún tipo de efecto asociado a cada una de ellas. En otras palabras: no se deriva ninguna consecuencia del hecho de que un cibercrimen lo sea por el medio utilizado o por el objeto contra el que se comete, pues en última instancia se trata de una sistematización tipológica que sirve para incluir conductas y no para separarlas.

Pese a ello, sin embargo, creo que es discutible en la actualidad la validez de esta clasificación tipológica de la cibercriminalidad dado que, a mi parecer y tomando en consideración los objetivos de la categoría, no todo ataque en el que el objetivo del mismo fuera un elemento de las TIC debiera formar parte del concepto global de cibercrimen. Me refiero especialmente a aquellas conductas no realizadas a través del ciberespacio en las que se atenta con-

---

WALL, D., «Cybercrimes and the Internet», en WALL, D. (ed.), *Crime and the Internet,* New York, Routledge, 2001, pp. 3 y ss. El propio Wall también estableció una diferenciación semejante a la que veremos ahora y que distingue entre *computer assisted crimes*, y *computerfocused crimes*, pero con una tercera categoría que hace que se asemeje a la que aquí se va a defender. WALL, D. S., «The Internet as a Conduit for Criminals», en PATTAVINA, A., *Information Technology and the Criminal Justice System*, California, Thousand Oaks, Sage Publications Inc., 2005, pp. 78 y ss.; y también en WALL, D. S., «What are Cybercrimes?», *op. cit.,* p. 59, que discrimina entre *computer integrity crimes, computer related crimes* y *computer content crimes.* Los primeros serían aquellos delitos en los que se atenta contra la integridad de una red o un sistema (*hacking, cracking, cyber-vandalism, spying, denial of service,* infecciones de *malware,* etc.); los segundos, son aquellos en los que se usan los sistemas en red para engañar a las víctimas con intenciones ilícitas (fraudes informáticos en general, *phishing*, etc.); y la última categoría englobaría los delitos en los que se distribuyen contenidos por medio de redes, tales como la distribución de material pornográfico o la difusión por Internet de mensajes de odio racial. Se acerca bastante esta clasificación de la cibercriminalidad a la que voy a sostener más adelante, quizás con la esencial diferencia de que Wall implícitamente se está olvidando en la segunda categoría de muchos otros cibercrímenes, *cyberbullying, cyberstalking*, etc., que no entrarían en tal sistematización.

[3] FURNELL, S., «Cybercrime: vandalizing the information society», *op. cit.,* p. 335.

[4] CLOUGH, J., *Principles of Cybercrime, op. cit.,* p. 10, que añade una categoría que no sería, a mi parecer, cibercriminalidad, que es aquella en la que el uso del sistema informático es incidental y simplemente puede ayudar a la averiguación del delito. Como aquí se sostiene, si el ciberespacio no es el medio a través del cual se lleva a cabo el delito, éste no debe ser conceptualizado como cibercrimen.

tra algún elemento físico, aunque conectado a Internet, como una terminal informática o la información en ella contenida. Estos comportamientos no plantean los problemas que, como después se verá, se asocian a la cibercriminalidad, como la modificación de los parámetros espacio-temporales con la consiguiente transnacionalidad de las conductas, entre otros caracteres, y que inciden en las dificultades de persecución jurídico-penal junto con otras consecuencias para el sistema penal. Los mismos, por el contrario, estarán presentes siempre que el ciberespacio, como ámbito abierto derivado del uso de las TIC en general, y de las redes telemáticas (también las telefónicas) en particular, sea el medio a través del cual se lleva a cabo la infracción, por lo que debiera restringirse a éstos, que por otra parte son la inmensa mayoría y los que realmente son una subespecie criminológica y conllevan una problemática penal, la categorización de cibercriminalidad. Así, no entrarían dentro de la categoría de cibercrímenes los comportamientos del *insider* de acceder directamente, no por medio de ninguna red telemática, al ordenador de un compañero para dañar sus archivos o para recopilar información íntima de la persona o confidencial de la empresa, pues estas conductas no plantean problemas de transnacionalidad ni están caracterizadas criminológicamente como todas aquellas otras, también cometidas en algunos casos por *insiders*, llevadas a cabo por medio del ciberespacio. En otras palabras: en muchos casos las TIC serán el objetivo del ataque además de ser el medio por el cual el mismo se realiza, pero sólo si eso es así, si coincide en ese caso que Internet sea el medio además del objetivo, estaremos entonces ante un cibercrimen.

Otra interesante clasificación es la aportada por Kshetri que, desde una perspectiva de análisis económico, diferencia entre *predatory cybercrimes* y *market-based cybercrimes* [5]. Los primeros son aquellos actos ilegales en el ciberespacio en los que el cibercriminal intencionadamente daña la propiedad o la persona de alguien, entre los que incluye el robo de dinero de la cuenta bancaria o la infracción de la propiedad intelectual. La característica esencial desde la perspectiva económica es que estos comportamientos no conllevan la producción de nuevos bienes o servicios, sino simplemente una redistribución de los existentes [6]. Por el contrario los que el autor denomina *market-based cybercrimes* se caracterizan por generar nuevos valores económicos más que por redistribuir los existentes, y consisten en la realización de servicios consistentes en actividades criminales, tales como la venta de *software* malicioso, la venta de drogas *online* o la venta de información referida a tarjetas de crédito [7]. Aunque se trata de una interesante clasificación que pone de manifiesto que la economía existente en el mundo del cibercrimen

---

[5] KSHETRI, N., *The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives,* Heidelberg, Springer Verlag, 2010, pp. 10 y ss., especialmente p. 13.

[6] *Ibid.,* p. 13.

[7] *Ibid.*

va mucho más allá de las presuntas pérdidas por robos a la banca electrónica, lo cierto es que la clasificación no nos sirve a los efectos que pretendemos de, por una parte, encuadrar todas las tipologías de comportamiento criminal en el ciberespacio existente y, por otra, aportar criterios de diferenciación entre ellas con la finalidad de comprender mejor la realidad criminológica y

Tabla 2.1. Modalidades de cibercrimen. Elaboración propia.

	Ciberataques puros	*Ciberataques réplica*	*Ciberataques de contenido*
CIBERCRÍMENES ECONÓMICOS	• *Hacking* • *Malware* intrusivo • *Malware* destructivo • Ataques de *insiders* • Ataques DoS • *Spam* • Ciberocupación red • *Antisocial networks*	• Ciberfraudes (*phishing, pharming, scam, auction fraud...)* • *Cyberspyware* (uso de *sniffers* y demás *spyware,* ciberespionaje de empresa) • *Identity theft* • *Spoofing* (*DNS spoofing, ARP spoofing, IP spoofing, web spoofing*) • Ciberblanqueo de capitales • Ciberextorsión • Ciberocupación	• Distribución de pornografía infantil en Internet • Ciberpiratería intelectual
CIBERCRÍMENES SOCIALES		• *Spoofing* • *Cyberstalking* • *Cyberbullying* • *Online harassment* (ciberamenazas, coacciones, injurias, etc.) • *Sexting* (y extorsión con imágenes de *sexting*) • *Online grooming*	
CIBERCRÍMENES POLÍTICOS	• Ataques DoS *(cyberwar)* • Ataques DoS *(Cyberhacktivism)* • *Malware* intrusivo	• Ciberespionaje terrorista • Ciberguerra	• *Online hate speech* • Ciberterrorismo (difusión de mensajes radicales con fines terroristas)

las necesidades preventivas de cada categoría de delitos dentro del general fenómeno del cibercrimen.

Partiendo de que el elemento común a todas las tipologías de conductas que situamos dentro del cibercrimen, es la utilización de redes telemáticas o sistemas de información y comunicación para su comisión o, en otras palabras, de que el ciberespacio es el ámbito en el cual las mismas se llevan a cabo, creo que es interesante realizar dos diferentes sistematizaciones de los cibercrímenes con dos finalidades distintas: en primer lugar, y para comprender las nuevas formas de comportamiento criminal surgidas en Internet debido al cambio tecnológico y sociológico producido en la sociedad de la información, diferenciaré tres tipos de cibercrímenes atendiendo al aspecto en que inciden las TIC en el comportamiento criminal. En segundo lugar, y en aras de identificar los ámbitos principales a los que afecta el cibercrimen y a encontrar para cada categoría por lo menos un ámbito de referencia en la criminalidad común en aras a la comprensión del fenómeno y a su mejor prevención, diferenciaré entre otras tres categorías de criminalidad en el ciberespacio atendiendo esta vez al propósito criminal con el que se actúa y al contexto de incidencia del ciberespacio al que afectan los delitos.

La unión de ambas sistematizaciones, que a continuación comentaré, da lugar a la tabla tipológica-criminológica de la delincuencia en el ciberespacio de la página anterior.

2. CLASIFICACIÓN ATENDIENDO A LA INCIDENCIA DE LAS TIC EN EL COMPORTAMIENTO CRIMINAL

El concepto amplio de cibercriminalidad que se ha sostenido aquí nos permite incluir muchas modalidades de comportamientos ilícitos en el ciberespacio que se pueden sistematizar atendiendo al papel que las TIC desempeñan en el acto criminal. Aunque el principal objetivo de esta clasificación es esencialmente el de enumerar todas las formas de ataque existentes en la actualidad en el ciberespacio, la configuración de las mismas en tres grandes bloques de tipologías de conductas si atendemos al papel que las TIC, o el ciberespacio como ámbito de desarrollo de las mismas, desempeña en el acto, nos permitirá, además, una mejor visión de la problemática global de la cibercriminalidad al ver las distintas formas en las que Internet y las tecnologías a él asociadas han influido en la aparición de una nueva forma de criminalidad. Así, la observación de la realidad criminológica nos enseña en primer lugar que el ciberespacio se ha convertido en algunos casos en un ámbito auténticamente generador de nuevas conductas delictivas cuando las TIC son la única forma de realización de la infracción; en otros, en cambio, la irrupción del «nuevo espacio» no ha supuesto la aparición de nuevas formas puras de delincuencia, sino de réplicas de otras ya existentes que cambian sus caracteres básicos al llevarse a cabo en el nuevo ámbito virtual;

y, por último, el ciberespacio de sistemas conectados en redes también ha potenciado la importancia de los contenidos al facilitar enormemente su difusión global, lo que ha generado todo un conjunto de conductas en las que la ilicitud no estriba más que en la difusión o acceso a determinadas formas de información ilícita o socialmente considerada peligrosa [8].

Se trata, al igual que las sistematizaciones que hemos desechado y de otras muchas, de una clasificación de carácter débil, en cuanto que la misma debe servir sólo para incluir conductas dentro del ámbito de la cibercriminalidad, pero no para extraer consecuencias de ningún tipo del hecho de la pertenencia de cada infracción a una u otra categoría. Es cierto, en todo caso, que todas las categorías, al estar unidas por el ámbito en el que se comete la conducta delictiva tendrán caracteres comunes, pues cada categoría, por la forma de incidencia de las TIC en la esencia de la conducta criminal, planteará particulares problemas criminológicos y penales.

Así, en el caso de los que denominaremos «ciberataques puros» (por ser únicamente posibles en el ciberespacio), la problemática más propia se derivará de la total novedad de los comportamientos, con la consiguiente falta de estrategias preventivas de carácter criminológico frente a ellas, así como de la inexistencia de preceptos que permitan la incriminación de los mismos. En el caso de la categoría a la que nos referiremos como «ciberataques réplica» (en la que el ciberespacio es el nuevo medio desde el que realizar delitos tradicionales), el problema será la potenciación del riesgo para los intereses sociales que se deriva del nuevo medio, vasto e inmenso como es el ciberespacio, en el que se ejecuta la infracción, así como la dudosa capacidad de los tipos penales existentes para dar cabida a conductas similares en lo injusto pero cambiantes en su forma de realización. Por último, las infracciones denominadas «cibercrímenes de contenido», plantean dificultades propias relacionadas tanto con la dificultad de prevenir la mera difusión de contenidos en el ciberespacio, como con la compleja cuestión de atribuir responsabilidad a todos los intervinientes en tal proceso.

Todas ellas, como se ha dicho, plantean problemas comunes que serán analizados posteriormente. Es momento éste, sin embargo, de identificar las diferentes modalidades de cibercrímenes, situándolas en estas tres categorías definidas al efecto.

2.1. Ciberataques puros

El ciberespacio como ámbito de unión de las TIC ha supuesto la aparición de nuevos objetos y bienes socialmente valiosos, así como de nuevos servicios con valor económico y social. En relación con ellos, aparecen nuevas relaciones sociales, novedosas conductas que adquieren sentido sólo en

[8] Wall, D. S., «What are Cybercrimes?», *op. cit.*, p. 59.

ese ámbito que es Internet. A los efectos que nos interesan, lo que esto supone es el surgimiento en Internet de todo un conjunto de conductas ilícitas en Internet, de infracciones que pueden considerarse totalmente nuevas al estar caracterizadas por dirigirse contra los nuevos servicios, los nuevos bienes, o las terminales que operan en el ciberespacio [9]. Se trata, por tanto, de cibercrímenes puros, de los únicos que podrían ser denominados como tales en el caso de que la condición de pertenencia fuera que solamente deben ser posibles en el ciberespacio. Y esto es así porque en ellos las TIC no sólo constituyen el medio comisivo de tales ataques, sino que son el único posible, en cuanto que son medio y objetivo, y no es posible producir la esencia de ilicitud de estas infracciones si no es en el ciberespacio.

2.1.1. *El* hacking

Entre estas infracciones podríamos incluir, en primer lugar, el *hacking* o acceso ilícito a sistemas informáticos, que en otras clasificaciones se suele considerar además, una concreta modalidad de un grupo de ataques más genérico, denominado en terminología de la comunidad informática *data breaches* o violación de datos, consistente en cualquier forma de destrucción, modificación o acceso a datos de empresas (generalmente se utiliza en este sentido) o de particulares. Según el estudio efectuado por Verizon Business RISK team en el año 2010 sobre la violación de datos en Estados Unidos, casi el 50 por 100 de ese tipo de ataques se realiza por medio de una acción desleal, generalmente de un *insider* que aprovecha su posición en la empresa para dañarla o vender la información a otros. Junto con esta forma de realización de la violación de datos también encontramos un 40 por 100 de acciones que son resultado del *hacking* y un 38 por 100 en las que se utiliza *malware*, entre otras [10]. Generalmente los *data breaches* se realizan como forma de espionaje informático y entrarían ya, pues, en el otro tipo de ataques.

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

---

[9] Respecto a estas últimas es cierto que si existieran las terminales y no Internet sería posible el ataque a las mismas de forma física, como en las primeras formas de daños antes de la irrupción del ciberespacio, lógicamente siempre que haya un contacto previo de algún elemento informático con el terminal objetivo. Sin embargo creo que si no existiera el ciberespacio universal y popularizado, la infección de virus y demás ataques a terminales no tendría el mismo sentido ni significación que tiene en la actualidad, por lo que me parece más acertado situar tales conductas como ciberataques puros que como réplica.

[10] BAKER, W. *et al.,* «2010 Data Breach Investigations Report. A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service», 2010. En Internet, en *http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf* (última visita el 29 de noviembre de 2010, p. 6).

en este sentido amplio, es la actividad de los *hackers* consistente en la superación de cualquier barrera informática, bien sea para el acceso a un sistema, bien para la configuración de una determinada programación funcional, etc. En sentido estricto, en cambio, es equivalente a otro término generalmente utilizado, el intrusismo informático, que pone el acento en que tal conducta conlleva la violación de una esfera de exclusividad reservada al titular del sistema, haya o no haya en ella información privada o confidencial. No es necesario, pues, para que haya *hacking* informático entendido en sentido estricto, que el sujeto que lo lleva a cabo llegue hasta archivos, datos o programas del sistema, si bien por la propia configuración de los sistemas informáticos este resultado acabará dándose en la mayor parte de las ocasiones. Así pues, y como se explicará después al hablar de los cibercriminales, se puede hablar de *hacking* en su forma de *hacking* blanco en el que el propósito del *hacker* es simplemente el de acceder al sistema o a sus datos e información, pero sin ningún propósito de sabotaje o utilización posterior de la información, o en su forma de *cracking*, en la que el *cracker* accede al sistema para realizar cualquier tipo de daño al sistema, a los elementos que él contiene, o a su titular al adquirir, eliminar o modificar información del mismo [11].

El *hacking* en el sentido estricto que ahora nos interesa, de acceso a los sistemas informáticos, se puede llevar a cabo de muy distintas formas, si bien generalmente, el modo de proceder consiste en la búsqueda de vulnerabilidades en los sistemas informáticos derivadas de una deficiente programación, de un cambio tecnológico que hace obsoleta la formulación binaria existente, o incluso, en la búsqueda y uso de las puertas que involuntariamente el propio titular del sistema informático o cualquiera de los múltiples sujetos que interaccionan con él pueden haber dejado abiertas. En todo caso, el *hacking* es siempre, por su propia naturaleza, un acceso remoto, esto es, realizado a distancia por el sujeto que, normalmente a través de Internet, se entromete en un sistema sin tener contacto físico con él. No es *hacking* propiamente dicho el acceso directo, en la propia terminal, y no autorizado a un sistema informático. Este comportamiento, usual en el ámbito familiar o laboral y generalmente realizado para obtener información sensible que puede estar contenida en el sistema, no puede considerarse *hacking* a efectos criminológicos, puesto que sus características de riesgo son distintas a las del acceso informático ilícito realizado en el ciberespacio. Es evidente, en todo caso, que tal forma de *hacking* cuyo análisis no interesa aquí, sí constituirá un acceso ilícito a un sistema informático conforme a la regulación jurídica de la mayoría de los países.

---

[11] Es la diferencia entre el *white hat hacking* y el *black hat hacking* o, respectivamente, *hacking* y *cracking* conforme a una terminología que ha tenido éxito en España y que también es aceptada por autores como WALL, D. S., «What are Cybercrimes?», *op. cit.,* p. 59. Sobre ello véase en profundidad el análisis criminológico de los *hackers* en cap. I.3.1.2, y su tipificación tras la reforma en cap. VI.

Por último, el *hacking* lo es en cuanto existe una intromisión o acceso a un sistema informático ajeno. No hay *hacking,* por el contrario, cuando el sujeto utiliza determinados programas informáticos para extraer información del sistema, pero sin que pueda decirse que el *hacker* haya tenido ningún tipo de acceso real al sistema. Es decir, que independientemente de que haya habido o no acceso a los datos, lo relevante para que podamos decir que el tipo de ciberataque que se ha cometido es *hacking*, es que haya existido una entrada no autorizada en el sistema ajeno, no bastando con que debido a la introducción de algún *malware* u otro tipo de rutina sea el propio sistema el que envíe información al *hacker*.

El *hacking* apareció en el mismo momento en que surgieron los sistemas informáticos, siendo al principio, y en algunos sistemas operativos todavía ahora, una forma de comportamiento imprescindible para lograr la evolución del sistema [12], descubriendo sus carencias o sus posibilidades y haciéndolo más seguro o más abierto, según las preferencias y necesidades. Con el paso del tiempo, sin embargo, se ha ido asociando socialmente la idea de *hacking* a la propia cibercriminalidad. La razón es que si bien no todo *hacking*, como se vio anteriormente, es *cracking,* esto es, se realiza en el marco de una actividad criminal como acto preparatorio para la posterior realización de un ataque que consista en el robo de información, el daño del sistema, o el fraude directo; el mero hecho de negar la exclusividad en el acceso al sistema privado, implícito al *hacking,* pone en riesgo el propio valor de los sistemas informáticos como instrumentos para la recopilación, ordenación y transmisión de información dirigida desde el ámbito personal o empresarial, privado. En efecto, junto al *cracking* llevado a cabo por quienes acceden al sistema con propósitos criminales, se distingue tradicionalmente el *hacking* puro o blanco en el que el propósito se agota en el propio acceso. En este último, la acción se agota en el propio hecho de salvar las barreras de protección existentes, hasta el punto de que en muchos casos es el propio *hacker* el que comunica a los titulares del sistema que existen vulnerabilidades que le han permitido entrar en el mismo. Pero, como se ha dicho, todo *hacking* implica una intromisión no autorizada y por ello, un acto de negación de la esfera de decisión de sujetos privados cuya seguridad es esencial para que Internet se convierta en un medio de comunicación y de transmisión de información universal.

Precisamente por ello, Internet, la herramienta tecnológica que ha abierto más posibilidades para el *hacking,* se ha acabado convirtiendo de algún modo

---

[12] En este sentido, es interesante la intervención de *hackers* en la evolución de Internet, tal y como relata, ROSENZWEIG, R., «Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet», en *AHR*, vol. 103, núm. 5, diciembre de 1998, pp. 1530 y ss., especialmente pp. 1542 y ss. Véase también sobre estos aspectos, el documentado y apasionado escrito de LEVY, S., *Hackers. Heroes of the computer revolution, O'reilly Media, Sebastopol, California,* 2010, pp. 11 y ss.

en la sentencia de muerte del *hacking* puro o blanco. En el esquema de ciberespacio abierto, pero también seguro para los sistemas que interaccionan en él, en el que pretende convertirse la Red de redes, la intromisión en sistemas ajenos no tiene cabida, cuanto menos en el marco de la legalidad. Prácticamente todos los países que han legislado sobre cibercriminalidad han acabado incluyendo en sus sistemas jurídicos una sanción, generalmente de carácter penal, para quienes lleven a cabo las conductas de *hacking.* El *hacking* como actividad idílica de superación de barreras informáticas mediante la comprensión total del medio para la creación de un ciberespacio libre y abierto, queda ya sólo para sistemas operativos de *software* abierto o para otros, pero siempre de forma concertada con los propios operadores del sistema, pues en caso contrario, se entra en el ámbito de la ilegalidad. En otras palabras, la consideración normativa de que todo *hacking* es *cracking* que se ha producido en muchos países, y entre ellos en España [13], puede llevar, como se analizará más adelante [14], a la desaparición de una forma de proceder en Internet que ha sido esencial para la creación y consolidación del sistema [15], pero que parece incompatible, cuanto menos en el plano de lo formalmente aceptado, con la necesidad de transmitir a los principales actores del medio la fiabilidad del mismo.

Las primeras formas de comportamiento ilícito relacionado con los sistemas informáticos, las que se llevaron a cabo incluso cuando Internet aún no existía como tal, las protagonizaba el *hacker,* aquel sujeto con conocimientos informáticos avanzados (en un momento en el que nadie parecía tenerlos) que vivía aislado socialmente y que encontraba en el acceso a otros sistemas un reto personal y un puro «divertimento». Ese *hacker* casi cinematográfico, que no se correspondía en realidad con los *hackers* que habían ayudado a convertir ARPANET en Internet [16], no era definido socialmente como un criminal, sino que, ya por gozar de conocimientos que los demás no tenían, ya por su actitud esencialmente intrusiva pero carente de intención de causar perjuicios, era visto como alguien en todo caso inadaptado, pero que no ponía en riesgo bienes esenciales de la sociedad, hasta el punto de que para algunos, de forma intuitivamente correcta, era más bien un elemento esencial para el desarrollo del sistema.

Sin embargo, la popularización de Internet y de las TIC, y la aparición de una generación completa que ha vivido ya en el uso de estas tecnologías, ha

---

[13] Véase, sobre la nueva regulación del *hacking* en el sistema penal español, Miró Llinares, F., «Cibercrímenes económicos y patrimoniales», en Ortiz de Urbina Gimeno, I. (dir.), *Memento práctico penal y económico de la empresa 2011-2012,* Madrid, Francis Lefebvre, 2011.

[14] Véase *infra* cap. IV.1.2.

[15] Véanse en este sentido las reflexiones de Nissenbaum, H., «Hackers and the contested ontology of cyberspace», en *NMS,* núm. 6, 2004, pp. 195 y ss., y 205 y ss., especialmente donde señala que marginar a los *hackers* supondría, no sólo perder su visión sobre el ciberespacio y el uso de las tecnologías de la información, sino también sus múltiples contribuciones técnicas para el desarrollo informático.

[16] Levy, S., *Hackers. Heroes..., op. cit.,* pp. 11 y ss.

llevado, por una parte, a una relativización de la significación del *hacker,* que ya no es uno entre millones sino tan sólo entre miles; y por otra, a una mayor preocupación por la seguridad de los sistemas informáticos y por tanto, a una desvalorización social de todas aquellas conductas que parecen ponerlos en riesgo. Si a esto unimos el impacto de la globalización de la cibercriminalidad y de sus efectos, y el hecho de que muchas de las mafias organizadas que lideran dichas actividades delictivas utilizan *hackers* (más bien *crackers*) para acceder a sistemas informáticos ajenos con fines diversos pero siempre nocivos, puede entonces entenderse que la imagen idealizada del *hacker* se haya desmoronado.

De este modo, la popularización de Internet y su institucionalización como lugar para la comunicación global en términos sociales y económicos, pese a parecer un lugar idílico para el *hacker,* va a acabar llevándole a su desaparición, a la muerte de la idea romántica del acceso lícito. Pues si bien los *hackers* existirán siempre, desde el momento en que sea tan delictivo acceder a un sistema como entrar en él para dañarlo, la diferenciación entre *hackers* y *crackers* carecerá de sentido por lo menos en el plano legal, no siempre buen receptor de las realidades sociales que trata de regular.

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

Uno de los principales riesgos que, para particulares y, muy especialmente, para empresas, conlleva el acceso al ciberespacio por medio de sistemas informáticos, es el de sufrir lo que se ha venido denominando «sabotaje informático», incluyendo a su vez en él tanto los comportamientos, ya conocidos y asumidos como comunes en el entorno virtual, consistentes en el envío a través de redes telemáticas de virus informáticos que aprovechan la inmensidad de la Red para multiplicarse y acceder a miles de terminales, como cualesquiera otras formas de destrucción de archivos o datos de terminales concretos y determinados, con fines industriales o de daño individual [17].

Íntimamente relacionado con este sabotaje informático debemos identificar el sabotaje cibernético, por otros denominado cibervandalismo [18], in-

---

[17] A la definición de Romeo Casabona, C. M., «Los delitos de daños en el ámbito informático», en *CPC,* núm. 43, 1991, p. 91, del sabotaje informático como «la destrucción o inutilización del soporte lógico o físico de un ordenador con el fin inmediato de imposibilitar la utilización de la información procesada o almacenada», en la que, como señala González Rus, J. J., «Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (art. 264.2 del CP)», en Díez Ripollés, J. L.; Romeo Casabona, C. M.; Gracia Martín, L., e Higuera Guimerá, J. F. (eds.), *La ciencia del Derecho penal ante el nuevo siglo. Libro homenaje al profesor doctor don José Cerezo Mir,* Madrid, Tecnos, 2002, p. 1282, se sitúa como elemento central de la conducta que la misma incida, directa o indirectamente, en elementos lógicos; habría tan sólo que añadir, para poder hablar de la conducta como un cibercrimen, el que tal destrucción se realice en el ciberespacio o, en otros términos pero en idéntico sentido, a través de Internet.

[18] Hay que tener en cuenta, sin embargo, que el término *cybervandalism* no siempre se utiliza en el sentido que en nuestro ámbito le solemos dar al concepto de sabotaje informático y que abarca

clusivo de aquellos ataques a los sistemas informáticos a su información, a las redes de comunicación o a los servicios de Internet, caracterizados por su realización a través del ciberespacio y que es el que aquí nos interesa. También es, sin lugar a dudas, el que representa una auténtica amenaza en la actualidad. Al fin y al cabo, es el hecho de que los sistemas informáticos estén conectados entre sí en un ciberespacio transnacional y universalizado, lo que acrecienta el riesgo de que se produzcan daños al sistema o a los datos en él contenidos.

Así, la conexión de un sistema informático a Internet supone generalmente la puesta en riesgo de recursos propios. Un riesgo que evidentemente es asumido, puesto que una de las bases del ciberespacio es el carácter abierto de sus recursos a la vez que el carácter cerrado y privado de los sistemas que acceden a los mismos. Y un riesgo que es inherente al propio funcionamiento del sistema de intercomunicación social y económica que es el ciberespacio: los sistemas informáticos que se conectan a las redes suelen estar repletos de información que puede tener un valor económico o personal, además tales terminales son económicamente evaluables y, por último, la actividad económica en Internet exige la operatividad de los sistemas en red para el ejercicio de sus funciones. En otras palabras, el sabotaje cibernético puede afectar bien a los propios sistemas informáticos y demás elementos de *hardware* que lo conforman y que son evaluables económicamente; bien a la información contenida en los citados sistemas y que puede tener un valor económico o personal, en el sentido sentimental y relacionado con su propia dignidad, para el sujeto pasivo; o bien a la propia funcionalidad del sistema informático en el marco de la actividad económica de que se trate.

Y no hay que olvidar, como se ha avanzado, que no son los datos y las terminales los únicos posibles objetivos de sabotaje dentro del ciberespacio. Las redes telemáticas y los servicios de la Sociedad de la Información pueden tener en la actualidad muchísimo más valor que los datos que transitan por los mismos. Hoy en día ya no sólo es posible la destrucción de la información, sino también la paralización de la difusión de la misma, lo cual obviamente supone la neutralización funcional de los servicios relacionados. Este tipo de sabotaje, también ayudado por la infección de *malware*, preocupará cada vez más a la sociedad conforme se vayan trasladando al ciberespacio servicios públicos y privados que hasta el momento únicamente se ofrecían en el espacio físico.

---

todas las formas de destrucción de datos y sistemas informáticos, sino que en ocasiones se utiliza tal término para hacer referencia a conductas que aquí integraremos dentro del *hacktivismo* y que están más cerca del gamberrismo y de las acciones protesta en el ciberespacio que de la causación de daños.

2.1.2.1. *Malware*

La más popular de las formas de sabotaje cibernético es la que se lleva a cabo mediante la infección de virus destructivos que se debe considerar, a su vez, como una tipología del más general comportamiento de distribución de *malware* o *software* malicioso destinado a dañar, controlar o modificar un sistema informático. Desde su aparición en los años setenta, los virus se han acabado convirtiendo en un fenómeno casi natural en el ciberespacio, si bien en los últimos años, conforme la interconexión de sistemas en Red se ha ido popularizando, ha habido un crecimiento exponencial, pasando de los más de dos mil virus que se calculaban en el año 2000 (con algunos de los más conocidos como el Melissa o el Love bug), hasta los 137.000 en 2003. En la actualidad se calcula que son millones los ordenadores infectados por todo tipo de *malware* [19]. Además no sólo aumentan los virus, sino que, al igual que el ente biológico, también cambian adaptándose a las nuevas necesidades. En la evolución de los tipos de *malware* y de su funcionamiento se observa perfectamente la característica citada del ciberespacio de «sujeto a revolución permanente», hasta el punto de que cuando se publique esta monografía muchos de los aquí contenidos apenas tendrán ya importancia y algunos que la tendrán no habrán sido reflejados [20].

Dentro del *malware* hay distintas modalidades de *software* con objetivos muy distintos, desde los que tratan de destruir el sistema o su información como los virus y algunos tipos de gusanos (*worms*) o troyanos (*trojans*), pasando por los que permiten el acceso remoto del sistema informático a través de la Red como los *botnets* o los *rootkits* que esconden el *software* malicioso o permiten el control del sistema, hasta los *keystroke loggers* o *spyware* que capturan información de los sistemas informáticos [21]. También podría añadirse aquí el denominado *adware*, menos nocivo que todos los anteriores pero de algún modo también molesto, pues se trata de programas anexos que en realidad espían nuestros hábitos en Internet (qué páginas visitamos, cuándo nos conectamos, qué programas nos bajamos, etc.).

Las primeras formas de sabotaje a través del ciberespacio, surgidas en los años ochenta, pero popularizadas y convertidas en amenaza grave a partir de

---

[19] HOAR, S. B., «Trends in Cybercrime: The Darkside of the Internet», en *Criminal Justice,* vol. 20, núm. 3, 2005, pp. 5 y ss.

[20] Un ejemplo de esto lo constituyen los denominados ataques de *dialers, software* malicioso cuya función consistía en tomar el control del módem *dial-up* para realizar desde ahí una llamada a un número de teléfono de tarificación especial en el que se dejaba la línea abierta y se le cargaba el coste de dicha llamada. Dado que las actuales conexiones a Internet son mediante ADSL, este tipo de virus prácticamente ha desaparecido.

[21] OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, junio de 2008, p. 15. Sobre el *spyware* volveré más adelante cuando analice en la tercera tipología de conductas estos ataques con más profundidad.

los noventa [22] y que siguen vigentes en la actualidad, consistían en un tipo de *malware* muy dañoso pero que ha ido perdiendo protagonismo en los últimos años. Se trata de los virus destructivos que se propagan de un sistema informático a otro, y que tienen incidencia en los propios sistemas y en la información en ellos contenida. La infección de un sistema informático con un virus puede suponer la propia destrucción de elementos de *hardware* básicos del mismo, con el valor económico que los mismos pueden llegar a tener; pero, sobre todo, puede afectar, en el sentido de dañar, alterar o suprimir, a la información contenida en el sistema. Los sistemas informáticos sirven para ordenar, almacenar, procesar y transmitir información, siendo millones las terminales conectadas a Internet que contienen innumerables archivos y datos que pueden tener, un valor sentimental o personal, no evaluable económicamente en el sentido de ser bienes sustituibles por otros en el mercado (aun funcionalmente), o un valor económico derivado del propio esfuerzo que ha supuesto su producción y del valor potencial que en sí misma tiene en el mercado. En ambos casos, en el del daño moral y el daño patrimonial según el valor personal o económico de la información alterada o suprimida, el sabotaje cibernético afecta a los titulares de dichos valores. En ambos casos además, el sabotaje supone la negación de la seguridad en el ciberespacio, al transmitir tales comportamientos la información de que todo *hardware* y *software* está sometido al riesgo de daño en la Red.

Como se ha dicho, los riesgos para la información devienen en gran parte de la amenaza de tal forma de *malware* destructivo. Son millones las personas e instituciones que han perdido informaciones valiosas (personal o económicamente) a causa de un archivo enviado remotamente y en muchos casos de forma aleatoria y expansiva, de modo que los primeros infectados y afectados reenvían involuntariamente a otros por medio del correo electrónico el *malware* malicioso, creándose una cadena destructiva que puede causar pérdidas millonarias. La mejora de los sistemas de seguridad y su popularización a nivel empresarial y particular, unida al cambio de la configuración del *malware* que actúa ahora menos con propósito destructivo y se caracteriza más por incorporar *backdoors* y otras formas de acceso para el posterior espionaje o fraude, ha reducido, aunque sea mínimamente, la significación de los daños en archivos, datos y programas. Y aunque la amenaza sigue siendo importante debido a que la creación de virus es una de las formas de evolución de los sistemas de protección, recientes estudios criminológicos ponen de manifiesto que la incidencia real de estos programas para empresas, gobiernos y particulares ha sido exagerada y no es tan grave en la actualidad [23].

---

[22] HUGHES, L. A., y DELONE, G. J., «Viruses, worms...», *op. cit.,* p. 79.

[23] *Ibid.,* pp. 78 y ss. A partir de la pregunta de si algunas de las formas de *malware* actuales suponen un *«major threat»* o tan sólo una *«minor irritation»,* los autores del estudio analizan más de novecientos informes de ataques observados por una empresa de productos de seguridad infor-

La auténtica amenaza que supone en la actualidad la infección de *malware* no deriva tanto del sabotaje a los sistemas o a los datos y las pérdidas que ello puede conllevar, como de la posible pérdida de control para el titular o, mejor, de la adquisición de poder externo sobre el sistema que puede lograr el *hacke*r gracias a la infección con un virus informático. Hoy el envío de *malware* para la infección de un sistema suele ser un paso rutinario dentro de una dinámica compleja definida para lograr objetivos generalmente consistentes en la defraudación económica. En otras palabras, el envío de *malware* en la actualidad no es más que un comportamiento inicial necesario para la realización del ataque final consistente en una agresión al patrimonio o a la intimidad de los usuarios. De hecho los últimos estudios demuestran que ése es ya el principal tipo de virus existente: troyanos, gusanos, *backdoors* y demás, todos los cuales tratan de permitir la posterior entrada en el ordenador o su control futuro creando vulnerabilidades que sean aprovechadas posteriormente por los *hackers*. Los usos que se le dan al sistema infectado, luego, pueden ser variados: desde constituir el propio objeto del ataque al abrir el *malware* una puerta para el *hacking*, pasando por su utilización para que el sistema envíe información para su propia victimización, hasta su uso como terminal desde la que realizar futuros envíos de *malware* para la infección de otras terminales.

Esto ocurre especialmente en el caso de los ataques de *botnet*, en los que se infecta con *backdoors* un conjunto de sistemas (*bots*) que pasan a ser controlados por un único usuario (*botmaster*) [24]. Una *botnet* puede ser instruida por su controlador para realizar funciones de muy diverso tipo [25], entre las que destacan los ataques de denegación de servicio que después analizaremos, situar en el sistema el *hosting* o alojamiento de webs maliciosas dedicadas al blanqueo de dinero, la realización de fraudes por medio de *phishing* o la distribución de pornografía infantil, la realización de actividades de escaneo de sistemas y webs vulnerables para la realización de otras conductas delictivas, o el envío de gran número de correos electrónicos no solicitados (*spam*) [26]. Este tipo de infección está creciendo, y significativamente, hasta el punto de que durante el segundo trimestre de 2010 Microsoft confirmó la reparación de 6,5 millones de ordenadores in-

---

mática y analizan tanto los sistemas afectados por cada uno de ellos, la gravedad que han supuesto, como las posibles razones de la misma. La conclusión del estudio es que la mayor parte de los virus apenas causan daños significativos, no llegan a expandirse por la Red, y son fáciles de contener. Por el contrario hay otros ataques, especialmente aquellos que permiten el acceso no autorizado y que tratan de robar información esencial de empresas o particulares, que son mucho más perjudiciales y que amenazan seriamente la seguridad.

[24] Sobre los *botnets* véase especialmente CHOO, K. K. R., «Zombies and Botnets», en *TICCJ,* núm. 233, Canberra, 2007, p. 4.

[25] PINGUELO, F. M., y MULLER, B. W., «Virtual Crimes, Real Damages: a Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals», en *VJLT*, vol. 16, núm. 1, primavera 2011, p. 133.

[26] CHOO, K. K. R., «Zombies and Botnets», *op. cit.,* pp. 2 y ss.

fectados como *bots*, el doble de lo que había reparado durante el segundo trimestre de 2009 [27].

2.1.2.2. Sabotaje de *insiders*

Tampoco todas las formas de sabotaje de *insiders,* aunque sí las realizadas a través de las redes telemáticas, se pueden considerar sabotaje cibernético, pese a que sea ésta, junto a los virus, la otra forma común de daño de archivos, más que la, también posible de borrado y destrucción directa por parte de un *cracker.* Se trata de la conducta del *insider* o persona que trabaja (o trabajaba pero aún tiene acceso a los sistemas) en la empresa o institución víctima, y aprovecha su posición para, como venganza o motivos similares, destruir la mayor cantidad posible de información.

2.1.2.3. Ataques DoS

Ya se ha resaltado que no es la información el único valor o bien relacionado con el uso de los sistemas informáticos que, como hemos visto, puede ser «dañado» en Internet. La función del sistema informático, de forma separada al *hardware* que lo contiene o al *software* y archivos que lo conforman, también tiene un valor económico por sí misma, de tal modo que tanto se daña al titular de un sistema informático cuando se suprimen archivos valiosos del sistema, como cuando se le impide realizar las funciones informáticas a las que le destina el titular. Así, la inutilización de un sistema informático por el motivo que sea, también debe valorarse como una pérdida en sentido económico. Y la importancia económica de la funcionalidad de los sistemas se ha ido acrecentando conforme los mismos han dejado de desempeñar como principal función la de archivo y ordenación de la información, y ha comenzado a ser el centro de muchos sistemas informáticos la transmisión de la información. Internet ya no es tan sólo una forma de comunicación entre personas, sino que ha pasado a ser un mundo virtual de actividad económica, lleno de servicios de todo tipo que, en el caso de ser dañados, pueden conllevar un enorme perjuicio patrimonial para el particular.

Si bien es cierto que el daño a la funcionalidad del sistema era ya una consecuencia indirecta de los ataques de virus o de los *insiders* que al destruir la información producían en muchos casos una paralización del sistema, en la última década ha comenzado a generalizarse una forma de ataque directo a este valor económico que, generalmente, se dirige hacia algunos prestadores

---

[27] Claburn, T., «Microsoft Finds U.S. Leads in Botnets», en *Information Week,* 14 de octubre de 2010. En Internet, en *http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=227800051&c id=nl_IW_daily_2010-10-15_html* (última visita el 19 de junio de 2012).

de servicios en Internet, pero que puede afectar casi a cualquier sistema del ciberespacio. Se trata de los ataques de denegación de servicios, correspondiente castellano del término inglés *Denial of Services* (DoS), consistentes en la utilización de técnicas, en ocasiones bastante primitivas y en otras más depuradas, para cargar los recursos del ordenador objetivo y producir la negación de acceso del servidor a otros sistemas informáticos [28].

Los ataques de denegación de servicio se popularizaron a partir de febrero de 2000, cuando se produjo un conjunto de ataques que incapacitaron páginas web comerciales muy conocidas en Internet, tales como Yahoo, Ebay o Etrade; y posteriormente en enero de 2001 el propio servidor de Microsoft fue inutilizado por un ataque similar [29]. La difusión que tuvieron en todo el mundo estas noticias explica uno de los principales objetivos que suele estar detrás de un DoS: dañar la reputación de las empresas que ofrecen servicios en Internet, impidiendo el correcto funcionamiento de sus actividades [30], o incluso como forma de perjudicar a un competidor en algún tipo de servicio en Internet [31]. En los últimos años, sin embargo, también se han utilizado este tipo de ataques con finalidades de *hacktivismo* político [32], esto es, de difusión de mensajes de protesta en Internet generalmente dirigidos contra organismos o Estados que, según las comunidades de usuarios de Internet, ponen en riesgo la idea del ciberespacio abierto que ellos defienden [33]. En

---

[28] SINROD, E. J., y REILLY, W. P., «Cyber-crimes a practical approach to the application of federal computer crime laws», en *CHTLJ,* vol. 16, p. 4.

[29] MOORE, D.; VOELKER, G. M., y SAVAGE, S., «Inferring Internet Denial-of-Service Activity», en *ACM,* vol. 24, núm. 2, 2006.

[30] Éste podría ser el caso del ataque que recibió en España el blog de *software* Genbeta por negarse a retirar un artículo en el que se advertía del riesgo de determinados mensajes en el programa de mensajería instantánea Messenger que servían para el posterior perfeccionamiento de estafas informáticas. Posteriormente otro blog, Menéame, al publicar la citada noticia también recibió un ataque de DoS.

[31] El competidor es el que contrata a los *hackers* (en este caso *crackers*) para que impidan el acceso a la web rival.

[32] El *hacktivismo* político es definido por Samuel como una nueva forma de protesta social en la que se utiliza Internet como herramienta para el cambio político. SAMUEL, A. W., *Hacktivism and the Future of Political Participation,* tesis doctoral presentada para el doctorado en la Harvard University Cambridge, Massachusetts, septiembre de 2004, p. 8. Por su parte Caltagirone lo define como el uso de las TIC para promover una causa política mediante la utilización no autorizada y/o la interrupción de un servicio informático, CALTAGIRONE, S., *A Practical Ethical Assessment of Hacktivism,* en Internet en *http://www.classstudio.com/scaltagi/graduate_papers.html* (última visita el 24 de septiembre de 2012); quien señala además que los ataques de DoS son una de las formas comunes de *hacktivismo*.

[33] El ejemplo más reciente y más conocido de este fenómeno es el del grupo de ciberactivistas denominado Anonymous que opera desde el portal americano 4chan, y que en su iniciativa llamada *operación Payback* atacó distintas páginas web relacionadas con las empresas de contenidos musicales y similares y las entidades de gestión de los derechos sobre los mismos. Así, el 17 de septiembre de 2010, este grupo inició su ciberprotesta impidiendo el acceso a las webs de la RIAA (Asociación Americana de la Industria Musical) y de la MPAA (Asociación Americana Cinematográfica), en respuesta a los supuestos ataques de DoS que estas mismas empresas habían contratado para que se realizaran sobre páginas web dedicadas al intercambio gratuito de archivos. Posteriormente, el

esos casos el daño económico del ataque puede ser leve e incluso inexistente, al ser el auténtico objetivo el «hacerse notar» cerrando algún tipo de web institucional conocida.

El objetivo directo de los ataques de DoS consiste en saturar el servidor del sistema logrando que se centre en la petición que realiza el atacante sin que pueda atender a ninguna más. Esto produce la «denegación de servicios». Exige enviar previamente un determinado mensaje o paquete malicioso (lo que se denomina contacto) para intervenir en el funcionamiento del sistema impidiendo a los demás acceder al servicio ofertado. Para hacerlo, como ha señalado recientemente Maciá Fernández, existen dos métodos básicos: la explotación de una vulnerabilidad descubierta en una máquina objetivo que constituye el denominado «ataque de vulnerabilidad»; o el envío hacia la víctima de un amplio número de mensajes de apariencia legítima, conocido como «ataque de inundación» [34]. En el primero se aprovecha algún tipo de fallo en la configuración del *software* o del recurso informático para enviar unos paquetes de datos que provocan un estado no previsto por el programador en el momento de su diseño que puede suponer la generación de un bucle infinito, o la ralentización de la velocidad de ejecución de la aplicación, etc., provocando el cese del funcionamiento del sistema o su inutilización total o parcial [35]. En el segundo se envían a la víctima numerosos mensajes produciendo el agotamiento de determinados recursos críticos para que los usuarios no puedan hacer uso de los mismos [36].

Aunque los ataques de DoS siguen siendo una amenaza para los servicios en Internet, palidecen en comparación con los ataques que están detrás de las siglas DDoS, correspondientes a *Distributed Denial of Services* (denegación de servicio distribuida). Estos ataques que vienen a ser una evidente evolución del DoS, consisten en que, frente a la terminal única que realiza el ataque, son numerosas las máquinas que, de forma coordinada, atacan a una sola víctima [37]. Evidentemente, el peligro de estos ataques es mucho mayor, puesto que complican las estrategias defensivas del servidor o sistema que está siendo atacado. Además, y como vimos en el análisis tipológico, hoy en día la infección de *bots* hace que pueda utilizarse una red de ordenadores (*botnet*) para llevar a cabo un ataque que además, en principio, puede parecer un mensaje lícito.

---

8 de octubre, Anonymous actuó en España provocando el cierre de las páginas web de la SGAE, Promusicae y el Ministerio de Cultura, como protesta por la futura Ley de Economía Sostenible, causando que los servicios web de dichos portales cayeran durante cuarenta horas.

[34] Maciá Fernández, G., *Ataques de denegación de servicio a baja tasa contra servidores*, tesis doctoral presentada para el doctorado en la Universidad de Granada, mayo, 2007, p. 63.

[35] *Ibid.,* p. 13.

[36] *Ibid.,* p. 14. Hay muchas otras formas de ataque que, generalmente, pueden situarse dentro de estas dos, como son los ataques de protocolo o los ataques a recursos específicos. Véase en este sentido su completo y profundo análisis, en pp. 15 y ss.

[37] Sinrod, E. J., y Reilly, W. P., «Cyber-crimes...», *op. cit.*, p. 4.

Los ataques de denegación de servicio pueden causar importantes daños económicos a las páginas web, especialmente a aquellas que realizan una actividad económica, y dentro de ellas, tanto a las que se dedican a la venta directa de productos que no pueden ofrecerse al público mientras la web está saturada, como a aquellas otras que obtienen el beneficio patrimonial de forma indirecta, por ejemplo por la publicidad que no cumple su función durante un ataque de este tipo. En otros casos, por el contrario, por ejemplo, en aquellos en los que el ataque es una forma de *hacktivismo* político, la denegación de servicios supondrá la negación de la libre expresión de contenidos en la Red. En todos ellos, sin embargo, no sólo se ven afectados los derechos de los emisores, esto es, de los titulares de las páginas web que no pueden difundir oportunamente sus contenidos, sino también los de los receptores, los usuarios de tales sitios web que ven impedido el acceso. Esto hace que la DoS sea una coacción (sin violencia, eso sí) [38] doble: en cuanto que se impide al titular de la página web comunicar y al usuario acceder a la comunicación. No puede dudarse de que, dada la duración de algunos de estos ataques web (horas e incluso días) y dada la creciente y general tendencia de gobiernos y entidades privadas de convertir el ciberespacio en un ámbito de servicios sociales (sanitarios, administrativos, educativos, etc.) y empresariales, cada vez de mayor importancia, la afectación a la libertad de prestadores de servicios y de usuarios puede ser de extrema gravedad y no tener únicamente una incidencia económica, sino también de afectación a la libertad de acceso a Internet.

Si sumamos, por tanto, el DoS a los otros ataques analizados dentro de ese cajón de sastre denominado sabotaje cibernético, y realizamos una recapitulación acudiendo a la terminología de «los bienes jurídicos protegidos», podemos decir que hay varios tipos de bienes o intereses sociales dignos de protección que pueden ser afectados por este tipo de ataques. En primer lugar estaría el patrimonio de los titulares de los sistemas informáticos o de los archivos contenidos en ellos, que pueden ser dañados en su esencia o que puede negarse el acceso a ellos con consiguientes pérdidas económicas. Relacionado con el mismo, estaría el interés socio-económico colectivo en que la actividad económica en Internet sea segura, sin que la conexión de sistemas informáticos a la Red pueda poner en riesgo los mismos o la información en ellos contenidos. Por otra parte, y aún desde la perspectiva del emisor, también se pueden ver afectadas las víctimas de un sabotaje cibernético en su derecho a la libre expresión en Internet, al impedírseles comunicar sus mensajes y llevar a cabo su actividad. Y ya en el plano del

[38] Y es que MORALES GARCÍA, Ó., «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del Consejo de Europa sobre Cyber-crime», en *CDJ,* núm. 9, 2002, p. 31, planteaba la posibilidad de sancionar los ataques de DoS como delitos de coacciones, siendo sin embargo, cuanto menos problemática, a mi parecer, la consideración de que en estos casos hay una *vis in rebus* suficiente para configurar el concepto de violencia.

receptor, todas las formas de sabotaje cibernético, pero muy especialmente la consistente en ataques de DoS, conllevan una negación de los derechos de todos los usuarios de Internet al acceso a los servicios existentes en la Red. Este interés va a ir adquiriendo una importancia creciente, conforme el ciberespacio vaya centralizando servicios administrativos y sociales que, si cayeran, pueden suponer graves daños para miles de personas en un determinado momento.

Evidentemente, no todo sabotaje informático causa tales daños. Más bien, debido a los sistemas de seguridad existentes, tanto en forma de antivirus como otros sistemas para la evitación o minimización de los daños de los ataques de DoS, son minoritarios los que afectan gravemente a dichos intereses. Pero también es cierto que pueden hacerlo.

2.1.2.4. *Spam*

Aunque pueda discutirse la consideración del *spam* como sabotaje, lo cierto es que se trata de un evidente ataque a los sistemas informáticos llevado a cabo a través del correo electrónico que puede afectar a la funcionalidad del sistema o, en la mayoría de los casos, transportar *malware* o información falsa como parte de la dinámica del *phishing* o de cualquier otro ciberataque realizado con intención defraudatoria.

Se denomina *spam* al correo electrónico no solicitado que suele enviarse a numerosas direcciones a través de una dirección electrónica de las ofrecidas por los servicios de correo gratuitos estilo Hotmail, o desde un sistema informático infectado, convertido en *bot* e integrado en una *botnet* y utilizado por el *spammer,* que adquiere las direcciones de correo *hackeando* sistemas informáticos o utilizando *spyware* u otros sistemas de búsqueda de direcciones electrónicas a través de la Red. El *spam* tiene diversas finalidades que van desde el envío ilícito de publicidad, hasta el intento de infección del sistema por medio de *malware*, pasando por el intento de *phishing*. En todo caso, el envío de *spam,* así como la previa recopilación de direcciones electrónicas, puede considerarse ya un ataque a la terminal informática y a la funcionalidad de su uso por parte de particulares y empresas.

Y es que pese a que el principal riesgo que conlleva la recepción de correos *spam* estriba en la posibilidad de ser infectado por algún tipo de *malware* que sea posteriormente utilizado para defraudar a la víctima, tampoco debe despreciarse la enorme gravedad que supone el mero hecho de recibir correos indeseados aun en el caso de no ser infectado por ellos. Según un estudio sobre los costes económicos del *spam*, éste representa un coste para las empresas de Estados Unidos de casi 9.000 millones de dólares al año, 2.500 millones para las de Europa y 500 millones para los prestadores de

servicios [39]. Estas macrocifras aún llaman más la atención cuando se concretan en el coste para las empresas que supone la limpieza de *spam:* entre 600 y 1.000 dólares de pérdidas por año en productividad por usuario, con una media de 874 dólares de pérdida de rendimiento por persona debido a los diez correos de *spam* diarios recibidos por cuenta de correo en el ámbito de la empresa [40].

2.1.3. *Ocupación o uso de redes sin autorización*

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

2.1.4. Antisocial networks

Para finalizar, y como una de las formas más novedosas de conducta criminal en el ciberespacio me referiré a las que un grupo de autores ha venido en denominar «*antisocial networks*», o redes sociales antisociales [41]. En realidad más que una conducta criminal se trata de un comportamiento preparatorio de las posteriores conductas criminales que trata de asegurarlas y facilitarlas, y consiste en la manipulación de redes sociales o de grupos de ellas con la finalidad de utilizarlas posteriormente para el fraude o para cualquier otro tipo de ciberdelitos. Al fin y al cabo, y como han señalado los

---

[39] Estudio citado por YEARGAIN, J. W.; SETTOON, R. P., y MCKAY, S. E., «Can-Spam act of 2003: How to spam legally», en *JSeC,* vol. 2, núm. 1, 2004, pp. 15 y ss.

[40] *Ibid.,* p. 16.

[41] ATHANASOPOULOS, E.; MAKRIDAKIS, A.; ANTONATOS, S.; ANTONIADES, D.; IOANNIDIS, S.; ANAGNOSTAKIS, K. G., y MARKATOS, E. P., «Antisocial Networks: Turning a Social Network into a Botnet», en *LNCS,* vol. 5222/2008, 2008, p. 147.

autores del trabajo en el que se describe esta nueva práctica de cibercriminalidad [42], las redes sociales tienen algunas propiedades intrínsecas que las hacen ideales para ser aprovechadas por adversarios o por quienes quieren utilizarlas para defraudar a otros: en primer lugar tienen una gran, y ampliamente distribuida, base de usuarios; en segundo lugar está formada por grupos de usuarios que comparten similares intereses sociales lo cual conlleva un desarrollo de la confianza entre ellos y el uso de recursos compartidos; en tercer lugar la plataforma permite a los usuarios la instalación de aplicaciones pensadas contra el fraude y similares cibercrímenes. Todas estas características dan la oportunidad a los cibercriminales de manipular las cuentas de Internet de los usuarios o a ellos mismos directamente y llevarlos a ejecutar conductas antisociales contra el resto de personas en el ciberespacio sin el consentimiento de que lo están llevando a cabo. Se trata [43], valga el ejemplo, de convertir la Red social en un *social bot* con una capacidad lesiva más que considerable.

2.2. Ciberataques réplica

Además de los intereses y bienes surgidos en el ciberespacio, éste alberga todos aquellos tradicionales que no requieren un traslado físico, sino una comunicación posible en Internet. Del mismo modo, a las nuevas formas de conducta que no existirían si no lo hiciera el ciberespacio debemos sumar, como realizadas en él, aquellas otras que son reflejo en tal ámbito de las tradicionalmente ejecutadas en el espacio físico. Estas conductas e intereses son los que están en el otro grupo de conductas incardinables en la cibercriminalidad, el de los cibercrímenes réplica, formado por las nuevas formas de realización de infracciones tradicionales de las redes telemáticas. En este caso el ataque no se realiza a un terminal informático, ni tampoco es el contenido el objeto de la ilicitud, sino que la Red es el nuevo medio a través del cual se comete una infracción que utilizaba anteriormente otros medios para llevarse a cabo. Se trata, por tanto, de réplicas, llevadas a cabo en el ciberespacio, de crímenes que ya se realizaban, de otro modo, en el espacio físico. Sin embargo, los especiales caracteres de este nuevo ámbito de realización criminal que es el ciberespacio confieren a la conducta una singularidad tal, que la hacen aparecer prácticamente como una conducta nueva, hasta el punto de que lo que en el espacio territorial podía apenas tener relevancia dañina, puede adquirirla significativamente en el espacio virtual.

[42] *Ibid.*
[43] *Ibid.*

2.2.1. *Los ciberfraudes (*auction fraud *y otros)*

En este grupo entrarían, en primer lugar, los fraudes de Internet, en los que las redes telemáticas se convierten en el instrumento mediante el cual lograr un beneficio patrimonial derivado de un perjuicio patrimonial a una víctima. Son muchas las formas en las que se puede lograr acceder al patrimonio de terceros, utilizando las múltiples formas de relación comercial existentes en el ciberespacio, así como las propias debilidades de seguridad de los sistemas informáticos que dan directamente acceso al patrimonio o indirectamente a él, al contener las claves o datos bancarios de los usuarios. Así, algunas de las más conocidas son: los distintos fraudes de tarjetas de crédito; los fraudes de cheques [44]; las estafas de inversión [45]; las estafas piramidales realizadas a través de Internet [46]; las conocidas estafas de la lotería [47]; las ventas *online* defraudatorias en las que no se envía el producto comprado (o se envía con otras características, como en el *auction fraud*) o no se paga lo que se ha recibido o se cobran servicios no establecidos previamente; las estafas de inversión en las que se cobran gastos no previstos o no se explican pérdidas inesperadas, así como los ataques de *scam* en los que se prometen cantidades importantes de dinero a cambio de pequeñas transferencias relacionadas con ofertas de trabajo, loterías, premios u otros [48]. Una variedad de fraudes que va transformándose (o adaptándose, conforme a la terminología que utilizaremos más tarde) constantemente [49].

---

[44] Especialmente el fraude denominado en inglés *the counterfeit cashier's check scheme*, o esquema de falsificación de cheques de caja, destinado a defraudar a personas que venden mercancías por medio de los anuncios clasificados en Internet. Véase la explicación del procedimiento por el IC3 en Internet en *http://www.ic3.gov/crimeschemes.aspx#item-3*.

[45] O *invest fraud,* por medio de la cual se ofrecen productos financieros, préstamos o similares, que resultan ser falsos.

[46] También denominadas *ponzi frauds* y que son en última instancia fraudes de inversión en los que a los inversores se les prometen beneficios anormales que, en realidad, no son (cuando se cobran) más que las inversiones, falsas, de otros sujetos idénticamente engañados.

[47] Aunque las hay de muchos tipos, el esquema del fraude de loterías suele caracterizarse por el envío de *spam* con *e-mails* en los que se informa a quien lo recibe de que ha ganado una lotería internacional por una cantidad altísima de dinero y que, para retirarla, se solicita el ingreso de una cantidad de dinero que es el objeto de la defraudación.

[48] Entre otros muchos citados por STADLER, W. A., «Internet Fraud», en FISHER, B. S., y LAB, S. P., *Encyclopedia of Victimology and Crime Prevention,* vol. 1, California/London, Sage Publications, 2010, pp. 492 y 493.

[49] Así, y tomando como referencia la página web del IC3, que hace una importante labor de recogida de denuncias para la sistematización de los diferentes ciberfraudes existentes, deberían tomarse en cuenta además de los citados, otros como el *debt elimination fraud,* o fraude en los planes de eliminación de deudas, llevado a cabo por falsas empresas que solicitan el ingreso de un dinero al cliente para refinanciar sus deudas hipotecarias y de tarjetas de crédito pero que nunca devuelven; el *scrow services fraud,* o estafa por servicios de custodia en la que se persuade a quien participa en subastas por Internet para que contrate un servicio de custodia que asegure el éxito de la llegada de la mercancía de modo tal que el comprador acaba pagando el dinero y perdiendo el envío.

Uno de los más comunes y que se mantiene como usual en los últimos años es el denominado *auction fraud*, o fraude en las subastas, consistente en la tergiversación de un producto o su no entrega conforme a lo pactado en los sistemas de subasta *online* tipo eBay. En general, la actividad relacionada con las subastas en Internet comprende una serie de acciones que requieren de la participación de los usuarios: es necesario el registro de una cuenta, la búsqueda de productos, la puja, ganar la puja, la transacción y finalmente informar sobre la reputación de los vendedores [50]. Cada una de estas acciones puede ser objeto de fraude. Chua y Wareham [51] han descrito varios tipos de *auction fraud* en Internet:

— *Shilling*. Los vendedores participan en la subasta pujando por sus propios artículos en competición con otros compradores, quienes por tanto deben pujar con cantidades más altas para adquirir los productos.

— *Bid shielding*. Dos personas se confabulan para pujar en la misma subasta, una de ellas realiza pujas bajas mientras que la otra hace pujas muy altas para disuadir a otros compradores. Después, el comprador que ha ganado la puja renuncia al artículo, por lo que la otra persona puede adquirir el producto.

— *Tergiversación.* Los vendedores proporcionan descripciones falsas de sus productos.

— *Ampliar la factura.* Los vendedores ocultan costes extra, como gastos possubasta por preparación del artículo.

— *Envío suspendido.* Los vendedores no envían los artículos adquiridos por los compradores.

— *Pago suspendido.* Los compradores no pagan después de adquirir un producto.

— *Reproducción y falsificación.* Los vendedores envían productos de imitación de otros auténticos.

— *Triangulación/custodia.* Los vendedores venden productos robados.

— *Comprar y cambiar.* Los compradores reciben los productos, sin embargo rechazan la transacción y devuelven a los vendedores otros productos similares o de inferior calidad.

— *Reclamación de pérdida o daños.* Los compradores reclaman falsos daños en los productos y piden el reembolso al vendedor.

— *Autosubasta.* Los vendedores organizan falsas subastas con la intención de obtener nombres de compradores e información de tarjetas de crédito.

---

[50] Chiu, C.; Ku, Y.; Lie, T., y Chen, Y., «Internet Auction Fraud Detection Using Social Network Analysis and Classification Tree Approaches», en *IJEC*, vol. 15, núm. 3, 2011, p. 124

[51] Chua, C. E. H., y Wareham, J., *Fighting Internet Auction Fraud: An Assessment and Proposal Computer,* 2004, p. 32.

2.2.1.1. Los ciberfraudes burdos o *scam*

También tiene especial importancia el envío de correos electrónicos denominados *scam,* y que no son más que las tradicionales estafas en las que, en este caso, la forma de comunicación entre las personas para la realización del engaño bastante es Internet, por correo electrónico o mediante el uso de las redes sociales [52]. Es ésta más bien una categoría genérica que podría englobar a casi todos los fraudes, si bien se suele utilizar como referencia de los más burdos de ellos, aquellos en los que el engaño es poco elaborado y en los que el error de la víctima puede ir más allá de lo común. En este caso podríamos integrar el conocido caso de las «cartas nigerianas», estafa clásica semejante al famoso «timo de la estampita» en el que el engaño se logra explotando el ánimo de lucro de la víctima, así como muchas otras que han surgido posteriormente como la de la lotería, la del trabajo desde casa, etc., siempre caracterizadas por tratar de interesar a la víctima o ganarse su confianza para que sea ella quien finalmente realice el acto de disposición patrimonial que le perjudica.

Por tanto, a pesar de que los sistemas técnicos han evolucionado y los niveles de protección a nivel de *hardware* y *software* son cada día más consistentes, en este tipo de estafas el factor humano, más concretamente su vulnerabilidad, constituye el elemento esencial para que el engaño tenga éxito [53]. De este modo, los ciberdelincuentes basan sus mensajes en ciertos principios del comportamiento humano que han sido estudiados, entre otros, por Stajano y Wilson [54]. En su investigación, estos autores describieron los patrones seguidos por los estafadores y establecieron los principios psicológicos en los que estaban basados sus mensajes y estrategias. Así, el principio de la distracción establece que mientras que las personas están centradas en lo que tienen que hacer, esta tarea les hace olvidar que deben protegerse a sí mismas. Este es el caso, por ejemplo, de los mensajes de supuestos administradores de sistemas que remiten un primer correo electrónico imponiendo estrictas configuraciones de seguridad, para posteriormente solicitar en un segundo mensaje el cambio de esta misma configuración por otra más sencilla y con la que, finalmente, lo que se busca es rebajar el nivel de protección

---

[52] Véase, extensamente, YAR, M., *Cybercrime and society, op. cit.,* pp. 81 y ss. En la actualidad, este tipo de ataques también se conocen en el mundo anglosajón como *cons,* abreviatura del término general *confidence trick*, igualmente denominado *bunko*. Consiste en tratar de defraudar a una persona ganándose previamente su confianza. En el fondo, no existe apenas diferencia entre los ataques de *scam* y los *cons*.

[53] Shadel describe ampliamente los principios psicológicos y las estrategias utilizadas por los delincuentes en sus estafas en general. Muchas de ellas han sido trasladadas directamente sin apenas modificaciones al ámbito del ciberespacio. SHADEL, D., *Outsmarting the Scam Artist: How to Protect Yourself From the most Clever Cons,* Wiley, 2012.

[54] STAJANO, F., y WILSON, P., «Understanding scam victims: Seven principles for systems security», en *ACM*, 2011, p. 9.

de los equipos. Otro principio es el de la adecuación social, cuya clave es la casi ausencia de cuestionamiento de la autoridad. Cuando una persona recibe un CD de un organismo oficial como la Policía generalmente lo acepta sin recelos, abriendo la posibilidad de instalar en su sistema un *malware*. Por su parte, el principio de la masa describe que incluso cuando las personas perciben señales que les hacen sospechar, su nivel de autoprotección baja cuando comparten riesgos con otros. Fraudes como las «cartas nigerianas» son el ejemplo clásico de otro principio, el de la deshonestidad, en el que la propia víctima pretende un lucro por medios ilegales. Finalmente los principios del engaño o la urgencia, provocan rápidas respuestas en los usuarios, desempeñando un papel fundamental en el éxito de la trampa.

2.2.1.2. El *phishing*

El perfeccionamiento de los sistemas de seguridad en la banca electrónica ha obligado a centrar los ataques en la obtención de la información secreta, bien por medio de *spyware* o *malware* o gracias a la intervención del propio sujeto, para la posterior utilización de tal información haciéndose pasar por el usuario, obteniendo así, de forma más o menos directa según las modalidades, el beneficio patrimonial. La modalidad estrella dentro de este subtipo de conductas de ciberfraude es el *phishing*[55], o pesca de incautos, definido por el grupo mundial *antiphishing* como el mecanismo criminal que emplea ingeniería social y subterfugios técnicos para robar los datos de identidad personales de los consumidores y los de sus tarjetas de crédito o cuentas bancarias[56]. El uso de la ingeniería social se produce cuando se utiliza la identidad personal de otro (*spoofing*) mediante la falsificación de sitios web, para conducir a los consumidores a que confíen en la veracidad del mensaje y divulguen los datos objetivos. Cuando se utilizan otros artificios técnicos, como por ejemplo redireccionar un nombre de dominio de una página web verdadera situada en la memoria caché del sujeto o de otro modo a una página web falsa, o monitorizar la intervención del sujeto en la verdadera, se utiliza el término de *pharming*.

Las primeras manifestaciones de este tipo de ciberfraude fueron descritas en 1996 por el grupo de noticias «alt.2600», en un mensaje en el que se hacía referencia al *phishing* en el ámbito de la creación fraudulenta de cuen-

---

[55] La palabra *phishing* es una evolución de *fishing*, en alusión al intento de hacer que las potenciales víctimas «muerdan el anzuelo». Los *hackers* frecuentemente reemplazan la letra «f» con las letras «ph», como raíz de la antigua forma de *hacking* telefónico conocida como *phreaking,* por lo que lo más probable es que éste sea el motivo por el que se escribe de este modo. No obstante, el término también se ha atribuido a la contracción de *password harversting fishing*, es decir, cosecha y pesca de contraseñas. El origen de esta denominación puede verse más extensamente en JAKOBSSON, M., *Phishing and Countermesasures: Understanding the Increasing Problem of Electronic Identity Theft,* John Willey & Sons, 2005.

[56] Véase JAISHANKAR, K., «Identity related Crime in the Cyberspace: Examining Phishing and its impact», en *IJCC*, vol. 2, enero-junio de 2008, p. 12.

tas de usuario de American Online (AOL) [57]. Estas cuentas robadas fueron denominadas *phish* y se convirtieron a partir de 1997 en habitual moneda de cambio entre los *hackers*, de modo tal que ciertas aplicaciones o juegos podían ser intercambiados por un determinado número de cuentas de AOL. Gordon y Chess [58] llevaron a cabo en 1998 una de las primeras investigaciones sobre ataques masivos a consumidores de servicios en Internet, tal fue el caso de los intentos de acceso a cuentas de AOL. En sus inicios, esta técnica se centraba en el engaño a través de correos electrónicos, con los que se pretendía obtener la respuesta del usuario atacado, es decir, provocar la remisión de contraseñas o detalles de las tarjetas de crédito. El nivel técnico de estos primeros fraudes era relativamente bajo; sin embargo, más tarde el aumento de la seguridad de las entidades y organismos que hacían uso de las TIC, así como los grandes beneficios obtenidos con escaso esfuerzo y la escasa probabilidad de detección del origen del fraude, devino en el incremento y refinamiento del engaño y de la calidad técnica de los ataques [59]. Así, por ejemplo, en el año 2000 se comenzaron a utilizar los *keyloggers*, un tipo de *software* que registra y memoriza en un fichero las pulsaciones que se realizan en un teclado; en 2001 los *phishers* iniciaron el uso de URL ofuscadas; en 2003 llevaron a cabo las primeras grabaciones de contenidos en pantalla o s*creenloggers*; en 2004 utilizaron por primera vez una web falsa y desde 2006 es habitual el *phishing* por VoIP [60]. Esta evolución no sólo ha modificado las técnicas de engaño, propagación de mensajes o construcción de webs falsas, sino que hoy día es incluso posible obtener *kits* de *phishing* en los que se incluyen plantillas para mensajes de correo y webs, bases de datos de destinatarios y técnicas para el blanqueo de dinero [61]. De igual modo, se ha producido una especialización en los delincuentes que realizan este tipo de

---

[57] Ollman, G., *The Phishing Guide: Understanding and Preventing Phishing Attacks. Informe Técnico,* NGSS, 2009, p. 6

[58] Gordon, S., y Chess, D. M., *Where There's Smoke, There's Mirrors: The Truth about Trojan Horses on the Internet,* Virus Bulletin Conference, 1998.

[59] El número y sofisticación de los ataques de *phishing* se ha incrementado a pesar de los ingentes esfuerzos en desarrollar contramedidas. El número de webs que informaron ser objetivo de *phishing* registró un incremento de 10.047 a 55.643 en diez meses en el período comprendido entre junio de 2006 y abril de 2007. Véase Dong, X.; Clark, J. A., y Jacob, J. L., *Defending the weakest link: phishing websites detection by analysing user behaviours,* Telecommun Syst, 2010, p. 215. Por su parte, el *Anti-Phishing Working Group* (APWG) informó que durante la primera mitad de 2011 una media de 32.650 webs fueron objeto de *phishing,* véase «Phishing Activity Trends Report», 1st Half/2011, consultado en línea el 14 de junio de 2012, en *http://apwg.org/reports/apwg_trends_report_h1_2011.pdf.*

[60] Ollman, G., *The Phishing Guide..., op. cit.,* p. 4.

[61] Verisign: *Fraud Alert: Phishing. The Latest Tactics and Potential Business Impact,* White Paper, 2009. En Internet, en *http://www.verisign.com/static/phishing-tactics.pdf* (última visita el 14 de junio de 2012). Véase también Ollmann, G., *The evolution of commercial malware development kits and colour-by-numbers custon malware,* Computer Fraud and Security, 2008, p. 5, en este interesante artículo se indica que el precio de estos kits de *phishing* puede oscilar entre los 50 y 800 dólares y se describen algunos kits. O también, Cova, M.; Kruegel, C., y Vigna, G., *There is no free phish: An analysis of free and live phishing kits,* Proceedings of the Second USENIX Workshop on Offensive Technologies, 2008, en el que se identifican más de quinientos kits.

estafas: no es extraño encontrar grupos de ciberdelincuentes que se organizan diferenciando entre mensajeros, recolectores y cajeros [62]. Los primeros, bien sean *spammers* o *hackers*, remiten un gran número de correos, generalmente a través de *botnets*, es decir, redes de ordenadores comprometidos y controlados por el mensajero. El segundo grupo, el de los recolectores, son *hackers* que construyen o alteran las webs a las que se dirigen los usuarios víctimas del *spam* y de las que se obtiene información confidencial como nombres de usuario, contraseñas o tarjetas de crédito. Un tercer grupo es el de los cajeros, los cuales obtienen información confidencial de los recolectores y hacen uso de ella, creando tarjetas de crédito para obtener dinero en cajeros, comprar productos en línea, hacer transferencias y, en definitiva, cualquier actividad que permita el lucro esperado.

En la actualidad, un típico ataque de *phishing* incluye tres componentes clave: el mensaje, la interacción y el robo. En el primero, el mensaje, las potenciales víctimas reciben un reclamo a través de un medio electrónico. En la mayoría de las ocasiones se trata de un correo electrónico remitido por el delincuente, pero también puede ser un SMS, VoIP [63], mensaje en una red social e incluso en videojuegos con múltiples participantes [64]. Este señuelo no suele ser muy sofisticado desde el punto de vista técnico, sino que a través de la ingeniería social aprovecha las debilidades de las potenciales víctimas. Poniendo en práctica diferentes estrategias de engaño, se consigue que el usuario siga un enlace a una URL inserta en un correo electrónico, proporcione determinada información sensible respondiendo a un correo o instale *malware*. Algunos ejemplos de la aplicación de estos principios, son los mensajes en los que se requieren actualizaciones de seguridad, se insta a completar información de cuentas para su mantenimiento, o se ofrecen incentivos financieros o falsas actualizaciones. Así, podemos encontrar mensajes del supuesto administrador de un sistema advirtiendo sobre un ataque, para evitar el cual debe instalarse urgentemente un «parche», o la notificación de problemas con la autenticación de usuario, cuya solución consiste en la remisión de una nueva contraseña. En otros casos, el mensaje contiene una proposición relacionada con futuras ganancias o beneficios, que en suma busca aprovechar el ánimo de lucro de la víctima para provocar ingresos de

---

[62] MYERS, S., «Introduction to Phishing» en JAKOBSSON, M., y MYERS, S., *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft,* John Wiley and Sons, 2006, p. 3

[63] La tecnología de VoIP (*Voice over Internet Protocol,* voz sobre protocolo de Internet) es básicamente un método por el cual tomando señales de audio analógicas, éstas se transforman en datos digitales que pueden ser transmitidos a través de Internet hacia una dirección IP determinada.

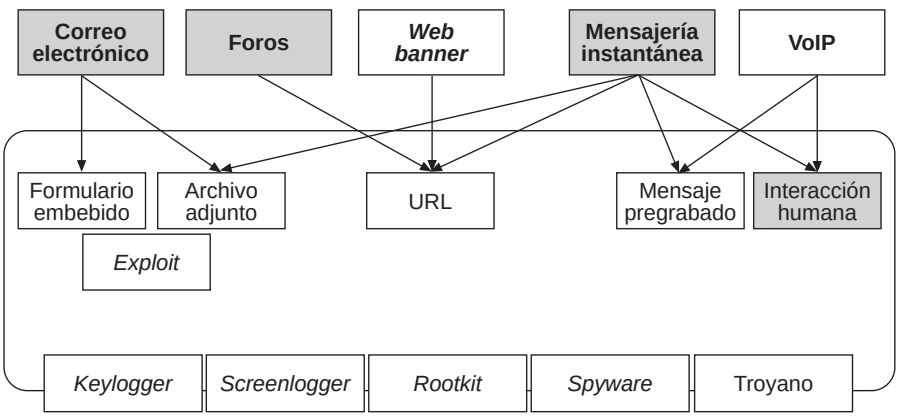
[64] HONG, J., «The State of Phishing Attacks», en *Communications of the ACM,* vol. 55, núm. 1, 2012, p. 74. En relación con los juegos masivos *online*, HILVEN, A., y WOODWARD, A., «How safe is Azeroth, or, are MMORPGs a security risk», *Proceedings of the 5th Australian Information Security Conference,* 2007, señalan que el valor de una cuenta robada de *World of Warcraft* es superior al de una tarjeta de crédito, lo que puede ayudar a comprender las complejas consecuencias de esta modalidad de fraude.

dinero en cuentas. Las ofertas, premios, promociones o regalos constituyen otro de los reclamos utilizados, junto con la solicitud de ayuda humanitaria para víctimas de desastres o situaciones desesperadas.

El segundo componente clave es la interacción. Recibido el mensaje por el usuario, a continuación se requiere que la propia víctima acuda a la web que se ha construido de manera idéntica a la de una organización de confianza, como un banco o una popular web de subastas, que instale el *malware* o que remita la información sensible. Para conseguir su objetivo, los *phishers* registran nombres de dominio parecidos a los de la entidad elegida; de este modo, podemos encontrar *ebay-login.com* en lugar de *eBay*, y también es posible encontrar imitaciones más burdas tales como *ebay.com.phishsite.com*. Por supuesto utilizan logos e imágenes de las empresas u organismos a los que suplantan, generando una falsa seguridad en la víctima. Para completar el engaño, emplean todo tipo de subterfugios técnicos, como la ofuscación de URL o la utilización de supuestas webs seguras de terceras partes o autoridades de validación, las cuales disponen de medidas de seguridad suplementaria como URL https, o certificados SSL. Estas entidades utilizan gráficos e imágenes que son igualmente replicados por los diseñadores de las falsas webs.

El tercer y último elemento es la utilización efectiva de la información robada. En algunos casos el delincuente usa directamente los datos de la víctima suplantando su identidad; no obstante, normalmente el *phisher* no explota por sí mismo la información obtenida, sino que la vende a terceros. Ejemplo de ello sería el caso mencionado de las cuentas de usuario para juegos masivos *online* o la venta de números de tarjetas de crédito. De este modo, se ha generado un mercado negro de compraventa de información robada.

Gráfico 2.1. Formas de transmisión, medios y tipos de *malware* en el *phishing*. Elaboración propia.



Podríamos decir, pues, que existen diferentes modalidades de *phishing* que, por otra parte, están en constante mutación y refinamiento según mejoran las medidas de seguridad y protección de organismos, entidades y usuarios. Así, podemos situar los diferentes tipos de *phishing* en un continuo que transcurre desde el mero engaño por medio de la ingeniería social, a las más sofisticadas técnicas de *hacking*, pasando por la combinación de ambos.

Tabla 2.2. Tipos de *phishing* en función del destinatario. Elaboración propia.

***Phishing* tradicional**	Utilización de imagen corporativa de entidades o instituciones solicitando datos bancarios indiscriminadamente.
Spear phishing	*Phishing* dirigido a entidades bancarias u otro tipo de organizaciones concretas, no a objetivos indiscriminados.
Business services phishing	El objetivo buscado son los empleados de entidades que utilizan servicios de Internet.
Whaling	*Phishing* dirigido a los directivos o individuos pertenecientes a los niveles altos de las organizaciones.

Puesta de manifiesto la dificultad de enumerar con exhaustividad las distintas técnicas de este tipo de fraude, a continuación se describen brevemente las más usuales:

En primer lugar encontramos el *phishing* tradicional, en el que se utiliza la imagen corporativa de una entidad bancaria o de una institución, para solicitar a la víctima por medio de correo electrónico que envíe a una dirección de correo que simula ser de tal entidad, los datos bancarios requeridos [65]. Esta forma de *phishing* ha comenzado a ser sustituida por otras más elaboradas como el *spear phishing* o «pesca con arpón», en la que en lugar de dirigirse a objetivos indiscriminados, se buscan clientes de entidades bancarias u otro tipo de organizaciones concretas. Una variante de este tipo de *phishing* es el *business services phishing*, en el que el objetivo ya no es siquiera un cliente de un banco, sino los empleados de entidades que

[65] Recuerda Fernández Teruelo que lo habitual es suplantar la imagen corporativa y la web original de entidades bancarias, pero que «se han detectado otras fórmulas como las siguientes: encuestas falsas en nombre de organismos oficiales que tienen por objeto recoger datos personales de los usuarios que decidan participar en la misma; páginas falsas de recargas de móviles con tarjeta de crédito o de venta de diversos productos (a precios sospechosamente baratos), en los que, una vez obtenidos los datos personales y de la tarjeta, la página enseña algún tipo de error o indica que la operación no se ha podido realizar; presuntos compradores que le piden al vendedor datos bancarios para pagarle el producto que tiene a la venta, los cuales serán utilizados para realizar transacciones ilícitas, etc.», Fernández Teruelo, J. G., «Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de red», en *RDPC*, núm. 19, 2007, pp. 217 y ss.

utilizan servicios como Google AdWords o Yahoo! De manera similar en la modalidad conocida como *whaling*, se ataca a los empleados de alto nivel de grandes empresas o gobiernos. En un ataque de *whaling* el *phisher* se centra en un pequeño grupo de personas de alto nivel de una organización concreta e intenta robar sus credenciales, preferiblemente a través de la instalación de *malware* que proporciona funcionalidades de «puerta de atrás» y *keylogging*. En estos casos, los señuelos no se limitan a la remisión de mensajes, puesto que lo que tratan es de infectar con *malware* el equipo informático, por tanto, utilizan todo tipo de medios como CD que contienen *software* de evaluación o que instalan *hardware* del tipo *keylogger* que permiten el registro de teclados y ratones.

Uno de los más recientes tipos de *phishing* es el denominado *vishing*, esto es, la combinación de voz y pesca de incautos [66]. Esta práctica consiste en la utilización de mensajes de telefonía basada en voz sobre IP, para conseguir de la víctima información personal, financiera o cualquier otro tipo de datos confidenciales.

Otro tipo de *phishing* es el basado en *malware*, es decir, cualquier tipo de *phishing* en el que se hace uso de *software* malicioso en el ordenador del usuario [67]. El ejemplo más común de este tipo de *phishing* es la ejecución de archivos adjuntos a mensajes de correo electrónico, o la descarga de *software* desde una web relacionada con pornografía o cotilleos sobre famosos. Este *malware* puede presentarse de diferentes formas, que por lo general explotan vulnerabilidades de los sistemas informáticos. De este modo podemos encontrar *keyloggers* o *screenloggers*, es decir, programas diseñados para monitorizar el teclado y el ratón o las entradas en pantalla. En estos casos el sujeto ni siquiera será conocedor de que está enviando las claves, ya que el correo electrónico enviado lleva un archivo que utiliza o bien *spyware,* del estilo de los programas *keylogger* o *sniffer,* para localizar los datos bancarios, o bien *malware* para lograr un acceso ilícito y descubrir los datos queridos; similares a éstas, los *hosts file poisoning* o alteración de los archivos de DNS, son defraudaciones que entran dentro de la denominación de *pharming.* Se trata de una táctica fraudulenta que consiste en cambiar los contenidos del DNS (*Domain Name Server*, Servidor de Nombres de Dominio) ya sea a través de la configuración del protocolo TCP/IP o del archivo *imhost* (que actúa como una caché local de nombres de servidores), para que el usuario, cuando teclea la dirección web de su entidad bancaria en su navegador, entre en realidad a una web falsa muy parecida o igual a la original, en la que acaba desvelando sus datos de acceso. Además, en caso de que el usuario afectado por el *pharming* navegue a través de un *proxy* para garantizar su anonimato,

---

[66] Del inglés *voice* y *phishing*.

[67] Para conocer una descripción de gran variedad de *malware* véase EMIGH, A., *Online Identity Theft: Phishing Technology, Clokepoints and Countermeasures. ITTC Report on Online Identity Theft Technology and Countermeasures*, 2005, p. 6.

la resolución de nombres del DNS del *proxy* puede verse afectada de forma que todos los usuarios que lo utilicen sean conducidos al servidor falso en lugar del legítimo; igualmente encontramos los *session hijackers* o secuestradores de sesiones, que permiten el acceso a los archivos del equipo o a los servicios del sistema; los troyanos web, o programas maliciosos que mediante ventanas emergentes recogen claves; y en general cualquier otra técnica que, utilizando *software,* permite perfeccionar el engaño haciendo creer a la víctima que está fuera de peligro.

También son frecuentes aquellos otros fraudes en los que el correo electrónico de la supuesta entidad bancaria incluye un *link* que redirige al sujeto, aparentemente, a una página web de la entidad que en realidad no es tal y que permite al atacante conocer los datos bancarios de su víctima, ya que el sujeto piensa que está tecleando las claves en su entidad bancaria. Esto se consigue accediendo a un servidor cuya seguridad se ha visto comprometida, y sustituyendo el contenido legítimo por otro malicioso, o aprovechando vulnerabilidades de las bases de datos SQL que permiten ejecutar *scripts*.

Para lograr el éxito de los ataques de *phishing*, se utiliza una amplia variedad de tretas, modificadas e incrementadas a medida que lo hacen los sistemas de seguridad. Los métodos más comunes son:

Man-in-the-middle (hombre en el medio). A través de esta técnica, el atacante es capaz de controlar y registrar las transacciones e información sensible del usuario, interponiendo un *proxy* entre el cliente y el servidor web. Al actuar de este modo, el usuario conecta con el servidor del *hacker* como si fuera el real, del mismo modo que lo hace el *hacker* transfiriendo los datos simultáneamente al servidor real. Así, no sólo es posible el acceso a las transferencias de datos mediante http, sino también por protocolo seguro https. Para tener éxito, obviamente, el atacante debe ser capaz de redirigir toda la comunicación de la víctima a su servidor, en lugar de al servidor real. Para ello se emplean diferentes técnicas, como por ejemplo *proxies* transparentes, que se sitúan en la misma red o ruta que el servidor real; *DNS Cache Poisoning* (envenenamiento de caché de DNS), que permite el enrutamiento a IP falsas; la ofuscación de URL, que permite redirigir el tráfico de datos a su servidor; o configurando el *proxy* en el navegador.

Ataques del tipo *cross-site scripting*, igualmente conocidos como CSS o XSS. En este caso el engaño consiste en introducir código o URL falsas en una web real. De este modo la mayor parte del contenido web es original, sin embargo una parte, la referida a la información sensible, está construida para obtener los datos objetivo sin que el usuario pueda detectar anomalías.

En la actualidad los navegadores son aplicaciones altamente sofisticadas; sin embargo, a pesar de ello en cada versión aparecen nuevas vulnerabilidades, ya que a medida que crece el número de funcionalidades que ofrecen, también lo hacen las posibilidades de que los *hackers* las aprovechen, como

es el caso de elementos añadidos al navegador o *add-ons* como Flash, RealPlayer y otras aplicaciones embebidas. El aprovechamiento de estas vulnerabilidades en el cliente posibilita, por ejemplo mediante el uso de *exploits* falsear la dirección que aparece en el navegador. De esta manera, se podría redirigir el navegador a un sitio fraudulento, mientras que en la barra de direcciones del navegador se mostraría la URL del sitio de confianza. También es posible aprovechar los fallos de aplicaciones Java, que permiten embeber servidores remotos en la red local del usuario. Mediante estas técnicas, también es posible falsear las ventanas emergentes *(pop-ups)* abiertas desde una página web auténtica. Algunos ataques de este tipo también hacen uso de *exploits* en sitios web fraudulentos que, aprovechando alguna vulnerabilidad de Internet Explorer o del sistema operativo del cliente, permiten descargar troyanos de tipo *keylogger* que robarán información confidencial del usuario.

2.2.2. Identity theft *y cibersuplantación de identidad o* spoofing

Precisamente el *spoofing* o suplantación de identidad, como expresión concreta y tecnológicamente avanzada del género de conductas que tratan de configurar el *identity theft* o robo de identidad, sería el siguiente grupo de ciberataques que no siendo nuevos adquieren una dimensión nueva de lesividad en el ciberespacio. El robo de identidad podría definirse como la adquisición en todo o en parte por un sujeto de los datos de otro sujeto para su posterior uso como si le pertenecieran a él [68]. No obstante, cuando se habla de *identity theft* se suele utilizar presuponiendo el futuro uso delictivo de la suplantación, esto es, como la utilización o explicación de los datos de identificación personal u otro tipo de información de la persona como el nombre, el número de DNI, etc., para cometer fraude o participar en otras actividades ilegales [69]. Aunque, como recuerdan los autores pioneros del estudio del *spoofing*, la suplantación de personalidades también se produce fuera del mundo virtual [70], lo cierto es que en el ciberespacio el robo de identidad resulta más sencillo de ejecutar y potencialmente mucho más peligroso: primero porque la eliminación de la inmediatez física y las posibilidades técnicas para la obtención de información personal y para la simulación, hacen que sea posible obtener datos privados necesarios para

---

[68] Lo define Cilli como «el uso de información sobre una persona obtenida desde Internet, con el propósito de identificarse a uno mismo como tal persona para llevar a cabo acciones ilegales», CILLI, C., «Identity Theft: A New Frontier for Hackers and Cybercrime», en *Information Systems Control Journal*, vol. 6, 2005, p. 1.

[69] CHAWKI, M., y ABDEL WAHAB, M., «Identity Theft in Cyberspace: Issues and Solutions», en *LE*, vol. 11, núm. 1, printemps/spring, 2006, p. 2.

[70] FELTEN, E. W.; BALFANZ, D.; DEAN, D., y WALLACH, D. S., «Web Spoofing: An Internet Con Game», en *Technical Report,* 540-96, Department of Computer Science, New Jersey, Princeton University, 1996, p. 2.

suplantar a la persona y actuar directamente haciéndose pasar por ella [71]; segundo porque, como ya se ha visto, son múltiples las personas conectadas en el ciberespacio que realizan operaciones financieras y de cualquier otro tipo. En definitiva, que Internet no sólo es el medio a través del cual se puede realizar el *identity theft*, sino que es la razón del gran riesgo que conlleva el mismo en la actualidad, al haber aumentado significativamente en el ciberespacio la necesidad de utilizar los datos personales para realizar transacciones, operaciones o acciones, no siempre comerciales, por parte de los titulares de esa identidad [72].

Hay que tener en cuenta, por otro lado, que si bien el robo de identidad suele realizarse generalmente como primer paso para la ejecución posterior de algún tipo de fraude informático, generalmente el *phishing*, dada la importancia actual de la denominada identidad digital, esta suplantación no sólo encierra un riesgo para el patrimonio de las personas, sino también para muchos otros bienes jurídicos como posteriormente se analizará en profundidad [73]. El robo de identidad en Internet se puede llevar a cabo de muchas formas, desde las más sencillas en las que se acude a la ingeniería social para la suplantación de la personalidad, hasta las más complejas en las que se utiliza la ingeniería informática para lograr los distintos mecanismos existentes para la identificación de los sistemas que actúan en el ciberespacio. En estas últimas es donde debe situarse el *spoofing* que, a su vez, también puede ser poco o muy elaborado.

En la actualidad, se diferencian por lo menos cinco formas de *spoofing*: *IP spoofing*, en el que mediante la utilización de programas específicamente destinados a ello se sustituye la dirección IP original por otra; el *ARP spoofing*, en el que se falsean las denominadas tablas ARP de una víctima para llevar a su sistema MAC a que envíe los paquetes al *host* atacante en vez de a su destino; el *DNS spoofing*, en el que lo que se modifica es el nombre de dominio-IP de un servidor DNS, aprovechando alguna vulnerabilidad, lo cual se suele utilizar para el *pharming* en el que el sujeto pone la dirección web de una entidad bancaria oficial y se le remite a una web falsa; el *web spoofing*, quizás el más común de todos estos ataques, en el que a través de un enlace u otras formas de engaño, se hace pasar una página web, imitada y albergada en otro servidor, por la real, por medio de un código que solicita la información requerida por el sistema víctima a cada servidor original y remite a la web falsa, y, por último, es el *mail spoofing*, consistente en la suplan-

---

[71] Así, señalan Chawki, M., y Abdel Wahab, M., «Identity Theft...», *op. cit.,* pp. 3 y ss., que la evolución que han supuesto las TIC en la forma de realizar transacciones comerciales, especialmente al eliminar la inmediatez física entre vendedor y comprador que tenía que producirse en un determinado momento, ha modificado, en el sentido de aumentar, la importancia de los datos personales, pues en la actualidad sólo con algunos de ellos ya se puede realizar un acto de disposición comercial.

[72] Cilli, C., «Identity Theft...», *op. cit.,* p. 1.

[73] Véase *infra* cap. III.

tación de la dirección de correo electrónico de otras personas o entidades, utilizada generalmente para enviar *spam* o como comienzo de la dinámica de ataque del *phishing*[74].

2.2.3. *El ciberespionaje*

En ocasiones como forma de robo de identidad, pero en realidad como conducta con singularidad propia, también podríamos situar el denominado espionaje informático, o *snooping* (en sentido amplio)[75], ya sea de carácter empresarial para el descubrimiento de secretos comerciales, ya sea para la interceptación de las comunicaciones personales mediante el acceso a correos electrónicos, conversaciones por medio de cualquiera de las redes telemáticas, etc., en esta modalidad de cibercriminalidad en la que las redes son el nuevo instrumento desde el que se debe interceptar la comunicación. Al fin y al cabo, el espionaje, tanto de datos personales como de información relevante para las empresas, ha existido siempre, pero de nuevo el ciberespacio dota de una potencial lesividad a estos comportamientos, potencialidad lesiva no existente hasta antes de la revolución de las TIC, dado que hoy casi toda la información sensible está contenida en sistemas informáticos que, a su vez, están conectados a redes telemáticas que unen a personas en todo el mundo.

El espionaje informático se puede realizar, como luego se verá con más profundidad, bien por un *insider* que aprovecha su situación en la empresa o su relación con la persona de confianza para dañarla, bien por un *hacker* que accede directamente al sistema informático, o por medio de todo un *software* cuya finalidad primera es la obtención de datos de muy diverso tipo y con diferentes objetivos últimos. Este es el *software* que se denomina *spyware* y que puede ser enviado por correo electrónico por el atacante o ser descargado inconscientemente por la víctima al descargar algún otro tipo de *software*. El *spyware* es un *software* que se instala en un sistema informático y que recopila determinada información de éste que después envía a otro sistema. Por medio del *spyware* se puede acceder a información personal o a secretos de empresa obtenidos en correos electrónicos y otro tipo de mensajes, pero generalmente este tipo de *software* lo que recaba es todo un conjunto de datos que son necesarios para realizar otros ataques posteriores a la intimidad o al patrimonio del sujeto como sus claves informáticas o bancarias, la dirección IP, los números de teléfono, etcétera.

Especial importancia tiene dentro del *spyware* el uso de *sniffers* y *keyloggers*, programas que pretenden en última instancia captar información bien

---

[74] Véase Isla Cortés, J. I. M., «Seguridad en redes informáticas» (2005). En Internet en *http://cybertesis.uach.cl/tesis/uach/2005/bmfcii.82s/doc/bmfcii.82s.pdf* (última visita el 30 de noviembre de 2010), pp. 88 y ss.

[75] El *snooping* es el acceso no autorizado a datos de otros, por lo que todo espionaje informático es, en última instancia, *snooping*.

para el espionaje industrial o bien para su posterior uso en ataques de *spam*, *phishing*, *botnet*, etc. Los *sniffers* son programas de captura de tramas de información que no están destinadas a él. En realidad, lo que hacen los *packet sniffers* es capturar todo el tráfico que viaja de una determinada forma o con unas determinadas características por la Red. Ello puede ser utilizado con la finalidad de detectar fallos en redes o sistemas o incluso *hackers*, con finalidad maliciosa, para capturar de forma automática contraseñas de sistemas informáticos o nombres de usuario de la Red para el posterior acceso informático o envío de *spam*, respectivamente, para tratar de interceptar mensajes de correo electrónico o espiar conversaciones de chat, etcétera.

En cuanto a los *keyloggers,* se trata de un tipo de *hardware* o *software*, el que más interesará aquí, que se dedica a registrar las pulsaciones que se realizan en el teclado con la finalidad de memorizarlas y posteriormente enviarlas al sujeto que posteriormente las utilizará para acceder a la información o al patrimonio de la víctima. Aunque en el ámbito de la empresa o incluso en las relaciones personales, en la misma familia, puede comenzar a darse el uso de *hardware keyloggers*, lo que aquí más nos interesa son aquellos casos en los que, a través de un troyano o una *backdoor*, se instala en un sistema informático ajeno un *software* que, gracias al registro de pulsaciones, consigue que el cibercriminal acceda a contraseñas del sistema o a claves bancarias entre otros datos.

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

Algunos autores sitúan dentro del *spyware*, aunque como conductas invasoras de la intimidad con menor lesividad [76], las denominadas *cookies*, archivos que almacenan información del usuario en su propio sistema y que sirven para que los sitios web identifiquen al visitante. La tecnología de las *cookies* permite que una página web, por defecto, inserte con disimulo su propio identificador en el terminal de forma permanente para poder así rastrear el comportamiento del individuo en Internet [77].

De este modo, la conservación de esa información permite al remitente, como ha advertido Morón Lerma, realizar una «fotografía digital del internauta, conocer su dirección, gustos, preferencias o entretenimientos, pudiendo efectuar un rastreo complejo de las actividades del usuario en la

[76] Desde luego, comparado con la gravedad que conllevan los programas rastreadores *sniffers* y el s*pyware* que permite el acceso directo a la información contenida en el sistema. Así, Morón Lerma, E., «Derecho penal y nuevas tecnologías. Panorama actual y perspectivas futuras», en Casanovas, P. (ed.), *Internet y pluralismo jurídico: formas emergentes de regulación,* Granada, Comares, 2003, p. 104.

[77] Poullet, Y., «Hacia nuevos principios de protección de datos en un nuevo entorno TIC», en *IDP*, núm. 5, 2007, p. 36.

Red»[78]. Para esto sirve particularmente la técnica denominada *data mining* o minería de datos, por la que se busca toda la información relativa a una persona, incluso aquella aparentemente menos trascendente, tratando de enlazarla y relacionarla posteriormente para poder configurar un retrato lo más certero posible de la persona contra la que se va a realizar el fraude o similar.

2.2.4. *Ciberblanqueo de capitales y ciberextorsión*

En otro orden, la anteriormente comentada relación entre el crimen organizado y la cibercriminalidad, hace que en la actualidad se utilice el ciberespacio y sus diferentes servicios para el blanqueo de capitales derivados, normalmente, de las actividades cibercriminales de dichos grupos[79]. Aunque existen muy diversas técnicas para el blanqueo del dinero virtual, las más comunes hasta la fecha son el uso de mulas para el envío de dinero y el logro de divisas por medio de los juegos *online*. Cuando se habla de las mulas, sobre todo en el ámbito del *phishing*, se hace referencia a los usuarios de Internet que tienen (o abren) cuentas bancarias, y que son reclutados vía web bajo la apariencia de un contrato de trabajo realizado desde casa, y que consiste en la recepción en sus cuentas bancarias de dinero y su envío, habitualmente por medio de sistemas como Western Union, o también por transferencia bancaria, a las cuentas corrientes de los cibercriminales a cambio de una pequeña comisión. En cuanto a las webs de juego *online,* éstas suponen la creación de una economía virtual en las que se intercambia el dinero real por dinero virtual para participar en los juegos. Esto es aprovechado por las organizaciones criminales para primero intercambiar el dinero real por dinero virtual y después volverlo a recuperar como real complicando la perseguibilidad de los bienes ilícitos.

Igualmente tiene relación con las bandas organizadas el siguiente comportamiento criminal que únicamente cambia en cuanto a que el ciberespacio es el nuevo medio intimidatorio utilizado, en este caso, aquello con lo que se amenaza. Me refiero a la extorsión realizada por cibercriminales, generalmente por bandas organizadas, consistente en la solicitud de importantes cantidades económicas a cambio de cesar en la realización de algún

---

[78] MORÓN LERMA, E., «Derecho penal y nuevas...», *op. cit.,* p. 104. Recuerda la autora que la proliferación de estas conductas con el subsiguiente envío de publicidad no autorizada ha provocado una respuesta normativa en la dirección de permitir tales dispositivos sólo cuando haya autorización directa de los afectados, concretada en la directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. Al respecto de esta norma y de la configuración del Derecho de datos en relación con las *cookies* véase el completo análisis de POULLET, Y., «Hacia nuevos principios...», *op. cit.,* especialmente pp. 41 y ss.

[79] WILLIAMS, P., «Organized Crime and Cybercrime: Synergies, Trends, and Responses», en *ATC,* vol. 6, agosto de 2001, p. 4.

tipo de ciberataque o incluso de empezar a ejecutarlo. Al igual que en los casos de extorsión normal, el criminal aprovecha el hecho de que para la víctima puede resultar más sencillo, e incluso beneficioso, atender a la solicitud del criminal y no recibir el ataque que ser víctima de él y tratar de defenderse posteriormente. En el caso de los comportamientos cibercriminales estas conductas parecen proliferar en relación con las páginas web dedicadas a las apuestas y a los juegos de azar *online*, a las que les interesa pagar cantidades no demasiado grandes a las mafias a cambio de no sufrir un ataque de denegación de servicios o similares en fechas concretas que les puede paralizar la página web y hacerles perder cantidades significativamente superiores [80].

2.2.5. *El ciberacoso*

El ciberespacio no sólo es un lugar para las relaciones de tipo económico, también es un medio de intercomunicación personal o social que, como decíamos, se ha popularizado a todos los sectores de la población. Por ello será del mismo modo común, dentro de esta categoría de infracciones tradicionales en las que lo que cambia es el medio de realización de las mismas (ahora virtual), los ataques a bienes personalísimos caracterizados ahora simplemente porque el medio de realización del mismo es Internet u otras TIC. Amenazas, coacciones, injurias, calumnias y otras agresiones al honor o a la libertad pueden realizarse «como siempre» pero a través del ciberespacio. Destaca entre todo ello el ciberacoso, entendido como una macrocategoría englobadora de todas las conductas en las que se aprovecha el uso de distintos instrumentos de comunicación como el Messenger, el correo electrónico, el sistema de comunicación oral Skype o las redes sociales como Twitter o Facebook para realizar el atentado contra la libertad de otra persona [81]. Tienen

---

[80] KSHETRI, N., «The Simple Economics of Cybercrimes», en *IEEE Security and Privacy. The IEEE Computer Society,* 2006, quien cita como ejemplo el pago de 30.000 dólares que desembolsó *BetWWWTS.com* ante la posibilidad de no poder gestionar más de cinco millones de dólares durante el tiempo que la web iba a estar parada por el ciberataque.

[81] Marco apunta que podemos entender como ciberacoso «la amenaza, el hostigamiento, la humillación o la molestia que una persona ejerce sobre otra, haciendo uso para ello de diferentes tecnologías que, a título de ejemplo pueden ser el correo electrónico, los chats, páginas web, la telefonía móvil, las cámaras digitales, las videoconsolas, etc.», MARCO MARCO, J. J., «Menores, ciberacoso y derechos de la personalidad», en GARCÍA GONZÁLEZ, J. (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet,* Tirant lo Blanch, 2010, p. 98. Pardo Albiach se refiere al ciberacoso como «el uso de información electrónica y medios de comunicación tales como *e-mail,* mensajería instantánea, mensajes de texto, blogs, teléfonos móviles, buscas, y *websites* (páginas web) difamatorios para acosar a un individuo o grupo, mediante ataques personales u otros medios», PARDO ALBIACH, J., «Ciberacoso: Cyberbullyng, grooming, redes sociales y otros peligros», en *ibid.,* p. 54. Chacón Medina lo define como la «conducta repetitiva de acercamiento, acoso y/o amenazas a otra persona, usando alguna de las herramientas de Internet (*e-mail,* listas, salas de charla, tableros electrónicos, mensajes instantáneos...), u otra vía o instrumento electrónico de comunicación», CHACÓN MEDINA, A., «Una nueva cara de Internet: el acoso», en *Revista Eticanet,* núm. 1, Granada, julio de 2003, pp. 1 y ss.

que concurrir, por tanto, dos elementos: que el sujeto activo atente contra la libertad o dignidad de la víctima y que esta conducta se produzca mediante el uso de las nuevas tecnologías [82]. Aunque el ciberacoso se puede dar de muy distintas formas, las más comunes han dado lugar a categorías propias como son el *cyberbullying* o ciberacoso escolar o a menores; el *cyberstalking* o ciberacoso continuado propiamente dicho y el ciberacoso sexual, dentro del cual estaría el *online grooming*. Las analizaré por separado.

2.2.5.1. El *cyberbullying* o acoso escolar o a menores en Internet

Como unión entre el prefijo *cyber* y el término *bullying*, utilizado para hacer referencia al acoso escolar o entre menores, el *cyberbullying* se concibe por la literatura especializada como una variante del ciberacoso en la que un menor atormenta, amenaza, hostiga, humilla, o molesta de alguna otra manera a otro, haciendo uso de Internet, teléfono móvil, videoconsola o alguna otra tecnología telemática de comunicación [83]. Así ha definido el *cyberbullying* Marco, y similar definición utiliza Belsey, creador de las páginas *www.cyberbullying.org* y *www.bullying.org*, al referirse a él como el uso de las TIC —entre las que menciona el correo electrónico, los mensajes de teléfono móvil (SMS y MMS), la mensajería instantánea y los blogs— por parte de un individuo o un grupo, para, deliberadamente y de forma repetitiva y hostil, dañar a otro [84].

En el *cyberbullying,* pues, se utiliza el ciberespacio para infligir a la víctima daño psicológico de forma voluntaria y repetida [85], o, como han señalado desde la psicología, Pérez Martínez y Ortigosa Blanch, «para ejercer el acoso

---

[82] Si bien hay determinados autores que exigen también la concurrencia de un tercer elemento para que podamos hablar de ciberacoso, como es la *continuidad* en las acciones de humillación, hostigamiento o molestia. Este tercer elemento determina, explica Marco Marco, «que un hecho aislado no es ciberacoso, no obstante, sí es cierto que una acción puntual en el entorno virtual del acosado puede suponerle un sufrimiento prolongado durante un tiempo (por ejemplo, una determinada imagen colgada en la Red)»; MARCO MARCO, J. J., «Menores, ciberacoso y derechos de la personalidad», en GARCÍA GONZÁLEZ, J. (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet,* Tirant lo Blanch, 2010, p. 98.

[83] MARCO MARCO, J. J., «Menores, ciberacoso y derechos...», *op. cit.,* p. 99. Similar es la definición que ofrece el profesor Pardo Albiach, al referirse al *cyberbullying* como la situación que se da cuando «un niño, adolescente o preadolescente es atormentado, amenazado, acosado, humillado y avergonzado por otra persona desde Internet, mediante medios interactivos, tecnologías digitales y teléfonos», especificando posteriormente que este acoso debe darse por parte de un menor de edad hacia otro menor. PARDO ALBIACH, J., «Ciberacoso: Cyberbullyng, grooming, redes sociales y otros peligros», en GARCÍA GONZÁLEZ, J. (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet,* Tirant lo Blanch, 2010, p. 56.

[84] BELSEY, B., «Cyberbullying: An Emerging Threat to the "Always On" Generation», 2005. En Internet, en *http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf* (última visita el 7 de octubre de 2011).

[85] PATCHIN, J. W., e HINDUJA, S., «Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying», en *YVJJ,* vol. 4, 2006, p. 148. También definen los autores al *ciberbully*, o ciber-

psicológico entre iguales» [86]. Al fin y al cabo las TIC conforman una importante forma de expresión de los jóvenes de la actualidad, por lo que no es de extrañar que los usos y formas de relación, incluso los no deseados, que se dan en el espacio físico se repliquen o extiendan al ciberespacio. En este sentido, y aunque sobre ello se volverá más adelante cuando se realice el perfil victimológico del ciberacosado [87], puede decirse que el *cyberbullying* no sustituye, sino que complementa muchas conductas de *bullying* entre menores, debido a la popularización también en ese espectro de la población del uso de las TIC en general, y de las redes sociales en particular. Así, se ha dicho que frente al *bullying* tradicional, el poder que se ejerce sobre la víctima ya no es físico ni (tan sólo, pues también puede serlo) social, sino que se trata de un poder en línea que se deriva de la unión entre la crueldad asociada a este tipo de intimidación y la habilidad: es el joven capaz de navegar y dominar el mundo electrónico, el que está en una posición de poder en relación con una víctima y puede utilizar las TIC para acosar a sus víctimas [88].

Se ha discutido en la literatura dedicada a la materia sobre la consideración del *cyberbullying* como una mera modalidad del *bullying* —en la línea de la definición que ofrece el profesor Marco [89]— o más bien como un fenómeno con identidad propia y caracteres, en lo relativo al agresor y a la víctima, particulares [90]. Por otro lado, hay quien, como Hernández Prados y Solano Fernández, considera que lo que sucede es que existen dos tipos de *cyberbullying*: «Aquél que actúa como reforzador de un *bullying* ya emprendido, y aquella forma de acoso entre iguales a través de las TIC's sin antecedentes» [91] que denominaré *cyberbullying* puro. Explican las autoras que en la primera modalidad se acude al *cyberbullying* cuando las formas tradicionales de acoso ya no son eficientes o satisfactorias para el acosador, utilizando la Red para ver amplificados los efectos sobre la víctima. En realidad probablemente se acuda al *cyberbullying* cuando el *bullying* no sea «suficiente» para el acosador, ofreciendo el ciberespacio alternativas o mayores posibilidades para su ejercicio de poder psicológico sobre la víctima. Frente a esta modalidad, se refieren las autoras con razón a otra modalidad en la que no tendría por qué haber un motivo basado

---

matón, como el agresor malévolo que busca explícita o implícitamente placer o beneficio con el maltrato de otros individuos.

[86] PÉREZ MARTÍNEZ, A., y ORTIGOSA BLANCH, A., «Una aproximación al ciberbullying», en GARCÍA GONZÁLEZ, J. (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet,* Tirant lo Blanch, 2010, p. 15.

[87] Cap. V.3.2.2.

[88] PATCHIN, J. W., e HINDUJA, S., «Bullies Move Beyond the Schoolyard...», *op. cit.,* p. 148.

[89] Es consciente este autor de que ambos fenómenos responden a causas distintas, «manifestándose de formas muy diversas y contando con estrategias de abordamiento y consecuencias que también difieren».

[90] PATCHIN, J. W., e HINDUJA, S., «Bullies Move Beyond the Schoolyard, *op. cit.,* pp. 149 y ss.

[91] HERNÁNDEZ PRADOS, M. A., y SOLANO FERNÁNDEZ, I. M., «Ciberbullying, un problema de acoso escolar», en *RIED,* vol. 10, 2007, pp. 17-36.

en una relación personal anterior para que se llevase a cabo el acoso, pues no hay antecedentes presenciales. Se trataría, por tanto, de un ciberacoso puro, en el sentido de que lo ejercería un menor contra otro al que, o bien no conoce en el espacio físico y sólo se relaciona con él a través de la Red, o bien lo conoce pero no realiza sobre él ningún acto de acoso en el espacio físico. Evidentemente no parece arriesgado adelantar que las características de estas dos modalidades de *cyberbullying*, del que se utiliza como refuerzo del acoso presencial, y del que se realiza únicamente en el ciberespacio sin que exista entre agresor y víctima ninguna relación de acoso en el espacio físico, serán distintas. Y es en este sentido en el que yo creo que asiste razón a Pérez Martínez y Ortigosa Blanch cuando señalan que, a pesar de compartir características con el *bullying,* el *cyberbullying* tiene una autonomía propia, pues atiende a otras causas, se manifiesta de formas muy diversas y sus estrategias de abordamiento y consecuencias también difieren.

Al fin y al cabo, detrás de la multiplicidad de definiciones del *cyberbullying* y de la aparente discusión sobre el carácter autónomo o «derivado» del ciberacoso escolar, hay sin embargo varios acuerdos fundamentales sobre su significado y alcance. El primero, que es tanto *cyberbullying* el realizado en el marco de una actividad de *bullying,* en el que se suma al acoso presencial el ejercido en el ciberespacio; como aquel, también realizado por medio de Internet contra una persona sobre la que no se ejerce ningún tipo de acoso fuera del ciberespacio.

El segundo acuerdo consiste en que, con esta definición, queda fuera del ámbito del *cyberbullying* el acoso de índole estrictamente sexual y también los casos en los que intervienen personas adultas. Por consiguiente, tanto el acosador como el acosado en el *cyberbullying* deben ser menores de edad, tratándose por tanto de un «acoso psicológico entre iguales» [92], elemento común entre el *bullying* y el *cyberbullying.* En cuanto a la desvinculación entre el *cyberbullying* y el acoso sexual, también existe acuerdo unánime de la literatura [93], si bien hay que tener en cuenta, como ha señalado Agustina [94], que en muchas ocasiones el *cyberbullying* se produce como consecuencia de otros fenómenos, como el *sexting,* utilizándose para el acoso las fotografías realizadas por parte de menores, de desnudos completos o partes desnudas,

---

[92] Marco Marco, J. J., «Menores, ciberacoso y derechos de la personalidad», en García González, J. (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet,* Tirant lo Blanch, 2010, p. 99.

[93] Por todos, Pérez Martínez, A., y Ortigosa Blanch, A., «Una aproximación al ciberbullying», en García González, J. (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet,* Tirant lo Blanch, 2010, p. 15.

[94] Agustina Sanllehí, J. R., «¿Menores infractores o víctimas de pornografía infantil? Respuestas legales e hipótesis criminológicas ante el *Sexting*», en *Revista Electrónica de Ciencia Penal y Criminología,* 12-11, 24 de diciembre de 2010, *http://criminet.ugr.es/recpc/12/recpc12-11.pdf*, pp. 11:6 y 11:34.

como medio de presión, chantaje, explotación y/o ridiculización contra el menor fotografiado.

Y es que son tantas las conductas aparentemente inocuas entre los adolescentes en el uso de las tecnologías, que pueden derivar posteriormente en *cyberbullying*, que la preocupación por este fenómeno ha llegado tanto a las instituciones estatales, como a los organismos de la Unión Europea. En tal medida es así, que la Comisión Europea firmó en 2009, en el Día para una Internet más segura, un acuerdo con las principales empresas de la web (Facebook, Google/YouTube, Microsoft Europe, Myspace, Yahoo! Europe, entre otras), en el que se pretendían tomar medidas para capacitar a los adolescentes a enfrentarse a los riesgos que puedan encontrar en línea, en el que se hacía referencia expresa al *cyberbullying* como uno de los principales fenómenos a erradicar [95]. En esta misma línea de estudio y prevención del problema del *cyberbullying* por parte de la Unión Europea, la encuesta *EU Kids online II* promovida por la Comisión Europea en su programa *Safer Internet,* realizada en marzo de 2011, desvela que la incidencia del *cyberbullying* entre los internautas españoles de 15 y 16 años es del 7 por 100 [96]. Y es que ya en una encuesta anterior, también financiada por la Comisión Europea, se había puesto de relieve que el fenómeno del *cyberbullying* es el riesgo *online* más frecuente entre los menores europeos [97].

2.2.5.2. El *cyberstalking* (y el *online harassment*)

El *cyberstalking* podría entenderse, siguiendo a Basu y Jones, como el uso de Internet u otra tecnología de comunicación para hostigar, perseguir o amenazar a alguien [98]. La palabra *cyberstalking* viene de la unión del prefijo *cyber,* derivado de la palabra *cyberspace,* y del término *stalking*, que se refiere, como plantean Pathé y Mulen a los comportamientos en los que un individuo inflige a otro intrusiones o comunicaciones repetidas y no deseadas [99].

El término *stalking* surgió en los años noventa en Estados Unidos, en concreto en el Estado de California tras la muerte de dos actrices famosas a manos de personas que las habían acosado y perseguido durante un tiempo [100]. Aunque su uso se propagó a países de Europa como Alemania o

---

[95] Este acuerdo se enmarca en la planificación de la Unión Europea para la protección de la infancia y la juventud en el período 2009-2013. En Internet, en *http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/232&format=HTML&aged=0&language=ES&guiLanguage=en*.

[96] En Internet, en *http://www.ciberbullying.com/cyberbullying/2011/03/28/el-7-de-los-quinceaneros-espanoles-sufre-bullying-en-internet/*.

[97] En Internet, en *http://www.ciberbullying.com/cyberbullying/2010/10/21/el-ciberbullying-es-el-riesgo-online-que-mas-hace-sufrir-a-los-menores-segun-un-estudio-europeo/*.

[98] Basu, S., y Jones, R., «Regulating cyberstalking», en *JILT,* vol. 22, 2007, p. 13.

[99] Pathé, M., y Mullen, P. E., «The impact of stalkers on their victims», en *BJP*, 1997, p. 12.

[100] Smith, A., *Protection of Children Online: Federal and State Lawes Addressing Cyberstalking, Cyberharassment and Cyberbuylling,* Congressional Research Service, 2009, p. 4.

Italia, y aunque en España hubo una época en que se hicieron manifiestas conductas de persecución, no sólo a famosos, consistentes en esperar a la víctima todos los días en un lugar, o en llamar repetidamente por teléfono y similares, el uso de este término no se encuentra generalizado y de hecho es casi desconocido [101] y, lo que es más relevante, no existe una regulación penal expresa que permita sancionar con claridad todos los casos de *stalking* [102]. Lo cual, obviamente, también puede decirse del *cyberstalking*.

Por su parte, la dinámica de victimización del *stalking* a través de los medios tecnológicos consiste en una combinación de distintas formas de acecho a través de los medios que facilita la tecnología como el chat, foros, redes sociales, etc. Se sustituyen las llamadas de teléfono a horas en que el sujeto está en casa, o las visitas al trabajo y a la casa, así como los seguimientos no deseados, por otras conductas como el envío de decenas de correos o de mensajes a través de las redes sociales, la puesta a disposición del público de fotos, mensajes o correos de la víctima en páginas web, etc. Lo habitual es que el *cyberstalker* elija a su víctima a través de chats, foros, etc., y que cuando seleccione su objetivo, realice una o distintas formas de persecución, como intentar contactar en repetidas ocasiones, amenazar con violencia física, solicitar sexo de forma explícita, enviar imágenes obscenas entre otras, siempre teniendo en cuenta el carácter repetitivo de la acción. Según Pittaro el medio más común empleado por los *cyberstalkers* es el correo electrónico para enviar mensajes de acoso, amenaza, odio, obscenos o incluir imágenes hirientes [103]. Otras formas de *cyberstalking*, aunque menos usadas, son instar a otros usuarios de Internet a acosar o amenazar a la víctima mediante foros o chat, enviar archivos infectados con la intención de dañar el sistema informático de la víctima y el robo de identidad, siendo estos dos últimos considerados como *cyberstalking* cuando el objetivo del agresor sea intimidar a la víctima.

De forma similar a lo que sucedía, con el *cyberbullying*, el principal debate que plantea la comunidad científica es si el *cyberstalking* es una extensión del *stalking* tradicional o debe ser entendido como un fenómeno diferente. Bocij afirma que ambos fenómenos son cualitativamente diferentes y por lo tanto deben entenderse por separado [104]. Bocij y McFarlene's aportan en este sentido tres razones principales: en primer lugar, porque los gobiernos y los medios de comunicación así lo entienden; en segundo lugar, hay

---

[101] Villacampa Estiarte, C., «La respuesta jurídico-penal frente al *stalking* en España: presente y futuro», en *Revista del Instituto Universitario de Investigación en Criminología y Ciencias Penales de la UV*, 2010. En Internet, en *http://www.uv.es/recrim/recrim10/recrim10a03.pdf*, p. 33.

[102] Véase al respecto el completo estudio de Villacampa Estiarte, C., *Stalking y Derecho penal. Relevancia jurídico-penal de una nueva forma de acoso*, Madrid, Iustel, 2009.

[103] Pittaro, M. L., «Cyber stalking: An Analysis of Online Harassment and Intimidation», en *IJCC*, vol. 1, núm. 2, 2007, p. 186.

[104] Bocij, P., «Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet», en *FMPRJI,* vol. 8, núm. 10, 2003.

ciberacosadores que no podrían acosar en el mundo físico; y en tercer lugar, porque las nuevas tecnologías traerán siempre nuevos delitos [105]. Henson mantiene la misma postura afirmando que entre ambos fenómenos existen tres diferencias claras [106]. La primera de ellas es referida a la proximidad física entre víctima y victimario. Mientras que para el *stalking* tradicional agresor y víctima deben estar en el mismo espacio físico, en el *cyberstalking* no es necesario [107]. Esto a su vez repercute en el tiempo pues si en el fenómeno tradicional hay inmediatez temporal cuando existe proximidad física, en el modo cibernético el tiempo de comisión puede ampliarse, pues el agresor puede mandar un *e-mail* amenazante pero pueden pasar varios días hasta que la víctima lo lea. La tercera diferencia viene determinada por el tipo de elementos de protección eficaz. En el *stalking* existen elementos físicos y sociales que actúan como sistemas de seguridad como el hogar, los amigos y los familiares, mientras que en la modalidad cibernética la seguridad viene dada por elementos electrónicos como sistemas de cortafuegos o por las conductas de autoprotección ejercidas por la víctima, como no hacer pública determinada información o privatizar las cuentas en las redes sociales.

Frente a esta posición, autores como Sheridan y Grant consideran que el *cyberstalking* debe ser entendido como una extensión del *stalking* tradicional porque comparten elementos comunes, como el proceso de acoso, el efecto sobre las víctimas, el efecto sobre terceros, la respuesta de las víctimas y el género del acosador, entre otros [108]. En el mismo sentido considera Pittaro que ambos comportamientos vienen alimentados por la rabia, el poder, el control y la ira, siendo el único elemento distintivo entre ambos fenómenos el medio empleado, el medio electrónico, principalmente Internet y otros dispositivos electrónicos de comunicación por lo que son iguales [109].

En mi opinión ambas consideraciones son compatibles. El *cyberstalking* puede ser entendido como una extensión del *stalking*, en cuanto que se ejecuten las mismas conductas de acecho, amenaza y acoso ejercidas con idéntico ánimo por un agresor pero empleando para ello medios tecnológicos. Pero esto no es incompatible con la afirmación, sobre la que luego se profundizará con carácter general, relativa a que el ciberespacio modifica el ámbito de oportunidad criminal y, por tanto, incidirá en el evento delictivo y, por ello, en el ciberagresor y en la víctima. El *cyberstalker* seguirá siendo

---

[105] Bocij, P., y McFarlane, L., «Seven fallacies about cyberstalking», en *PSJ*, núm. 149, 2003.

[106] Henson, B., «Cyberstalking», en Fisher. B. S., y Lab, S. P. (eds.), *Encyclopedia of Victimology and Crime Prevention*, Thousand Oaks, CA, Sage, 2010, p. 254.

[107] El mismo argumento plantea Pittaro, M., «Cyber Stalking: Typology, Etiology, and Victims», en Jaishankar, K. (ed.), *Cyber Criminology. Exploring Internet crimes and criminal behavior*, Boca Ratón, CRC Press, 2011, p. 283.

[108] Sheridan, L., y Grant, T., «Is cyberstalking different?», *PCL,* 2007.

[109] Pittaro, M., «CyberStalking: Typology, Etiology...», *op. cit.,* p. 278.

un sujeto que seleccionará a su víctima y la acosará aunque la misma le manifieste su intención de no comunicar más con él, y sólo cambiará, aunque puede significar mucho, la no necesidad de un contacto físico entre agresor y víctima, las posibilidades que da el anonimato para que las conductas de acoso se perpetúen, o los cientos de miles de víctimas a las que puede acceder el *stalker* cuando su ámbito sea el ciberespacio.

Cuestión distinta sucede con el que podríamos denominar *cyberstalking* en sentido amplio o suma de actos de *cyberharassment.* En efecto, hasta el momento nos hemos referido al *cyberstalking* en sentido estricto, aquel que cumple los requisitos exigidos para el *stalking* pero se realiza en el ciberespacio, tal y como es entendido por Pathe y Mullen [110], Basu y Jones [111] o Fraser *et al*. [112]. Hay, sin embargo, otras definiciones de *stalking* que se limitan a citar los tipos de comportamiento que puede llevar a cabo el *cyberstalker* [113] incluyendo conductas concretas y no una referencia general al acoso continuado. Así, Henson entiende por *cyberstalking* «cualquier tipo de conducta que utiliza dispositivos electrónicos de comunicación, a sabiendas y voluntariamente de cometer cualquiera de los siguientes actos en dos o más ocasiones, con ningún propósito legítimo: ponerse en contacto o intentar contactar con alguien después de haberle pedido esa persona que cesara en el contacto; acosar, atormentar o atemorizar a alguien; robar o intentar robar la identidad de alguien o información acerca de esa persona para perjudicarle; hacer insinuaciones sexuales no deseadas o injustificadas hacia alguien; y amenazar con causar un daño físico a alguien» [114]. Los autores que aplican este tipo de definiciones consideran que para que exista un caso de *cyberstalking* deben haberse producido alguna o varias de las conductas planteadas en dos o más ocasiones [115]. En realidad aquí estaríamos más cerca del *cyberharassment*, también llamado *online harassment*, que es el término que suele utilizarse para referirse a los actos concretos, y no continuados, de *bullying* o *stalking* en el ciberespacio.

La primera de las consecuencias de esta visión distinta del *cyberstalking* es la diferencia abismal que presentan los estudios respecto a la prevalencia del fenómeno. Así observamos que entre los estudios americanos encontramos porcentajes de victimización que oscilan entre el 3,7 por 100 de los encuestados y el 82,1 por 100, aunque haciendo una estimación entre estudios, el porcentaje se sitúa aproximadamente en el 20 por 100 de los

---

[110] PATHÉ y MULLEN: «The impact...», *op. cit.*, p. 12.

[111] BASU, S., y JONES, R., «Regulating...», *op. cit.,* p. 13.

[112] FRASER, C.; OLSEN, E.; LEE, K.; SOUTHWORTH, S., y TUCKER, S., «The new age of stalking: technological implications for stalking», en *JFCJ,* vol. 61, núm. 4, 2010, pp. 39 y ss.

[113] REYNS, B. W., HENSON, B., y FISHER, B. S., «Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization», en *CJB*, 2011; HENSON, B., «Cyberstalking»..., *op. cit.*

[114] HENSON, B., «Cyberstalking», *op. cit.,* pp. 253 y ss.

[115] REYNS, B., «Being Pursued Online...», *op. cit.,* p. 14.

sujetos estudiados que han sufrido algún tipo de comportamiento de *cyberstalking* [116]. Por ejemplo, en la encuesta de victimización nacional realizada en Estados Unidos (*National Crime Victimization Study*) obtuvieron que el 26 por 100 de las víctimas de *stalking* habían sufrido algún tipo de *cyberstalking* [117]. Es evidente, en todo caso, que el *cyberstalking*, especialmente en su concepción más amplia receptora de cualesquiera concreciones de un acoso no deseado realizado en el ciberespacio, encuentra en la web 2.0 unas condiciones realmente fértiles para desarrollarse como conducta criminal. Será necesario realizar estudios empíricos para tratar de situar la dimensión real del fenómeno, y será necesario hacerlo por medio de una metodología común, dado que las investigaciones realizadas hasta el momento difícilmente permiten hacer comparaciones válidas [118].

2.2.5.3. El ciberacoso sexual, el *sexting,* el *online grooming*

Dentro de esta genérica modalidad de conductas en el ciberespacio en las que se utilizan los nuevos medios para realizar comportamientos criminales tradicionales, tienen especial importancia, por la significación de los intereses puestos en juego, toda una serie de comportamientos relacionados con la negación del ejercicio libre de la sexualidad por parte de los adultos y con la afectación del proceso de formación de tal libertad sexual en los menores. En realidad son muchas y variadas las conductas en las que se aprovecha el uso de distintos instrumentos de comunicación como el Messenger, el correo electrónico, el sistema de comunicación oral Skype o las redes sociales como Twitter o Facebook para realizar el atentado contra la libertad sexual de otra persona. Hay que tener en cuenta que el atentado puede ser de todo tipo, puesto que la popularización del uso de las *webcams* amplía profundamente el catálogo de comportamientos relacionados con la libertad sexual que pueden ser realizados a través de Internet: ya no se trata únicamente de la posibilidad de realizar un acoso sexual por medio de palabras, sino que ya es posible la difusión directa de contenido sexual a un menor o, incluso, la visualización de una actitud sexual de la víctima coaccionada por una amenaza.

De entre todas las conductas posibles una de las más llamativas, por tratarse de un comportamiento relacionado con la libertad sexual de menores de edad, y por haberse convertido en algo usual entre adolescentes, es el denominado *sexting* [119]. Consiste en la realización, por parte de menores, de fo-

---

[116] Henson, B., «Cyberstalking», *op. cit.,* p. 44.

[117] Baum, K.; Catalano, S.; Rand, M., y Rose, K., «Stalking Victimization in the United States», en *BJS,* U. S. Department of Justice, Office of Justice Program, enero, 2009. En Internet, en *http://bjs.ojp.usdoj.gov/content/pub/pdf/svus.pdf* (última visita el 18 de junio de 2012).

[118] Henson, B., «Cyberstalking», *op. cit.,* p. 44.

[119] La locución *sexting* aparece por primera vez en el *Sunday Telegraph Magazine* utilizado por Roberts, Y., «The One and Only», 31 de julio de 2005, p. 22.

tografías propias de desnudos completos o parciales y su envío, generalmente por medio del teléfono móvil, a otros, junto con textos obscenos y con la finalidad de conocer personas o de enviar mensajes de amor o de odio [120]. Aunque en países como China estas actividades han dado lugar a la aplicación de los delitos de pornografía infantil [121], hay varios caracteres que diferencian el *sexting* de esa conducta, especialmente el que los autores sean generalmente adolescentes, como también quienes reciben los mensajes, si bien en muchos casos, esas fotos pueden ser posteriormente utilizadas por el receptor para ser colgadas en la Red [122]. El *sexting* todavía no se ha popularizado en España, pero no deja de ser un fenómeno de riesgo si tenemos en cuenta el estudio de Lenhart, que concluye que el 4 por 100 de los adolescentes de 12 a 17 años propietarios de un móvil en Estados Unidos reconocen haber enviado imágenes de desnudos o muy sugerentes de ellos mismos a otra persona vía SMS, y que el 15 por 100 de ellos admite haber recibido tales mensajes [123].

Recientemente, ha salido a la luz un estudio español llevado a cabo por el Instituto Nacional de Tecnologías de la Comunicación y la empresa Orange que refleja a través de sus cifras que este fenómeno comienza a tener una repercusión importante en España. Este estudio hace la misma diferenciación que Lenhart, entre *sexting activo* (realización de autofotos/vídeos en una postura sexy, provocativa o inapropiada), que entre los niños españoles alcanza asombrosamente el mismo porcentaje que en Estados Unidos (un 4 por 100), y el *sexting pasivo* (recepción de fotos/vídeos de personas de su entorno en una postura sexy, provocativa o inapropiada), que entre los niños españoles es menor que en Estados Unidos (un 8,1 por 100) [124]. No obstante, la mayoría de los estudios empíricos que sobre este fenómeno se han realizado hasta la fecha son estadounidenses [125], y es precisamente el referido

---

[120] LENHART, A., «Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging», en *PIALP*, Washington D. C., 2009. En Internet en *http://www.pewinternet.org/Reports/2009/Teens-and-Sexting.aspx* (última visita el 9 de septiembre de 2010, pp. 1 y ss.).

[121] JAISHANKAR, K., «Sexting: A new form of Victimless Crime?», en *IJCC*, vol. 3, enero-junio de 2009, p. 22.

[122] *Ibid.,* pp. 21 y ss. Añade que esas fotos pueden incluir imágenes de situaciones comprometidas con otras personas, y que pueden ser enviadas para hacer *bullying*, como forma de venganza durante la ruptura de una relación emocional o por propia solicitud de un tercero que tiene relación con esa persona. Aunque se trata de una conducta que puede no tener trascendencia, el *sexting* puede producir traumas tanto a quien lo crea y envía, como a quien lo recibe.

[123] Otras conclusiones interesantes se refieren a que son más bien los adolescentes mayores los que envían y reciben esas imágenes. Véase al respecto, LENHART, A., «Teens and Sexting: How and why...», *op. cit.*

[124] INTECO, ORANGE, «Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles», 2010. Disponible en Internet, en *http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_moviles_menores*, pp. 76 y 77.

[125] Desde el primero que se efectuó que data de diciembre de 2008, con el nombre «Sex and Tech», realizado por *The National Compaign to Prevent Teen and Unplanned Pregnacy*. En Internet, en *http://www.thenationalcampaign.org/sextech/PDF/SexTech_Summary.pdf*.

estudio estadounidense de Lenhart el que concluye que los adolescentes de más edad son más propensos a recibir *sexting*: en Estados Unidos, el 4 por 100 de los niños de 12 años ha recibido un mensaje con imágenes sugerentes (desnudos o semidesnudos) de una persona que conocen. A los 16 años, el 20 por 100. Y a los 17, el 30 por 100. Sin embargo, debemos señalar que el fenómeno del *sexting* no sólo se da en los menores de edad, sino que datos estadounidenses revelan que la incidencia del *sexting* entre los adultos es superior a la detectada entre los propios menores: un 31 por 100 de las personas de 18 a 29 años han recibido *sexts* (imágenes con contenido sexual procedentes de una persona conocida), y un 17 por 100 en la franja de edad de 30 a 49 [126].

Pese a lo alarmante de estas cifras, algunos autores han propuesto no intervenir en los casos de *sexting* por cuanto se diferencian, como ya habíamos apuntado anteriormente, con claridad de los casos propiamente de pornografía infantil [127]. Así, se propone catalogarlo entre los *victimlesscrimes* (delitos sin víctima) [128].

Pero el riesgo del *sexting* no deviene exclusivamente de la propia violación del proceso de formación de la sexualidad que en algunos casos podría suponer, sino más bien de la utilización posterior de las imágenes para otros ataques más graves y para los que ya no habrá consentimiento. Concretamente el *sexting* puede ser el primer paso para posteriores conductas como el *cyberbullying,* un posible abuso o corrupción del menor o la exposición a un chantaje de tipo sexual relacionado con el denominado *grooming*. Además, la difusión de las imágenes a terceros puede desencadenar en conductas de pornografía infantil e incluso puede suponer una presión de tal magnitud en el menor que se ha relacionado con conductas de intento de suicidio y suicidio consumado [129]. Y no siempre el que realice esas conductas será un menor, sino que es perfectamente posible que sea ya un adulto quien acceda a ellas y las utilice con ánimo delictivo.

Debemos insistir en que la peligrosidad de este fenómeno, no reside en la conducta del menor en sí misma, sino que lo preocupante es que ese material, en el contexto tecnológico actual, «puede ser difundido de manera muy fácil y ampliamente, de forma que el remitente inicial pierde totalmente

---

[126] LENHART, A., «Pew Research Center. Pew Internet & American Life Project. Teens, Adults & Sexting: Data on sending & receipt of sexually suggestive nude or nearly nude images by American adolescents & adults». Disponible en Internet en *http://www.pewinternet.org/Presentations/2010/Oct/Teens-Adults-and-Sexting.aspx*.

[127] En el mismo sentido, JAISHANKAR, K., «Sexting: A new form of...», *op. cit.,* pp. 21-25.

[128] Schur definió los *victimlesscrime*s como aquellos intercambios voluntarios de servicios personales u objetos o productos que están socialmente desaprobados y legalmente prohibidos. SCHUR, E. M., *Crimes without victims: Deviant behavior and public policy: Abortion, homosexuality, drug addiction*, Englewood Cliffs, Prentice Hall, 1965, pp. 10 y ss.

[129] AGUSTINA SANLLEHÍ, J. R., «¿Menores infractores...», *op. cit.,* p. 11:6. Así, podrían citarse como casos recientes los suicidios de Amanda Todd y Tim Ribberink.

el control sobre la difusión» [130] de estos contenidos de carácter sexual. Este contexto tecnológico unido a la falta de experiencias y de perspectiva [131], hace que los adolescentes minusvaloren los riesgos asociados a una conducta de *sexting* [132]. De este modo, producen y difunden *sexting* como regalo a su pareja o elemento de coqueteo [133]. También pueden llegar a realizar este tipo de conductas porque alguien se lo pida, o por mera diversión, así como para impresionar a alguien o para sentirse bien (autoafirmación) [134]. Los adolescentes son, por todo ello, más vulnerables a este tipo de conductas, como destaca la novedosa «Guía sobre adolescencia y *sexting*: qué es y cómo prevenirlo» [135], que enumera como motivos de esta especial vulnerabilidad de los adolescentes, la falta de cultura de privacidad, la menor consciencia de los riesgos y el exceso de confianza, la sexualización precoz de la infancia y la inmediatez de las comunicaciones.

Centrando nuestra atención ahora en las diferentes modalidades conductuales, lo primero que debemos señalar es que el *sexting* no tiene por qué realizarse necesariamente, como ya he apuntado antes, a través de un teléfono móvil, ya que existen otros comportamientos que podrían encajar en la anterior descripción de este fenómeno. Así, por ejemplo, sería *sexting* la realización de una foto de un desnudo propio por un menor mediante la *webcam* de un ordenador para mandarla a través de un mensaje privado por una red social a la chica que le gusta, así como también el envío mediante mensajes electrónicos de fotos eróticas propias. Como señala Agustina en su reciente obra [136], entre las posibles formas en las que puede manifestarse este

---

[130] *Ibid.,* p. 11:7.

[131] No obstante, algunos autores afirman que conviene ser prudentes al formular afirmaciones estereotipadas sobre adultos y menores, ZHANG, X., «Charging children with child pornography. Using the legal system to handle the problem of Sexting», en *Computer Law& Security Review,* vol. 26, núm. 3, 2010, pp. 251-259. En Internet, en *http://ac.els-cdn.com/S026736491000052X/1-s2.0-S026736491000052X-main.pdf?_tid=f3375b4efb6a7df49c6cdf1ad2a856e2&acdnat=1339672723_cec44b38454988e124a22b2b94559b61.*

[132] McLaughlin recuerda que los menores y adolescentes son, por un lado, tremendamente vulnerables a la presión del ambiente y de su círculo de amigos y compañeros; y, por otro, poseen un elevado nivel de atracción hacia las actividades de riesgo. MCLAUGHLIN, J. H., «Crime and Punishment: Teen Sexting in Context», Express, 2010. En Internet, en *http://works.bepress.com/julia_mclaughlin/1*, pp. 136 y ss.

[133] En el mismo sentido, GOODMAN, E., «Is "sexting" same as porn?», en *Boston Globe*, 24 de abril de 2009, p. 1: «[i]f you look at the reasons why they share naked content, one is a form of flirting. Another is a way of brokering trust, a guy saying, "You don't trust me? You won't send me a naked picture?"». En Internet, en *http://www.boston.com/bostonglobe/editorial_opinion/oped/articles/2009/04/24/is_sexting_same_as_porn/*.

[134] COX COMMUNICATIONS: *Teen Online & Wireless Safety Survey. Cyberbullying, Sexting and Parental Controls,* Atlanta, GA, 2009.

[135] INTECO y PANTALLAS AMIGAS, «Guía sobre adolescencia y *sexting:* ¿qué es y cómo prevenirlo?», febrero de 2011. En Internet, en *http://www.inteco.es/Seguridad/Observatorio/guias/Guia_sexting*.

[136] AGUSTINA, J. R. (dir.) *et al., La pornografía: sus efectos sociales y criminógenos. Una aproximación multidisciplinar,* BdeF-Edisofer, 2011, pp. 1 y ss.

fenómeno, además de las ya apuntadas, se encuentran los materiales enviados a terceros de menores fotografiados o grabados manteniendo relaciones sexuales con sus parejas; exparejas desdeñadas que mandan fotografías de su pareja anterior a otros por venganza; o menores que, simplemente, siguen la cadena de transmisión de imágenes reenviándolas irreflexivamente a terceros [137]. Los coleccionistas de pornografía siempre están a la búsqueda de nuevas imágenes y una buena fuente de ellas son las publicaciones que hacen los jóvenes en Facebook o Myspace; de hecho, gran parte del material pornográfico infantil que se maneja en la Red tiene origen en este tipo de conductas [138].

Leary en un reciente artículo [139] hace una clasificación de los distintos comportamientos de *sexting*, diferenciando entre las siguientes modalidades conductuales: *a)* el menor que manda una imagen a alguien importante para él; *b)* el menor que hace y/o distribuye imágenes de sí mismo y otros participando en conductas sexuales explícitas; *c)* el menor que transmite o difunde una imagen desnuda de otro joven sin su conocimiento; *d)* el menor que publica dichas imágenes en un sitio web; *e)* el adolescente mayor que pide (o coacciona) a otro joven por tales imágenes; *f)* la persona que se hace pasar por un compañero de clase para engañar y chantajear a otros para que le envíen imágenes; *g)* los adultos que envían fotos o vídeos a menores de edad o poseen imágenes sexualmente explícitas de menores de edad, y *h)* adultos que envían mensajes de texto con imágenes sexualmente sugerentes a otros adultos.

En todo caso, el comportamiento más conocido de ataque relacionado con la indemnidad y la libertad sexual en el ciberespacio es el denominado *child grooming*, que consiste en contactar con menores por medio de las redes sociales o de otras formas de comunicación como salas de chat, canales de mensajería instantánea o similares, para acercarse a ellos e intentar posteriormente un contacto sexual. El *cybergrooming* u *online grooming* definido aquí como ciberacoso sexual [140], proviene de la unión entre el prefijo *cyber* y

---

[137] En algunos estudios se han ampliado los límites de la definición de *sexting* hasta tal punto que entrarían dentro de este fenómeno el intercambio de mensajes de contenido sexual explícitamente provocativos que no incorporen imágenes, siempre que se pueda deducir de ellos una clara intencionalidad provocativa de acuerdo con los usos sociales. AGUSTINA SANLLEHÍ, J. R., «¿Menores infractores...», *op. cit.,* p. 11:4.

[138] En este sentido, Humbach afirma en su artículo que: *«In fact, a significant portion of teen-produced material may even be intentionally so»,* HUMBACH, J. A., «"Sexting" and the First Amendment», *Hastings Constitutional Law Quarterly,* vol. 37, 2010, p. 445.

[139] LEARY, M. G., «Sexting or Self-Produced Child Pornography? The Dialogue Continues. Structured Prosecutorial Discretion within a Multidisciplinary Response», *Virginia Journal of Social Policy and the Law,* 2010, p. 492. En Internet, en *http://scs.student.virginia.edu/vjspl/17.2/Leary%20--%20Structured%20Discretion.pdf*.

[140] MARTÍN LORENZO, M., y RAGUÉS I VALLÈS, R., «Libertad e indemnidad sexuales», en ORTIZ DE URBINA GIMENO, Í. (dir.), *Memento experto reforma penal 2010. Ley Orgánica 5/2010,* Madrid, Francis Lefebvre, 2010, p. 104, también CUGAT MAURI, M., «Delitos contra la libertad e indem-

el término *grooming,* que comenzó a usarse en la literatura dedicada al estudio criminológico y psicológico de los delincuentes sexuales para describir los comportamientos del «depredador sexual» llevados a cabo durante la primera fase del abuso, en la que el abusador trata de ganarse la confianza del menor y de acceder a información esencial sobre él para la posterior consumación del abuso [141]. El *grooming,* propiamente dicho, abarcaría todas las conductas preparatorias llevadas a cabo por el abusador sexual hasta lograr el encuentro con la víctima potencial [142], y consistiría generalmente en un proceso de seducción [143] de algún menor que, por la general inexperiencia de los menores en las relaciones amorosas [144], y por la general incapacidad en la fase temprana de la adolescencia (12 a 14 años) para comprender la naturaleza sexual que tienen muchas de las conversaciones [145], son especialmente vulnerables a este tipo de ataques. Aun así, es el propio abusador que lleva a cabo el *grooming* el que aprovecha los puntos débiles de los niños y adolescentes para tratar de ganarse su confianza: bien simulando compartir *hobbies* [146], o más generalmente convirtiéndose en el «adulto que comprende» a la víctima potencial como, por el contrario, no parecen hacer los adultos cercanos a ella [147]. De hecho, la víctima del *grooming* es seleccionada por el abusador, quien busca a los menores más débiles, especialmente aquéllos con vulnerabilidades relacionadas con la incomprensión familiar o social, para centrar en ellos el ataque [148]. Y ésta es una de las características del

---

nidad sexuales», en ÁLVAREZ GARCÍA, F. J., y GONZÁLEZ CUSSAC, J. L., *Comentarios a la reforma penal de 2010,* Valencia, Tirant lo Blanch, 2010, p. 235. Aunque el *grooming* no es propiamente un acoso sexual tal y como técnicamente se concibe por el ordenamiento jurídico español, creo que el término podría ser válido siempre que se le añada «a menores», pues en caso contrario el término no se correspondería con lo que pretende describir.

[141] SALTER, A. C., *Predators: Pedophiles, Rapists, and Other Sex Offenders: Who They Are, How They Operate, and How We Can Protect Our Children*, New York, Basic Books, 2003, pp. 46 y ss.

[142] MCALINDEN, A. M., «Setting "Em Up": Personal, Familial and Institutional Grooming in the sexual Abuse of Children», en *SLS,* vol. 15, núm. 3, 2006, p. 339.

[143] BERSON, I. R., «Grooming Cybervictims: The Psychosocial Effects of Online Exploitation for Youth», en *JSC*, vol. 2, núm. 1, 2003, p. 11.

[144] WOLAK, J.; FINKELHOR, D.; MITCHELL, K. J., e YBARRA, M. L., «Online "predators" and their victims: myths, realities and implications for prevention and treatment» (2008), en *APs,* vol. 63, en Internet en *http://psycnet.apa.org/journals/amp/63/2/111/* (última visita el 21 de diciembre de 2010), p. 114.

[145] *Ibid.,* p. 115. En todo caso, señalan los autores a partir de la revisión de los estudios psicológicos sobre la sexualidad en la etapa adolescente, que no se puede atribuir el riesgo de ser objeto de ataques de *grooming* a la supuesta «inocencia sexual», sino a una suma de factores asociados a la sexualidad en la adolescencia, como el crecimiento de la curiosidad sexual y la necesidad de conocimiento y de experiencias del joven durante la transición de la infancia a la etapa adulta.

[146] YOUNG, K. S., «Profiling online sex offenders, cyber-predators, and pedophiles», en *JBP,* vol. 5, núm. 1, 2005, p. 9.

[147] LANNING, K. V., «Law enforcement perspective on the compliant child victim», en *APSACA,* vol. 14, núm. 2, 2002, p. 5.

[148] Véase en este sentido, la revisión criminológica llevada a cabo por MCALINDEN, A. M., «Setting "Em Up"...», *op. cit.,* pp. 349 y 350, donde señala, a partir de la revisión de los estudios empíricos existentes, los rasgos principales de victimización frente al abuso sexual de un extraño,

grooming que hacen que el mismo entrañe una gran peligrosidad, en sentido cuantitativo, cuando se realiza a través de Internet.

Lo cierto es que el *grooming,* tal y como lo hemos definido, existe mucho antes de que apareciera la Red de redes, y tampoco fue esta conducta la primera o por lo menos la primeramente conocida forma de pedofilia (y en general realización de ataques sexuales contra menores) en Internet, que mucho antes de la constatación del problema de la seducción de menores con fines de encuentro sexual, ya se había convertido en el paraíso de la pornografía infantil. Sin embargo, ya a finales del siglo pasado se comenzó a percibir que algunos pedófilos accedían a los chats en Internet para «molestar» a los menores y hacerles proposiciones [149], asemejándose dichas prácticas al *grooming* tradicionalmente entendido. Bien por medio del envío de mensajes, por *e-mail* o, más comúnmente, a través de las salas de chat, algunos adultos intimaban con menores y conversaban con ellos tratando, y en algunos casos logrando, contactar personalmente con ellos. Y este tipo de conductas de los también denominados depredadores sexuales se ha incrementado significativamente debido al general incremento y popularización del uso de Internet [150].

El ciberacoso sexual a menores, o *cybergrooming,* se puede llevar a cabo usando cualquiera de las TIC que permiten el contacto con menores. Sin embargo, hay importantes estudios criminológicos que analizan qué prácticas en Internet son las que más pueden incidir en el hecho de ser víctima de un ataque de ese tipo y que nos informan, por tanto, sobre las formas en las que suele aparecer el *online grooming.* Pues bien, toda la literatura americana que ha tratado el tema, coincide en que el *grooming* está particularmente presente en las *chat rooms* o salas de chat. También lo certifican los estudios empíricos victimológicos que demuestran que sobre un tercio de los jóvenes que reciben solicitaciones explícitas vía *online,* las han recibido en salas de chat [151]. Al fin y al cabo, en el chat, frente a otras formas de comunicación como los correos electrónicos o los foros, hay una comunicación instantánea entre sujetos, siendo habituales las charlas sobre sexo explícito y el envío de solicitudes de relaciones sexuales explícitas [152]. También hay otras formas de realización del *online grooming*, que, como se vio en el estudio criminológico

---

como pueden ser el tratarse de niños con necesidades especiales y problemas de aprendizaje, menores en entornos familiares muy conflictivos donde hay un traumático proceso de separación, donde la madre está enferma o tiene problemas con las drogas, o también menores solos sin un entorno familiar protector, etcétera.

[149] Durkin, K. F., «Misuse of the Internet by Pedophiles: Implications for Law Enforcement and Probation Practice», en *FP,* vol. 61, 1997, pp. 14 y ss.

[150] Wolak, J.; Finkelhor, D.; Mitchell, K. J., e Ybarra, M. L., «Online "predators"...», *op. cit.,* p. 112.

[151] *Ibid.,* p. 113.

[152] Mitchell, K. J.; Finkelhor, D., y Wolak, J., «Youth Internet users at risk for the most serious online sexual solicitations», en *AJPM*, vol. 32, núm. 6, 2007, pp. 532-537.

general, parten del envío por la víctima de información personal a personas desconocidas. Por el contrario, no parece que el uso de redes sociales conlleve, por sí mismo, un mayor riesgo de ser víctima del *grooming* [153], lo cual tiene gran importancia si tenemos en cuenta el estudio de Lenhart y Madden, que certifica que a finales de 2006, cuando todavía no se había producido la explosión de Facebook, el 55 por 100 de los usuarios de Internet jóvenes de 12 a 17 años empleaban ese tipo de redes tipo Myspace [154]. Las encuestas a usuarios jóvenes muestran, según sus propias experiencias, que es por la vía de los mensajes directos o por medio del chat, más que a través de las redes sociales, por donde reciben solicitudes de naturaleza sexual en Internet [155].

Pero Internet no sólo ha cambiado la forma de hacer *grooming*, sino que, y como se verá posteriormente, ha modificado el perfil del sujeto que lo hace [156] y de la víctima que lo padece [157], y ha incrementado el número potencial de agresores y víctimas, todo lo cual ha supuesto, asimismo, el incremento del temor social ante una conducta que era tan peligrosa, o quizás más, que la actualmente realizada por Internet, pero que ahora es más visible a los ojos de «la sociedad insegura». Esto es absolutamente lógico si tenemos en cuenta, además del actual empuje de los medios de comunicación social y su papel transmisor de sensación de inseguridad, que la conducta de molestar a menores proponiéndoles relaciones sexuales ha aumentado cuantitativamente al ser realizada en Internet. Sin embargo, no parece que cualitativamente dichas conductas sean más peligrosas, ni siquiera iguales, a las del *grooming* tradicional en las que la propuesta se realizaba por parte de un pedófilo sobre un menor de doce años y existiendo un contacto directo y no virtual, entre ellos. Y la cuestión no es baladí, dado que el CP español ha procedido a tipificar en el artículo 183 bis únicamente el *grooming* realizado a través de las TIC, y no el auténtico y más peligroso para los preadolescentes. Como se ha visto, gran parte de las proposiciones sexuales a través de Internet no buscan mantener un contacto con un menor de trece años para posteriormente abusar de él, sino que más bien buscan adolescentes de entre quince a diecisiete años con experiencias sexuales anteriores que estén dispuestos a mantener una relación con un adulto, mientras que el pedófilo sobre todo usa esos medios para obtener información sobre las potenciales víctimas y acercarse luego a ellas.

---

[153] Wolak, J.; Finkelhor, D.; Mitchell, K. J., e Ybarra, M. L., «Online "predators"...», *op. cit.,* p. 114.

[154] Lenhart, A., y Madden, M., *Teens, privacy and online social networks: How teens manage their online identities and personal information in the age of MySpace* (2007), en Internet en *http://pewresearch.org/pubs/454/teens-privacy--online-social-networks* (última visita el 10 de septiembre de 2010).

[155] Wolak, J.; Finkelhor, D.; Mitchell, K. J., e Ybarra, M. L., «Online "predators"...», *op. cit.*, p. 115.

[156] Cap. IV.2.3.

[157] Cap. V.3.2.2.

2.3. Ciberataques de contenido

El último grupo de tipologías de cibercriminalidad es, en realidad, una forma concreta de los que hemos denominado ciberataques réplica, pero con una singularidad tal y con problemáticas jurídicas tan especiales que merece ser tratada por separado. Se trataría de la categoría de ciberataques de contenido, y aglutinaría a todas aquellas en las que el centro de la infracción lo constituye el contenido que se comunica o se transmite a través de las redes telemáticas, particularmente de la Red de redes, Internet [158]. La facilidad con la que hoy se puede digitalizar cualquier tipo de información y con la que se puede comunicar la misma a múltiples receptores simultáneamente y situados en lugares diversos de todo el mundo, convierte a la Red en un medio abierto en el que los contenidos ilícitos, al igual que los lícitos, también pueden «campar a sus anchas». Hay que tener en cuenta además que, frente al resto de medios de comunicación, Internet funciona simultáneamente como un medio de edición y de comunicación [159], en el sentido de que, como bien advirtió Morón Lerma, la dicotomía entre emisor y receptor se difumina en el ciberespacio [160], donde un usuario puede pasar de ser receptor a ser comunicador y productor de contenidos [161]. Si a ello se suma la ya comentada popularización de Internet y la facilidad para el acceso y el envío de información a través del mismo, y la progresiva utilización por los menores de este sistema de comunicación, se puede entender entonces que desde hace ya más de una década surgiera una preocupación por los contenidos [162], ante la aparición de todo un conjunto de conductas a las que

---

[158] La doctrina admite generalmente la existencia de esta categoría de cibercriminalidad, si bien distingue aquellas conductas en las que lo que se transmite son contenidos ilícitos, de aquellas otras en las que el objeto de la difusión son contenidos nocivos. LÓPEZ ORTEGA, J. J., «Libertad de expresión y responsabilidad por los contenidos en Internet», en *CDJ,* núm. 10, 2001, p. 96. Los primeros son aquellos cuya tenencia o difusión supone, en todo caso, una ilicitud, como ocurre con la pornografía infantil; los segundos, en cambio, serían aquellos a los que no se vincula sanción penal alguna, pero que pueden resultar ofensivos o perjudiciales para un receptor inadecuado (material pornográfico en general, que puede resultar delictivo si se transmite a menores de edad). Junto a ellos, podríamos incluir un tercer grupo en el que el contenido no es lícito o ilícito dependiendo de sí mismo o de a quién se transmite, sino de si su transmisión se realiza con o sin autorización del titular. Éste sería el caso de los objetos de derecho de propiedad intelectual e industrial, cuya difusión o puesta a disposición de terceros puede resultar ilícita cuando no tenga la autorización del titular de los derechos. En el mismo sentido véase MORÓN LERMA, E., «Derecho penal y nuevas...», *op. cit.,* pp. 99 y 100, y MORALES PRATS, F., «Los ilícitos en la Red (II): Pornografía infantil y ciberterrorismo», en ROMEO CASABONA, C. M. (coord.), *El cibercrimen..., op. cit.,* pp. 271 y ss.

[159] LÓPEZ ORTEGA, J. J., «Libertad de expresión...», *op. cit.,* pp. 117 y ss.

[160] MORÓN LERMA, E., *Internet y Derecho penal: Hacking y otras conductas ilícitas en la Red,* Cizur Menor, Aranzadi, 2002 (2.ª ed.), p. 117.

[161] Paradigmático es el ejemplo de las redes P2P de intercambio de archivos, donde a menos que se opte expresamente por no compartir un contenido, en el mismo momento en que se descarga un archivo, ya se está poniendo el mismo a disposición de cualquiera que entre en la Red.

[162] LÓPEZ ORTEGA, J. J., «Libertad de expresión...», *op. cit.,* p. 91.

les une que la ilegalidad deviene, no del medio utilizado, sino del contenido distribuido por Internet, y a las que, pese a afectar a bienes jurídicos muy diferentes entre sí, les une todo un conjunto de problemáticas penales relacionadas con la distribución de contenidos: especialmente la atribución de la responsabilidad en cascada o a varios sujetos distintos (entre ellos los prestadores de servicios) [163], o la tensión entre la eficacia en la persecución de estos contenidos con los derechos fundamentales, en general, y la libertad de expresión en particular [164]; equilibrio que, como señaló Morón Lerma, si ya es difícil lograr en la realidad analógica, resulta aún más complejo en el ciberespacio en el que siempre subyace una pugna «recrudecida tras lo ocurrido el 11-S, entre libertad y control" [165].

Dentro de este tipo de infracciones que son llevadas a cabo por sitios webs (páginas y blogs) más que por particulares, habrá que diferenciar además, aquéllas en las que se distribuye directamente el contenido ilegal, de las otras, mayoritarias, en las que lo que se hace es poner a disposición de terceros el mismo, e incluso de otras en las que simplemente se sistematizan los contenidos y se facilitan enlaces para su acceso en otros terminales y sistemas informáticos. Por último, dentro de esta tipología de comportamientos, en los que la ilicitud se relaciona directamente con el contenido, habría que incluir aquellas conductas, directamente relacionadas con las acabadas de mencionar, en las que no se difunde o distribuye el mismo, sino que tan sólo se posee. Generalmente la ilicitud de muchas de las conductas ilícitas relacionadas con el uso de las TIC deviene de la transmisión del contenido, pero dada la dificultad de la prueba de tal actividad no es inusual el adelantamiento de la punición a comportamientos en los que no hay comunicación del contenido pero sí posesión. Esto ocurre, como se verá, con la pornografía infantil, cuya tenencia dará lugar directamente a infracción penal en el artículo 189.2 CP. Lo que igualmente sucede con la tenencia de determinados dispositivos y programas informáticos destinados a la supresión de barreras de protección relacionadas con la piratería intelectual o con el fraude informático en el artículo 248 CP.

Junto a todas estas infracciones en las que se comunica o distribuye contenido ilegal, hay que añadir como ataque caracterizado por que el centro de la infracción lo constituye el contenido que se transmite a través de redes telemáticas, la piratería intelectual en Internet. En este caso, el contenido no es en sí ilegal, pero sí puede serlo su transmisión sin autorización de los titulares de derechos de explotación exclusiva que se ven afectados por la misma.

---

[163] Véase *infra* cap. II.

[164] López Ortega plantea el conflicto entre la eficacia y la tutela de la intimidad, LÓPEZ ORTEGA, J. J., «Libertad de expresión...», *op. cit.,* pp. 91 y ss., puesto que es evidente que el mismo puede resultar en ocasiones un obstáculo para la identificación de los responsables de las infracciones.

[165] MORÓN LERMA, E., «Derecho penal y nuevas tecnologías...», *op. cit.,* p. 99.

Por último también deben diferenciarse estas tipologías de ciberataques de otras en las que la ilicitud no deviene del propio contenido, sino de las características del propio receptor del mismo. Así, la pornografía no es ilícita en el ciberespacio, pero sí puede ser parte de un ciberataque sexual a un menor.

Con todo esto podríamos decir que hay tres clases de cibercrímenes de contenido en el ciberespacio tal y como se ve en la siguiente tabla, si bien sólo las dos primeras plantean las características criminológicas similares y las problemáticas jurídicas derivadas de ellas que hemos comentado.

Tabla 2.3. Clases de cibercrímenes de contenido en el ciberespacio. Elaboración propia.

Cibercrímenes por la ilicitud del contenido	*Cibercrímenes por la no autorización en la explotación del contenido*	*Cibercrímenes por la víctima que recibe el contenido*
Pornografía infantil	Piratería intelectual	Pornografía a menores
Ciberterrorismo (incitación a la delincuencia terrorista)	Piratería industrial (marcas, diseños)	
Cyberhate speech o incitación al odio racial en el ciberespacio	Descubrimiento de secretos de empresa en Internet	

2.3.1. *La ciberpiratería intelectual*

Ya nadie niega la incidencia que ha tenido Internet en los derechos de propiedad intelectual y, por ello, en el mercado de obras del ingenio, que se nutría de la explotación de los mismos. Aquello que se dijo respecto a los derechos de propiedad intelectual a raíz de la aparición del ciberespacio de que «todo lo que conocíamos es ahora falso, vamos a tener que aprenderlo de nuevo» [166], podría valer también para una industria que se ha visto significativamente afectada por las nuevas formas de explotación no autorizada de los derechos de autor sobre obras videográficas, cinematográficas, musicales o *software*. Aunque las estadísticas existentes han sido generalmente realizadas por la propia industria afectada y existan estudios que ponen en duda la neutralidad de las mismas, es indudable que la popularización del ciberespacio ha conllevado significativas pérdidas de ingresos de la industria de las obras del ingenio.

La principal razón de tal disminución de ingresos por parte de la industria se sitúa generalmente en la que, se ha denominado, no siempre con la

[166] BARLOW, J. P., «A Not Terribly Brief History...», *op. cit.*

precisión necesaria, piratería digital o ciberpiratería digital. Así, y conforme a los datos ofrecidos por el Observatorio de Piratería, el valor total de los contenidos digitales pirateados en España ascendió en el primer semestre de 2011 a 5.229,4 millones de euros, casi cuatro veces el valor del consumo legal, sobre una industria que generó un volumen de negocio de 1.538,1 millones en ese mismo período. Conforme a ese estudio, la tasa media de piratería es del 77,3 por 100 para el conjunto de los mercados analizados, si bien el de la música con un 98,2 por 100, y el de las películas con el 73,9 por 100, son los que mayores porcentajes alcanzan, seguidos de los videojuegos, con un 61,7 por 100, y de los libros, con un 49,3 por 100 [167]. Es obvio que el cálculo que se realiza parte de dar valor, a partir de la consideración hipotética de que fuera contenido legal y según su precio de mercado, a una mercancía que no la tiene, por lo que no resulta posible asimilar a pérdidas el valor de los contenidos digitales. Pero también existen datos sobre la pérdida de ingresos de la industria, sobre la venta de música grabada y la venta de música digital que demuestran la clara relación entre la popularización de la piratería intelectual y el descenso de las ventas de música. Así, según el informe IFPI (International Federation Phonografic Industry) [168] de 2012, en 2011 las ventas de música grabada a nivel mundial cayeron un 3 por 100 en 2011 y un 37 por 100 acumulado desde 1999, año en que la industria discográfica marcará su récord histórico con un valor de facturación mundial de 38.600 millones de dólares [169]. Concretamente, las ventas de música en España se redujeron alrededor del 55 por 100 entre 2005 y 2010 —una tasa de disminución muy por encima de la media mundial—, pues ya sólo en 2010 el mercado se redujo en un 22 por 100 [170]. Otras fuentes, como Promusicae [171], también ponen de relieve la especial disminución de las ventas en España, explicando que durante el año 2009 los españoles gastaron 211 millones de euros en música, lo que supone un 17 por 100 menos que el año 2008 y debido a esta gran caída, el crecimiento en el mercado digital no ha

---

[167] Según este mismo estudio, por tipo de contenidos los resultados son los siguientes: el valor de lo pirateado en la industria de la música alcanzó en el primer semestre de 2011, un total de 2.746,4 M €. El valor de lo pirateado para la industria de las películas alcanzó en el primer semestre de 2011 un total de 1.401,6 M €. El valor de lo pirateado para la industria del videojuego alcanzó en el primer semestre de 2011 un total de 288,2 M €. El valor de lo pirateado para la industria del libro fue en el primer semestre de 2011 de un total de 793,1 M €. Por tanto, del total del valor de los contenidos pirateados, 5.229,4 M €, en el primer semestre de 2011. ACHAERANDIO, R., y MALDONADO, F., «Observatorio de piratería y hábitos de consumo de contenidos digitales», 2011, p. 2. Véase al respecto de los hábitos de consumo, PEUKERT, A., «Why Do "Good People" Disregard Copyright on the Internet?», en *Social Science Research Network,* 17 de agosto de 2010, pp. 2 y ss.

[168] IFPI representa a la industria discográfica mundial, con 1.400 compañías como miembros en 72 países y asociaciones afiliadas en 44 países.

[169] Informe de la Música Digital de IFPI 2012.

[170] IFPI Digital Music Report 2011, p. 15.

[171] Promusicae agrupa a 86 miembros, tanto filiales de empresas discográficas multinacionales como empresas independientes que, en su conjunto, representan a más del 95 por 100 de la actividad nacional del sector de la música grabada.

podido paliar el declive general del sector [172]. Y es que las tendencias de piratería varían considerablemente según el país, pues el Informe IFPI de 2011 confirma que Brasil y España están entre los mercados con el mayor número de usuarios que acceden a los servicios sin licencia, con el 45 y el 44 por 100 respectivamente [173], una proporción muy por encima de la europea —donde el promedio es del 23 por 100 [174]—.

Ahora bien, ¿qué es la ciberpiratería [175] digital? Paralelamente al crecimiento del valor de los bienes intelectuales en la nueva sociedad de la información, bien por la potencialidad de la *www* como medio de difusión o bien por materializarse en diferentes formas de *software* con el valor que el mismo tiene en la actualidad, hasta convertirse en los bienes más importantes económicamente del mundo en el que vivimos; han surgido formas de explotación ilícita de obras protegidas. Desde la venta directa de obras digitalizadas, pasando por la comunicación pública de las obras vía *streaming* a cambio de una cantidad de dinero, entre otras muchas, Internet ha dado lugar a variadas conductas caracterizadas por la infracción de derechos de propiedad intelectual y que englobarían lo que se viene denominando ciberpiratería.

La mayor parte de ellas, sin embargo, han acabado desapareciendo debido al impacto del comportamiento que, sin lugar a dudas, más daño ha hecho a la industria del entretenimiento, pero sobre el que más podría discutirse su consideración como piratería digital [176]: el intercambio gratuito de archivos.

En efecto, si hay un comportamiento que ha puesto en jaque los intereses de los titulares de derechos de explotación exclusiva de propiedad intelectual en el ciberespacio ése es el del intercambio de archivos. El uso compartido de archivos se inició con el protocolo IRC (*Internet Relay Chat*) a mediados de la década de los noventa, alcanzando en el cambio de milenio su apogeo con Napster, primero, y luego con un nuevo sistema de intercambio de archivos con un protocolo P2P (*peer-to-peer*) [177]. Este sistema

---

[172] GIMENO, M. (dir.), «eEspaña, Informe anual...», *op. cit.,* p. 224.

[173] IFPI Digital Music Report 2011, p. 14.

[174] *Ibid.,* p. 15.

[175] Algunos autores, como Filby, se refieren a este concepto de la siguiente forma: *«The literal term of piracy is defined as "the unauthorized use or reproduction of another's work", while cyber is attributed as "relating to or characteristic of the culture of computers, information technology, and virtual reality". Thus cyber piracy in the context of the entertainment industries can encompass any person who utilises IP in a digital form without the authorization of the rights holder».* FILBY, M., «File-Sharers: Criminals, Civil Wrongdoers or the Saviours of the Entertainment Industry? A Research Study into Behaviour, Motivational Rationale Legal Perception Relating to Cyber Piracy Hertfordshire», en *Law Journal*, 5 (1), 2-77, p. 57.

[176] Sí lo hace así, incluyendo entre las conductas de piratería no sólo la descarga directa sino también el intercambio de archivos en sistemas P2P, el citado informe de ACHAERANDIO, R., y MALDONADO, F., «Observatorio de piratería...», *op. cit.,* 2011, p. 2.

[177] PEUKERT, A., «Why Do "Good People" Disregard Copyright...», *op. cit.*, p. 2. Sobre la evolución del sistema Napster al P2P, véase MIRÓ LLINARES, F., *Internet y delitos contra la propiedad intelectual*, Madrid, Iberautor Promociones Culturales, 2005.

permaneció en auge, con programas como eMule o Ares que compartió con los sistemas de *streaming* [178], hasta que se ha puesto en boga el sistema de descarga directa, surgiendo sitios de hospedaje como Megaupload, RapidShare o MediaFire, que si bien servían en apariencia para guardar archivos y codificarlos, se relacionaban con múltiples blogs y páginas que enlazaban los nombres de los contenidos protegidos con los de los códigos de descarga en webs de este tipo. Y si bien el cierre de Megaupload por parte del FBI pudo suponer un aparente golpe al sistema de descargas en Internet, su sustitución inmediata por otras webs y otros sistemas de intercambio gratuito de archivos conlleva que, de momento, no sea la opción más cómoda para el consumidor de bienes culturales en el ciberespacio el pagar por ello. De hecho, además de la proliferación de sitios de descarga gratuita de archivos y de nuevas formas de explotación, en ocasiones lícitas, pero contrarias a la configuración tradicional de la propiedad intelectual, se une el hecho de que en los motores de búsqueda como Google, Yahoo! y Bing, muchos de los principales resultados que brindan sus páginas proporcionan enlaces a contenidos no autorizados o a sitios que infringen los derechos de autor. Estas empresas, sin embargo, tratan de responder inmediatamente a las demandas y solicitudes de los titulares de los derechos.

Aunque millones de personas son conscientes de que pueden estar infringiendo los derechos de autor, continúan cargando y descargando datos ilegalmente [179]. Este problema global se está tratando de afrontar de muy distintas formas, que van desde la atribución de responsabilidad civil en Estados Unidos directamente a los que realizan descargas gratuitas, pasando por la imposición de penas privativas de libertad en Alemania a los usuarios que copien archivos para uso privado en sistemas P2P, hasta el cierre de los sitios web dedicados a intercambiar archivos o a sistematizar enlaces para ello por medio de un procedimiento administrativo, solución prevista en Francia y que ha sido parcialmente copiado en España por la llamada Ley Sinde. Y todo ello mientras se mantiene el mismo sistema penal que en ningún caso permite sancionar el intercambio gratuito entre usuarios de archivos protegidos [180]. Pese a no ser éste el lugar para realizar un análisis jurídico, me resisto a obviar el absurdo que supone que junto a comportamientos que sí tienen una lesividad potencialmente muy importante como el plagio, conductas como la distribución física de copias (el conocido top manta), cuya incidencia en la actualidad es casi ridícula para los intereses patrimoniales

---

[178] También con modelos de distribución *online* exitosos, como Spotify, que cuenta con casi ocho millones de usuarios en los países que opera. La distribución de los contenidos musicales se basa en el *streaming* y tiene un modelo mixto de financiación, una versión gratuita a cambio de la escucha de publicidad cada dos o tres canciones, y el pago por suscripción mensual que da opción a trasladar la música al teléfono móvil. GIMENO, M. (dir.), «eEspaña, Informe anual sobre el desarrollo de la sociedad de la información en España, Fundación Orange», *op. cit.,* p. 220.

[179] PEUKERT, A., «Why Do "Good People" Disregard Copyright...», *op. cit.,* p. 6.

[180] MIRÓ LLINARES, F., *Internet y delitos..., op. cit.*

de los titulares de los derechos, pueden ser sancionadas penalmente pese a que el perjuicio patrimonial de muchas de ellas, analizado individualmente, no llegue a los cuatrocientos euros. Mientras, el intercambio gratuito de archivos llevado a cabo en webs que obtienen gracias a las visitas, pingües beneficios económicos similares a los perjuicios que obtienen los productores por la disminución de las ventas en un mercado de distribución de ejemplares físicos que está literalmente agonizando, es impune para los usuarios y difícilmente punible para las páginas web que, además, van adaptando sus formas de comunicación para huir de la persecución penal de estos comportamientos.

2.3.2. *Pornografía infantil en Internet*

Pese a tratarse de un concepto que socialmente parece no tener discusión, no es sencilla la definición de la pornografía infantil tal y como demuestran las variantes ofrecidas por la Decisión Marco 2004/68/JAI del Consejo, de 22 de diciembre de 2003 [181], o el Protocolo Facultativo de la Convención sobre los Derechos del Niño, relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, hecho en Nueva York el 25 de mayo de 2000 (RCL 2002, 300) y ratificado por España (*BOE,* 31 de enero de 2002) [182]. La compleja construcción de un concepto unánime de este fenómeno viene dada, según ha puesto de manifiesto Morales Prats [183] entre otros [184], por la multiplicidad de factores que en él influyen, tanto de tipo cultural como moral, pero sobre todo por lo «confuso y altamente inadecuado» [185] del propio término como ha señalado buena parte de la doctrina [186]. Y es que en realidad, como subraya Agustina, no debemos

---

[181] Según la cual (art. 1), se entiende por pornografía infantil cualquier material pornográfico que describa o represente de manera visual: «*a)* un niño real practicando o participando en una conducta sexualmente explícita, incluida la exhibición lasciva de los genitales o de la zona púbica de un niño; *b)* a una persona real que parezca ser un niño practicando o participando en la conducta mencionada en el inciso *a)*, o *c)* imágenes realistas de un niño inexistente practicando o participando en la conducta mencionada en el inciso *a)*».

[182] Que define como pornografía infantil «toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales».

[183] Quien apunta que estas fluctuaciones conceptuales tienen un reflejo en los conceptos legales utilizados por los ordenamientos de cada país. MORALES PRATS, F., «Pornografía Infantil e Internet: La respuesta en el Código Penal español», en CASALLO LÓPEZ, M. (dir.), *Problemática jurídica en torno a fenómenos de Internet*, Madrid, Escuela Judicial Consejo General del Poder Judicial, 2000, pp. 178 y ss.

[184] También en este sentido, SANZ MULAS, N., «Pornografía en Internet», en *Revista Penal,* núm. 23, 2009, p. 185.

[185] AGUSTINA SANLLEHÍ, J. R., «¿Menores infractores...», *op. cit.,* p. 11:33.

[186] En este sentido, TAYLOR, M., y QUAYLE, E., *Child Pornography. An Internet Crime,* New York, Routledge, 2003; LEARY, M. G., «Self-Produced Child Pornography: The Appropriate Societal Response to Juvenile Self-Sexual Exploitation», *Virginia Journal of Social Policy and the Law,*

referirnos únicamente al describir este fenómeno al material pornográfico con temáticas de niños (o menores), que es a lo que parece reducirse en ocasiones esta expresión, sino que es un fenómeno más complejo que en todo caso debería describirse haciendo referencia a las «imágenes explotadas con fines sexuales en las que las víctimas son niños» [187]. Por todo ello, parece insuficiente la definición que del fenómeno se dio en el World Congress Against Commercial Sexual Expoitation of Children (WCACSEC), al referirse a la pornografía infantil como la reproducción sexualmente explícita de la imagen de un niño o niña [188]. Parece en todo caso más acertado el concepto que proporciona el Grupo de Interpol especializado en crímenes contra los niños, al definir la pornografía infantil como «toda forma de representación o promoción de la explotación sexual de los niños, incluidos los materiales escritos y de audio, que se concentren en la conducta sexual o los órganos genitales de los niños» [189], descripción [190] esta última que se aproximará mejor a los distintos tipos de comportamientos que pueden incluirse dentro del macroconcepto de pornografía infantil a los que nos referiremos más adelante.

El fenómeno de la pornografía infantil, a pesar de no ser propiamente informático, está cada vez más vinculado al uso de las nuevas tecnologías de la información, hasta tal punto que, en la actualidad, desde una perspectiva criminológica puede decirse que la mayoría de estos comportamientos se perpetran básicamente a través de Internet [191]. Así lo pone de manifiesto la Consulta núm. 3/2006, de 29 de noviembre, de la Fiscalía General del Estado, que en un apartado especialmente reservado al análisis de los as-

---

vol. 15, 2008, núm. 1. OST, S., *Child Pornography and Sexual Grooming. Legal and Societal Responses,* Cambridge, Cambridge University Press, 2009.

[187] AGUSTINA SANLLEHÍ, J. R., «¿Menores infractores...», *op. cit.,* p. 11:33.

[188] En Internet, en *http://www.csecworldcongress.org/sp/yokohama/Background/index.htm* (última visita el 11 de junio de 2012).

[189] En concreto, explica que «la pornografía infantil se crea como consecuencia de la explotación o abuso sexual sobre un niño, pudiendo definirse como cualquier forma de representación de la explotación sexual de menores, incluyendo material escrito o sonoro referido al comportamiento sexual de los niños o a sus genitales», Interpol Specialist Group on Crimes Against Children: *http://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children* (última visita el 11 de junio de 2012).

[190] Ya no sólo es polémico el concepto de pornografía infantil en sí mismo, sino también la determinación de cuál debe ser la *edad* para acotar el concepto de niño o de menor. Por no detenernos demasiado en esta cuestión, simplemente señalaremos que la Convención sobre Delincuencia en la Red de 23 de noviembre de 2001, que se celebró en el seno del Consejo de Europa y tenía como objetivo armonizar las legislaciones europeas, consideró menor a todo aquél que tuviera menos de 18 años, si bien permitió que las legislaciones nacionales redujeran esta edad hasta los 16 años, si lo consideraban conveniente, límite que algunos países han utilizado y otros no. MORILLAS FERNÁNDEZ, D. L., *Análisis dogmático y criminológico de los delitos de pornografía infantil, Especial consideración de las modalidades comisivas relacionadas con Internet*, Colección Monografías de Derecho Penal, Madrid, Dykinson, 2005, p. 73.

[191] DE LA ROSA CORTINA, J. M., *Los delitos de pornografía infantil. Aspectos penales, procesales y criminológicos,* Valencia, Tirant lo Blanch, 2011, pp. 25 y ss.

pectos criminológicos de este fenómeno, destaca que la eclosión de Internet ha revolucionado por completo el mercado de la pornografía infantil hasta prácticamente monopolizarlo como consecuencia de las ventajas que proporciona a los usuarios: «desde la facilidad para descargarse archivos, los menores costes económicos, la aptitud para entablar relación con un enorme número de internautas con la consiguiente facilitación de los intercambios, y las grandes posibilidades de permanecer en el anonimato». Y añade esta Consulta que si «a ello unimos la accesibilidad técnica y económica a equipos de audio/vídeo que posibilitan la captación y grabación de imágenes y eventualmente de material pornográfico, con una facilidad impensable hace escasos años, puede comprenderse el fuerte incremento en la distribución de este material no tanto con ánimo de lucro cuanto como vía de intercambio de materiales entre pedófilos, sin propósito comercial y con la única finalidad de satisfacer sus inclinaciones sexuales, con la consiguiente creación espontánea de auténticas redes de intercambio de material».

La pornografía infantil se ha convertido de este modo en un problema con claras dimensiones internacionales, pues la irrupción de las nuevas tecnologías ha transformado completamente las pautas de su producción y difusión [192], suponiendo Internet, ahora más que nunca, el acceso a un mercado global de forma inmediata. Por ello, el impacto de Internet en este fenómeno, desde una perspectiva meramente cuantitativa supuso un incremento notable, como evidencia el estudio de Carr [193]. Y es que las especiales características de la Red, la convierten en el medio idóneo para realizar este tipo de conductas, pues ofrece innumerables ventajas [194] .

---

[192] Morales Prats, F., «El Derecho penal ante la pornografía infantil en Internet», en Morales Prats, F., y Morales García (coords.), *Contenidos ilícitos y Responsabilidad de los Prestadores de Servicios de Internet,* en *Revista Aranzadi de Derecho y Proceso Penal,* núm. 8, Navarra, Aranzadi, 2002, p. 95.

[193] Las cifras que aporta Carr en su estudio demuestran el impacto que supuso la Red para la pornografía infantil: «en 1995, posiblemente el último año antes de que Internet despegara definitivamente en el Reino Unido, la Unidad de Policía de Manchester se apoderó de un total de 12 imágenes abusivas de niños en papel o vídeo; en 1999 el mismo equipo incautó un total de 41.000, la mayoría de las cuales habían sido obtenidas de ordenadores que, a su vez, las habían captado de Internet. [...] En diciembre de 2003, un hombre británico fue declarado culpable de tener 450.000 imágenes en su poder, superando fácilmente el récord, establecido a principios de año, de 250.000 imágenes. [...] En Nueva York, en una sola incursión, la policía se incautó de un total estimado cercano al millón de imágenes. Todos estos números están muy lejos de las doce fotografías en Manchester en 1995», Carr, J., «Child abuse, child pornography and the Internet», disponible en Internet, en *http://www.make-it-safe.net/esp/pdf/Child_pornography_internet_Carr2004.pdf* (última visita el 12 de junio de 2012), pp. 1 y ss.

[194] Como las que ampliamente enumera Rojo García: «La Red se extiende de manera que cubre todo el mundo, con lo que el seguimiento de conductas ilícitas o sospechosas de ilicitud se dificulta. Por otra parte, se hace también mucho más difícil la propia detección de dichas conductas, bien porque el apogeo experimentado por Internet durante la década de los noventa ha hecho aumentar de manera ostensible la cantidad de páginas web existentes sobre cualquier tema, conse-

Hemos sido testigos de cómo la utilización de Internet en la difusión de pornografía infantil ha pasado por varias fases a lo largo de los años, y son precisamente estas fases las que al mismo tiempo han ido conformando algunos de los distintos tipos de comportamientos a los que vamos a referirnos con la definición anteriormente esgrimida de pornografía infantil. Comenzando por el primer tipo de comportamiento, en una primera fase se empleaban páginas web alojadas en servidores de Internet, en las que el traficante comerciaba con el material pornográfico infantil que ponía a disposición de los usuarios que previamente accedían a pagar una contraprestación, que se satisfacía por medio de un cargo en la tarjeta de crédito del adquirente cuyo número previamente tenía que proporcionar éste. Así, en esta primera fase de distribución de pornografía infantil a través de páginas web, podemos diferenciar dos modalidades conductuales. Por un lado, la del usuario de Internet que decide navegar con el objeto de acceder a una página web concreta cuyo contenido sabe con certeza que contiene material pornográfico infantil, y por otro lado, la de aquél que crea la página web misma, pues como apunta Morillas Fernández [195], «la inserción de una página de contenido pornográfico infantil es algo que puede realizarse de forma totalmente libre si bien es cierto que las dificultades en cuanto a su creación aumentan conforme avanzan los años».

No obstante, como la distribución de pornografía por medio de páginas web localizables a través de buscadores se reveló como muy vulnerable a las denuncias penales y a las acciones de piratas informáticos, se abandonó este sistema para pasar a otras nuevas modalidades conductuales. Una de ellas, eran los chats desarrollados en tiempo real en las que «los pedófilos dialogan entre sí y acuerdan intercambiarse a través del correo electrónico el referido material; la compra directa de este elemento por medio de alguna página web o la simple descarga de archivos» [196], en los que el intercambio de fotografías de pornografía infantil es cuestión de segundos. Otra de estas nuevas

---

cuentemente, también sobre pornografía, con lo que es más sencillo camuflarse en la multitud, bien porque se utilicen otras formas distintas de difusión del material, como el correo electrónico o las charlas eróticas, donde, sobre todo en éstos últimos, no hay una estabilidad suficiente por parte de los usuarios que permita que lleguen a detectarse y perseguirse eficazmente este tipo de conductas. Estas ventajas particulares para los difusores de la pornografía infantil en la Red se convierten en limitaciones para las personas que se encuentran al otro lado, dificultándose la acción policial y judicial sobre estos delitos. [...] Además, son también aplicables las ventajas generales del uso de Internet, como puede ser la rapidez de las comunicaciones, que hace el intercambio de imágenes mucho más ágil; la amplitud del mercado, que ya no se ve reducido a los clientes especiales del traficante, sino que se extiende a cualquier persona del mundo que llegue a ponerse en contacto con el traficante; y la seguridad, ya que los programas de encriptación de datos, ampliamente utilizados en las comunicaciones por la comunidad internauta ofrecen a los traficantes la posibilidad de eliminar posibles intromisiones de terceras personas en sus envíos», Rojo García, J. C., «La realidad de la pornografía infantil en Internet», en *Revista de Derecho Penal y Criminología,* 2.ª época, núm. 9, 2002, p. 218.

[195] Morillas Fernández, D. L., *Análisis dogmático y criminológico...*, *op. cit.,* p. 86.

[196] Morales Prats, F., «El Derecho penal ante la pornografía...», *op. cit.,* p. 67.

modalidades conductuales que surgieron fueron los grupos de noticias y foros como medio de comunicación, así como el camuflaje de las páginas web de pornografía infantil, no accesibles a través de buscadores y localizables solamente para iniciados.

Posteriormente, debido a que las salas de chat son evitadas por los pedófilos al darse cuenta de que pueden estar infiltrados por agentes encubiertos [197], la figura del traficante de pornografía infantil es sustituida en gran medida por la de los consumidores que informalmente se asocian sin ánimo de lucro. Estos socios, actuando coordinadamente, pueden descargarse en su ordenador multitud de fotografías en poco tiempo a través de técnicas de intercambio por medio de correo electrónico o de fórmulas como *send to receive*. En cuanto al intercambio de material pornográfico por medio de correo electrónico, se ha planteado por la doctrina la posibilidad de imponer a los servidores de correo electrónico un especial deber de cuidado en relación con el contenido que transmiten, cuestión de muy compleja solución en la práctica, que además se agrava si tenemos en cuenta que la mayoría de estos servidores ofrecen cuentas gratuitas con el simple relleno de un formulario, cuyos datos pueden ser totalmente falsificados [198]. Por lo demás, el procedimiento para el envío de *e-mails* con contenido pornográfico, no es distinto al envío de un *e-mail* con cualquier otro contenido. Se podría pensar, que las personas que se envían correos con este contenido son personas conocidas que tienen la dirección electrónica de sus destinatarios, pero como señala Morillas Fernández, «aplicando este razonamiento debería hablarse de un círculo cerrado en el que tarde o temprano escasearía el material» [199]. Por ello, aunque hemos dicho que los chats dejaron de utilizarse para intercambiar el material pornográfico, sí se han seguido utilizando posteriormente para poner en contacto a estos usuarios de pornografía infantil, que intercambian sus direcciones de correo electrónico, abriendo el círculo a otras fuentes para poder adquirir nuevo material pornográfico.

En esta acelerada evolución, los programas de globalización de archivos individuales han habilitado nuevas vías comisivas, en tanto permiten al usua-

---

[197] WORTLEY, R., y SMALLBONE, S., «Child pornography on the Internet», en *Problem-Oriented Guides for Police,* núm. 41, mayo de 2006. En Internet, en *http://www.cops.usdoj.gov/Publications/e04062000.pdf*.

[198] Morillas Fernández plantea en este sentido el caso de un sujeto que, por ejemplo, «acude a un cyber-café, crea una nueva cuenta de correo electrónico en el servidor YYY, falseando los datos necesarios para ello, y envía *e-mails* de contenido pornográfico infantil a gran escala a través de ficheros adjuntos a otros individuos repitiendo tal acción en sucesivos días pero siempre desde cyber-cafés distintos. Esta práctica, como puede suponerse, es incontrolable y aún en el hipotético caso de descubrir material, se determinarían los ordenadores a través de los cuales se realiza la transmisión pero no el sujeto que ha procedido a realizarla», MORILLAS FERNÁNDEZ, D. L., *Análisis dogmático y criminológico...*, *op. cit.,* p. 93.

[199] *Ibid.,* p. 94.

rio la posibilidad de compartir parte del contenido de su ordenador con las personas que se encuentren conectadas a la Red utilizando ese mismo programa (programas tipo Napster), de forma que los usuarios de los programas de archivos compartidos ponen en común su material pornográfico sin necesidad de entablar contacto directo, realizar adquisiciones individualizadas o mantener conversación alguna [200]. Así, el intercambio mutuo de material sustituye a la compra al traficante. Dentro de esta modalidad, debemos hacer referencia a dos tipos de protocolos, el FTP y el P2P, que dan lugar a dos tipos de comportamientos muy distintos. Con relación al uso del protocolo FTP (protocolo de transferencia de ficheros), que es uno de los más antiguos, se aprecia que es uno de los menos usados para la propagación de archivos ilícitos, ya que no existen buscadores para este protocolo al estilo de Google que permitan saber qué ordenadores están actuando en un momento dado como servidores FTP, aunque sí que existen páginas web que proporcionan listas de servidores y una descripción genérica de los archivos almacenados. Por otro lado, el protocolo P2P (*peer-to-peer,* de igual a igual), según apuntan algunos autores, es el medio del futuro para la distribución de estos archivos de pornografía, pues «el hecho de que cada uno de los servidores posea una descripción, sólo como recomendación, de los archivos de los ordenadores conectados a él hace que supere la ya explicada falta de información de FTP» [201].

Es por este último tipo de modalidades conductuales que la mera tenencia de material pornográfico infantil para su uso adquiere una mayor importancia, puesto que sin esta posesión de material en los ordenadores de los usuarios no se podría distribuir a los otros usuarios, especialmente en estas redes de P2P, en las que cada nodo funciona al mismo tiempo de servidor y cliente al mismo tiempo. Por todo ello, además de estas formas de difusión de pornografía infantil, habrá que tener en cuenta otros comportamientos que sin tratarse de «difusión» entran dentro del fenómeno de la pornografía infantil, como pudieran ser las grabaciones caseras o la mera tenencia de material pornográfico infantil para su uso.

Como destaca Morillas Fernández [202], normalmente estas conductas de pornografía infantil «suelen ir encubiertas con falsas informaciones sobre adopciones, ofertas de empleo, etc. Frente a ello los Estados poco pueden hacer si se tiene en cuenta que las fotografías o vídeos mostrados han podido ser filmados en Indonesia, haberse insertado en la Red en Filipinas, hallarse el servidor en Johannesburgo y recibir las imágenes en cualquier parte del mundo». Y es que una de las características más importantes de este fenómeno es la deslocalización en cada una de las fases del proceso, pues en la

---

[200] Consulta núm. 3/2006, de 29 de noviembre, de la Fiscalía General del Estado.
[201] Morillas Fernández, D. L., *Análisis dogmático y criminológico..., op. cit.,* p. 98.
[202] *Ibid.,* p. 22.

gran mayoría de las ocasiones no suele coincidir el lugar donde se obtienen las imágenes pornográficas, con el país del servidor al que se «suben» las mismas, y mucho menos con los distintos países a los que pertenecen los distintos usuarios que visualizan las mismas. Precisamente este rasgo es el que complica en demasía la imputación a una persona física, problema que se agrava si tenemos en cuenta que las personas físicas que están detrás de este tipo de conductas pertenecen en su gran mayoría a mafias organizadas, en las que hay una importante distribución de competencias (captación de niños, filmación de imágenes, «colgar» las mismas en la Red, fotografiado, publicidad, etc.) [203].

Y es que en la actualidad, la principal fuente de producción de pornografía infantil es la Red, pero a través de organizaciones criminales internacionales, cuyo único fin es la obtención de beneficios económicos, que realizan su actividad a través de asociaciones o empresas encubiertas que operan permanentemente [204]. El objetivo económico de estas organizaciones se satisface al abonar el destinatario una determinada cantidad de dinero como contraprestación a la adquisición del material pornográfico; una vez se abona esta cantidad, «recibirá una clave de acceso a la página en cuestión o recibirá las imágenes requeridas vía correo electrónico, o contra reembolso» [205], el producto que haya demandado, normalmente un vídeo.

Uno de los factores que adquiere en este punto un especial interés de análisis, es la determinación de la procedencia de los niños víctimas del fenómeno de la pornografía infantil. La Resolución del Parlamento Europeo sobre la Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre la aplicación de las medidas de lucha contra el turismo sexual que

---

[203] Ante estos problemas que apuntamos, la doctrina ha señalado como posible alternativa «detectar el IP del ordenador desde el que se introdujo el referido contenido pornográfico», para poder erradicar el problema desde su origen, pero como ya apunta Morillas Fernández, «las redes que se dedican a este tipo de delincuencia no suelen emplear dos veces el mismo equipo y, si lo hacen, cuentan con los mecanismos necesarios para que no se detecte el IP». Además, seguiríamos arrastrando el problema que siempre comporta la detección de la IP, pues con su identificación podremos deducir cuál ha sido el equipo desde el que se ha transmitido la información, pero todavía tendríamos que averiguar la identidad del usuario que accedió a ese ordenador en el momento.

[204] Los casos más característicos son los de adopciones u ofertas de empleo en Internet, a través de las cuales estos entes contactan con los menores e incapaces víctimas de la futura acción pornográfica. Una vez insertado el contenido de la página lo que hacen es actualizarla introduciendo material nuevo cada cierto tiempo. El único problema con el que pueden encontrarse es la localización de la página en cuestión y su expulsión del servidor con el que trabajan. La solución es muy simple, basta con cambiar la dirección del sitio —sin necesidad de modificar el contenido— y continuar así hasta que vuelva a ser descubierta o bien, cuando se calcule que el rastreo de los organismos competentes puede volver a afectar a la integridad de la página, cambiar nuevamente su ubicación a fin de no ser detectada. *Ibid.,* pp. 119 y ss.

[205] *Ibid.,* p. 121.

afecta a los niños (A5-0052/2000) [206], señala expresamente a los países de la antigua Unión Soviética como núcleo del problema del turismo sexual y la trata de seres humanos, debido a factores como las difíciles condiciones de vida y a la fronterización existente con la Unión Europea [207]. No obstante, la procedencia de estas víctimas varía dependiendo del medio o vía de difusión del material pornográfico, así, por ejemplo, la pornografía infantil que se difunde a través de DVD en video-clubs normalmente está protagonizada por menores de zonas del Tercer Mundo y Asia. Por otro lado, en aquella que se difunde a través de Internet, lo normal es que sus protagonistas sean de nacionalidad tailandesa o de algún país asiático [208]. Posteriormente, estas imágenes captadas se transmiten a través de la Red a todo el mundo [209].

2.3.3. *Difusión de otros contenidos ilícitos (especial atención al* online hate speech *o difusión por Internet de odio racial)*

No es la pornografía infantil el único contenido ilícito que se difunde actualmente a través de la Red, puesto que, como ha señalado Romeo Ca-

---

[206] *DO* C 378, de 29 de diciembre de 2000, pp. 80-87.

[207] Esta tesis es apoyada, entre otros, por el Documento 9535 de la Asamblea Parlamentaria del Consejo de Europa, de 5 de septiembre de 2002, titulado «Explotación sexual de niños: tolerancia cero».

[208] También debemos diferenciar estos comportamientos de la denominada «pornografía técnica», que es definida por Morales Prats y García Albero como aquélla «protagonizada por mayores de edad que aparentan ser menores por muy diversos medios o procedimientos ("retoque" de fotografías o filmaciones consistentes en eliminación de vello púbico o facial, suavizaciones de facciones, empleo de vestimentas de adolescentes», en los que la víctima no es un menor, sino que se trata de un adulto que se hace pasar por menor. MORALES PRATS, F., y GARCÍA ALBERO, R., «Artículo 189», en QUINTERO OLIVARES, *Comentarios al nuevo Código Penal*, Navarra, 2004.

[209] En el año 2001, ANESVAD (Organización no Gubernamental para el Desarrollo sin fines de lucro) puso en marcha una campaña de investigación sobre la pornografía infantil en Internet denominada «Nymphasex» (*http://www.anesvad.org/nymphasex*), publicándose una supuesta página pornográfica en la que se ofrecían una serie de «servicios con menores». La web se promocionó de todas las formas posibles durante 15 días con el objetivo de comprobar la reacción de todos los sectores implicados, con el problema de la pornografía infantil y los resultados fueron impactantes: 6.000 personas visitaron el sitio (400 entradas diarias de media); 542 visitantes accedieron de forma regular con el fin de comprobar si la web ofertaba nuevos servicios; cerca de 200 usuarios incluso dejaron su dirección de correo electrónico para que se les informara sobre las novedades. Transcurridos unos meses, concretamente en enero de 2002, comenzó una segunda fase. La web permaneció colgada, sin ningún tipo de publicidad, únicamente dada de alta en los diferentes buscadores que existen en Internet. El propósito era comprobar si los usuarios eran capaces de encontrar este sitio, averiguar de dónde accedían y tratar de concienciarles de la problemática de la pornografía infantil. A lo largo del año 2002, las entradas totales en Nymphasex superaron las 49.000 con una media de 4.000 al mes (usuarios únicos, ya que es muy difícil que entren más de una vez al comprobar que realmente no es una web con contenidos pedófilos). Los que más visitaron la web fueron Estados Unidos con 20.602 entradas (41,96 por 100) y España con 18.335 (37,34 por 100).

sabona, la posibilidad de introducir información en la Red con contenidos ilícitos diversos y de difundirlos a través de ella, ha convertido a la Red en un medio potente para la comisión de delitos como la apología y otros actos preparatorios del terrorismo [210]. Este tipo de cibercrimen que ha venido siendo denominado, a veces con finalidades diversas, ciberterrorismo, será analizado posteriormente cuando tratemos la cibercriminalidad política, debido a que el mismo engloba cibercrímenes «de contenido» como la difusión de mensajes de incitación a la violencia terrorista, pero también otro tipo de cibercrímenes que no entran dentro de esta categoría.

El cibercrimen que sí cuadra perfectamente en la categoría de los cibercrímenes de contenido es el que se ha denominado *cyberhate speech* o incitación al odio racial en el ciberespacio [211], delito que no es más que una adaptación al ciberespacio del crimen, ejecutado en el espacio físico en librerías y similares comercios, de difusión de contenidos de odio racial [212]. Obviamente el ciberespacio incrementa el riesgo que tal actividad supone: como ámbito transnacional y mundial, es un peligroso lugar para la difusión de mensajes racistas y violentos, que se vierten con más facilidad en Internet ante la dificultad de persecución de la cibercriminalidad y las mayores facilidades para el anonimato que da el medio [213].

Como han señalado Keats Citron y Norton, los grupos racistas pronto descubrieron las potencialidades del ciberespacio para sus objetivos [214]: Internet permitía sustituir prospectos y folletos racistas que eran difundidos localmente, por webs y blogs fáciles de hacer y que resultaban mucho más eficaces para transmitir ideas odiosas a millones de personas en todo el mundo [215]. Así cita el ejemplo de 1984 del grupo fascista *Nación Aria* que financió una publicación digital en la que se ponía una lista de objetivos del grupo, entre ellos un hombre que fue asesinado por un simpatizante de Nación Aria meses después [216].

---

[210] ROMEO CASABONA, C. M., «De los delitos informáticos al cibercrimen...», *op. cit.,* p. 4.

[211] AKDENIZ, Y., «Controlling illegal and harmful content on the Internet», en WALL, D. (ed.), *Crime and the Internet,* London, Routledge, 2001.

[212] Para un análisis profundo de este delito y de su relación con el crimen tradicional en el espacio físico de difusión de mensajes de odio racial, véase POLLOCK, E. T., «Understanding and Contextualising Racial Hatred on the Internet: A Study of Newsgroups and Websites», en *Internet Journal of Criminology*, 2010, pp. 1 y ss.

[213] En este sentido, resulta ilustrativo el trabajo de LEVIN, B., «Cyberhate: a legal and historical analysis of extremists' Use of computer networks in America», en *ABS,* núm. 45, 2002, pp. 958 y ss., especialmente pp. 966 y ss., donde se centra en la época post-Internet.

[214] KEATS CITRON, D., y NORTON, H. L., «Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age», en *Boston University Law Review,* vol. 91, 2011, pp. 1435 y ss.

[215] TIMOFEEVA, Y. A., «Hate speech online: restricted or protected? Comparison of regulations in the United States and Germany», en *JTLP*, vol. 12, núm. 2, 2003, p. 256.

[216] KEATS CITRON, D., y NORTON, H. L., «Intermediaries and Hate Speech:...», *op. cit*., pp. 1435 y ss.

Aunque no hay cifras fiables, se calcula que son miles las webs que, mayoritariamente provenientes de Estados Unidos, fomentan y difunden ideas racistas, generalmente relacionadas con la supremacía blanca, aunque también las hay que difunden similares mensajes fascistas bajo otras apariencias ideológicas [217].

A veces tales mensajes se contienen en las mismas webs de asociaciones defensoras de la supremacía blanca u otras ideologías fascistas, y en otros casos, los de las denominadas *cloaked websites*, se tratan de sitios web que aparentan ser de ONG u otras organizaciones preocupadas por problemas sociales de cualquier tipo o que simulan ser lugares de transmisión de información, y que ocultan una ideología racista que va apareciendo poco a poco en forma de mensajes web [218].

También podríamos integrar dentro de este tipo de cibercriminalidad otras páginas web en las que el mensaje de odio y de incitación a la violencia y de difusión de ideas racistas es menos abstracto y mucho más localizado contra partidos políticos, gobernantes o asociaciones concretas y determinadas. Es cierto, sin embargo, que estas conductas apenas se pueden deslindar de la incitación que suponen algunas formas de terrorismo: dos ejemplos bien conocidos serían la campaña, focalizada en Internet, de amenazas e incitación a la violencia realizada desde sectores islamistas radicales contra Dinamarca y el dibujante de un periódico que identificaba en sus viñetas a Mahoma y a los musulmanes con los terroristas [219], y por otra parte la campaña llevada a cabo por medio de vídeos en Youtube en la que se promocionaba la quema de ejemplares de el Corán como forma de protesta ante la decisión de construir en Nueva York, en la denominada Zona Cero, una mezquita.

Ambos comportamientos comparten no sólo el tratarse de mensajes de incitación al odio y a la violencia, sino que pese a realizarse en un ámbito localizado muy concreto (un humorista en Dinamarca y frente a él varios estudiantes musulmanes desde sus universidades en Siria o Irán, o un sacerdote de una pequeña iglesia de un diminuto pueblo de Estados Unidos),

---

[217] Además la tendencia es hacia el incremento exponencial de las páginas web que incitan a la violencia. Así lo señala Mahooney quien constata un incremento significativo en los últimos 15 años de las páginas web que promueven la violencia: en 1995 se estimaba que sólo había una página de Internet de ese tipo, mientras que en 2005 se han contabilizado por lo menos 5.000. MAHOONEY, K., «Hate speech, equality, and the state of canadian law», en *Wake Forest Law Review*, vol. 44, p. 322. Señala la autora que la conexión entre propaganda de odio, Internet y terrorismo también se ha intensificado a partir del 11 de septiembre de 2001.

[218] DANIELS, J., «Cloaked websites: propaganda, cyber-racism and epistemology in the digital era», en *NMS,* vol. 11, núm. 5, 2009, p. 661, donde define los *cloaked websites* como aquellos sitios web de individuos particulares, grupos u organizaciones que ocultan su verdadera identidad y la paternidad de la web para disfrazar una agenda política oculta.

[219] Dibujos sobre los que también existe la discusión de si los mismos podrían o no considerarse *hate speech* al atentar contra la dignidad de una religión y de los que la profesan. Así, al respecto, MAHOONEY, K., «Hate speech, equality, and...», *op. cit.,* p. 331.

al utilizarse Internet para la difusión del mensaje el mismo acaba llegando a muchísimas personas y generando un clima de odio con consecuencias difíciles de medir.

Qué duda cabe que la cibercriminalidad política comparte caracteres y medios con las otras formas de delincuencia en el espacio que hemos calificado como económica y social y que su prevención tendrá que ver con la de las otras formas de conducta (distribución de pornografía infantil, puesta a disposición gratuita en el ciberespacio de archivos protegidos) en las que la característica de ilicitud deviene del contenido que se difunde. Sin embargo tampoco puede negarse que el perfil criminológico de unos y otros cibercriminales es significativamente distinto, por lo que la prevención ciberespacial de los mismos tendrá que ser también diferente.

3. OTRA CLASIFICACIÓN ES POSIBLE: ATENDIENDO AL MÓVIL Y CONTEXTO CRIMINOLÓGICO

La anterior clasificación fenomenológica, en la que se distinguen los cibercrímenes teniendo en cuenta la diferente incidencia de las TIC en la esencia de la conducta criminal, puede convivir con otro tipo de clasificación aun fuera de lo jurídico cuando se diferencien los crímenes en el ciberespacio atendiendo a los distintos intereses sociales con trascendencia jurídica que se pueden ver afectados por los mismos. Me refiero, como se ha avanzado anteriormente, al punto de vista criminológico, en el que se atienda a los sujetos que realizan el delito y a sus objetivos últimos. Con esta mirada criminológica podemos afirmar la existencia de dos grandes categorías de delitos en el ciberespacio, la que reúne todos los ataques cuyo propósito último es la obtención de un beneficio patrimonial, y la que reúne todos aquellos otros en los que el objeto de ataque es una persona individual, en cualquiera de los aspectos de su desarrollo personal. Junto a ella podríamos incluir una tercera aún más incipiente que la primera, que englobaría todos los comportamientos de cibercriminalidad en los que no existe ni un propósito económico, ni un conflicto vinculado con una relación social entre personas, sino un objetivo ideológico o institucional.

La primera categoría podría denominarse «cibercriminalidad económica», atendiendo al propósito de obtención de un beneficio patrimonial por parte de quien realiza el delito; la segunda podría titularse «cibercriminalidad personal», dado que engloba ataques que afectan a las más personales esferas de desarrollo del individuo, sin embargo prefiero referirme a este tipo de delitos como «cibercrimen social» al expresar este término mejor la característica esencial del, quizá más nuevo, otro grupo de delitos en Internet: aquellos que tienen que ver con las relaciones sociales entre las personas y que no son más que la trasposición al ciberespacio de los crímenes

tradicionales derivados de conflictos entre personas. La tercera categoría la hemos querido denominar «cibercriminalidad política», aunque también podría denominarse ideológica, al pretender incluir entre otras formas de cibercrimen el *cyberhate speech* o difusión por Internet de mensajes de odio racial, así como el que se ha denominado *hacktivismo* o ciberactivismo político en la Red. En esta categoría también entrarían el ciberterrorismo, en sus distintas formas, y los ataques de denegación de servicio cuya finalidad no sea la obtención de un beneficio económico derivado del daño causado a un competidor comercial, sino más bien la causación de daños a infraestructuras u objetivos sensibles con propósito de desestabilizar a un Estado o a una institución política.

A mi parecer, la distinción entre estas tres categorías, cibercriminalidad económica, cibercriminalidad social y cibercriminalidad política, sí que es, frente a la anterior de carácter fenomenológico, una clasificación «fuerte». Es cierto que muchas de las tipologías de comportamientos que hemos situado anteriormente en la clasificación que atiende al papel de las TIC en el comportamiento, podrían ser evitadas en dos o incluso en las tres categorías. Así ocurre con el *hacking,* que puede ser una forma de obtención de datos para un posterior fraude económico, pero también un ataque a la intimidad personal de un individuo en concreto por una relación existente entre agresor y víctima, e incluso parte de un ciberataque con contenido político como el espionaje de un país a otro o la entrada en una página web gubernamental de un grupo *hacktivista.* Algo similar ocurre con los ataques de denegación de servicio que difícilmente van a constituir un cibercrimen social pero sí pueden utilizarse bien para obtener un beneficio económico o bien como ataque ciberterrorista o ciberactivista. También puede haber conductas concretas que tengan una doble motivación [220]. Pero lo usual será que los cibercrímenes de cada una de estas categorías tengan rasgos criminológicos esencialmente diversos, y que su prevención requiera de estrategias diferenciadas.

Y es que la diferenciación entre el cibercrimen económico, el cibercrimen social y el cibercrimen político no es más que la correspondencia en términos de comportamiento criminal de la distinción entre los tres grandes ámbitos funcionales del uso de las TIC. Los dos más evidentes son los dos primeros: el ciberespacio como ámbito de desarrollo de las relaciones económicas, y el ciberespacio como ámbito de comunicación y desarrollo personal. Es indudable que las dos facetas más relevantes de Internet y aquellos ámbitos en los que mayor desarrollo tiene el cibercrimen, son por una parte

[220] Difícilmente un ataque o cibercrimen económico puede ser al mismo tiempo un cibercrimen social o personal, excepto en el caso de la grabación de pornografía infantil y su posterior difusión en el ciberespacio. También improbable, aunque no imposible, es que un ciberataque terrorista acabe causando daños económicos e incluso que, en un determinado momento, se realice con esa intención.

el haberse convertido en un espacio para el intercambio económico transnacional (además de un bien económico en sí mismo y en el que confluyen bienes con valor patrimonial), y por otra el constituir el ciberespacio un nuevo ámbito para las relaciones sociales, para el contacto interpersonal entre sujetos con la consiguiente puesta en común de intereses relacionados con la intimidad, la libertad, la dignidad, etc. Es cierto que al principio, el ciberespacio tuvo mucha más trascendencia para lo primero, para el desarrollo de relaciones económicas, para mejorar la comunicación entre empresas y clientes, lo que conllevaba la entrada en el ciberespacio de bienes económicos (en forma de dinero, de datos valiosos, de nuevos servicios, etc.), consecuencia de lo cual las primeras formas de criminalidad se centraran en aprovechar ese nuevo medio para obtener beneficios económicos. Pero hoy en día Internet también sirve para que las personas contacten con otras personas, para crear redes de amigos, para comunicarse y relacionarse como seres sociales, lo que hace que las esferas más privadas de la personalidad de los que se relacionan socialmente en el ciberespacio puedan verse también afectadas.

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

Obviamente los cibercrímenes de las tres categorías comparten entre sí los caracteres del medio en el que se llevan a cabo. Pero también lo es que son fenómenos criminológicos distintos, al serlo la finalidad con la que actúan los cibercriminales en uno y otro caso y tener ellos, por eso mismo, un diferente perfil, y al ser distintos tanto el objetivo adecuado contra el que se dirigen como la incidencia de los sistemas de control en uno y otro caso. La concreción de estas diferencias en uno y otro caso las iremos analizando más adelante, cuando llegue el momento de analizar cómo cambia el ámbito de oportunidad criminal en el ciberespacio y de apuntar los perfiles de agresores y víctimas teniendo en cuenta tal clasificación criminológica. Es momento ahora, cuanto menos, de situar las tipologías de cibercrímenes que hemos analizado en el punto anterior dentro de cada uno de estos tres grandes grupos de delitos en el ciberespacio.

3.1. El cibercrimen económico: la simbiosis de los ciberataques con finalidad económica

La principal categoría de delitos en el ciberespacio es aquella que engloba a todos los comportamientos criminales llevados a cabo con la finalidad de obtener un beneficio patrimonial directo o indirecto del mismo. En sentido criminológico el cibercrimen económico, por tanto, no es tan sólo aquel tipo de ataque delictivo que afecta al patrimonio de las personas individuales o al sistema económico en relación con las transacciones comerciales en Internet. También entrarían dentro de esta categoría todos los ciberataques cuyo objetivo final sea la consecución de un beneficio económico aunque afecten a otros bienes jurídicos como la intimidad, la seguridad de los sistemas y redes, etc. El cibercriminal económico utiliza la Red, los sistemas conectados a ella, la información en ellos contenida, los servicios y cualquier otro elemento de las TIC como medio u objeto para el lucro económico, siendo en muchos casos necesario crear una cadena de ataques que, como se verá posteriormente, puede incluso ser llevada a cabo por cibercriminales distintos, pero siempre con el objetivo final del lucro económico.

En ese sentido, y como se refleja en la siguiente tabla, podríamos diferenciar dos tipos de cibercrímenes económicos, los mediales o instrumentales, y los económicos (generalmente fraudes) en sentido estricto, siendo los primeros actos preparatorios de estos últimos.

Tabla 2.4. Tipos de cibercrímenes económicos. Elaboración propia.

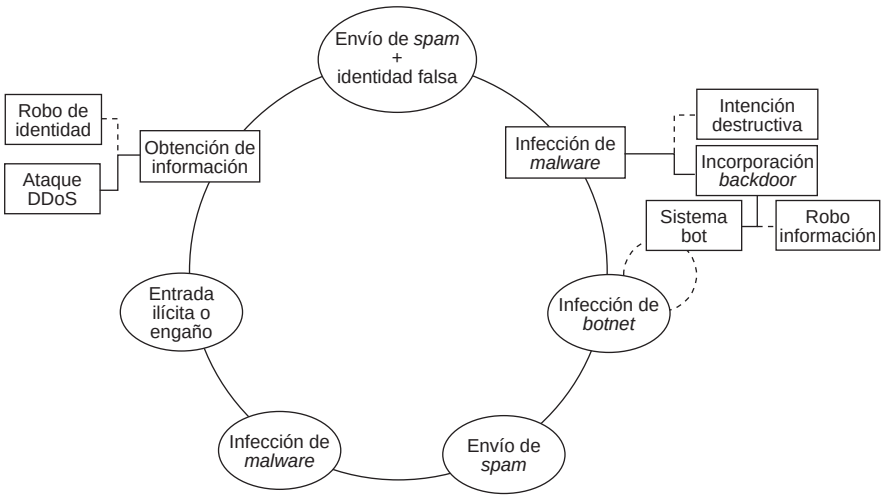
Cibercrímenes económicos mediales	*Cibercrímenes económicos puros*
Hacking	*Phishing*
Infecciones de *malware* destructivo	*Auction fraud*
Infecciones de *malware* intrusivo	*Scam*
Envío de *spam*	Extorsión
Spoofing e *identity theft*	Revelación de secretos de empresa
Uso de *spyware* (*sniffers, keyloggers*)	
Ataques DoS	

En otras palabras: la mayoría de las modalidades de ciberataques que hemos analizado por separado, no lo están en la realidad virtual de Internet. Más bien la relación entre ellos es tal que puede hablarse de una simbiosis entre gran parte de los comportamientos ilícitos realizados en el ciberespacio: unos y otros no sólo se entremezclan, sino que generalmente forman parte de una misma dinámica comisiva cuyo objetivo final es la obtención de lucro

por parte de las organizaciones cibercriminales. El envío de correos *spam*, por ejemplo, como forma de ataque a innumerables terminales informáticas, es en muchos casos, el primer paso para la posterior infección con *malware*, bien con intención destructiva de información de usuarios o de empresas (a veces con propósito de extorsión), bien con intención de incorporar una puerta trasera o *backdoor* que permita el acceso ilícito al sistema para el apoderamiento de información privada o para convertir el sistema informático en un *bot* que permita, posteriormente, su uso como *botnet* para un ataque de denegación de servicio a otra web o para el envío de cantidades ingentes de *spam* con la consiguiente «vuelta a empezar» de la cadena de ataque, o, en la mayoría de casos, para el envío de publicidad falsa tras la cual existe un ataque de *phishing,* cuyo propósito puede ser, de nuevo, la infección con *malware* para la consecución del fraude, o el engaño directo para que sea el usuario el que envíe la información privada bancaria.

La dinámica suele ser generalmente la misma con pequeños cambios, y no está muy alejada de esta:

Gráfico 2.2. Dinámicas del cibercrimen económico. Elaboración propia.



E incluso se pueden integrar en la cadena otros cibercrímenes relacionados con la distribución ilícita de contenidos. Así sucede en muchos casos con la distribución de material pornográfico, sea o no de menores, que puede encerrar un primer paso para un ataque de *phishing* o de *pharming* por parte del cibercriminal. También con la descarga de material protegido por derechos de autor, que puede esconder en muchos casos virus troyanos o infecciones de *botnet*. En el caso de la distribución de material pornográfico «lícito», se aprovecha el enorme potencial de difusión de este contenido para

atraer a los usuarios con ofertas de gratuidad. De nuevo la cadena comienza con un ataque de *spam,* en el que el correo electrónico reenvía a una página de *phishing* que contiene material pornográfico y en la que al registrarse el usuario con la promesa de material pornográfico gratuito de mayor impacto (contactos con otros usuarios, videochats pornográficos, etc.), el usuario se descarga involuntariamente un *malware* con el propósito de la posterior obtención de datos privados bancarios [221]. En el caso de la distribución de material pornográfico ilícito, usualmente de menores, los cibercriminales muchas veces controlan las propias redes de difusión del citado contenido, y aprovechan la vulnerabilidad del sujeto que trata de descargarse el mismo y el hecho de que la víctima del ataque final difícilmente denunciará unos hechos que le convertirían a él mismo en autor de un delito, para incluir entre los objetos descargados algún tipo de *malware* que permita posteriormente el acceso a las cuentas corrientes de la víctima o para utilizar su sistema informático como parte de una *botnet* que realice posteriores ataques de *spam* o de denegación de servicios. En cuanto a la descarga de obras audiovisuales o musicales, las redes P2P se han convertido en un ámbito de riesgo en el que los cibercriminales simulan el *malware* como archivos de obras protegidas con la consiguiente infección de los sistemas cuando el usuario descarga los mismos.

La perspectiva criminológica nos permite comprender, pues, que incluso los ataques que parecen tener menor lesividad como los ataques de *spam,* suelen formar parte de una cadena de ataque que puede terminar en una defraudación del patrimonio de la víctima o en la utilización de su sistema para la comisión de otro tipo de infracciones. La prevención de tales comportamientos de menor lesividad, por tanto, es esencial para evitar la proliferación de ciberataques económicos de todo tipo, y sin entrar todavía en si los mismos merecen o no una respuesta penal, lo que es indudable es que la gravedad de estos comportamientos no puede valorarse teniendo en cuenta únicamente los bienes individuales que se ven afectados sino que, en términos de riesgo penal, deben interpretarse como lo que son, auténticos actos preparatorios esenciales de los ataques lesivos más dañinos.

También son modalidades de cibercrimen económico el *hacking* más directo en el que se accede directamente a la información bancaria o incluso a la entidad para realizar el fraude, generalmente aprovechando las vulnerabilidades del sistema o las que ha ido creando la propia víctima. A veces, incluso no es necesario acceder al sistema y se puede recopilar la información necesaria para el fraude por medio de programas *sniffers*. En otros casos, incluso, el procedimiento puede ser más sofisticado y, por medio de la

[221] MANIYARA, M., «Post del blog Security Response de Symantec, 3 de febrero de 2010». En Internet, en *http://www.symantec.com/connect/blogs/phishing-using-pornographic-content-bait* (última visita el 1 de diciembre de 2010, p. 1).

minería de datos, accediendo a datos por medio de los perfiles de la víctima en las redes sociales y demás, se puede lograr información sobre una vulnerabilidad o bien configurar un *spam* personalizado con más posibilidades de éxito que el masivo [222].

La cibercriminalidad económica es, por tanto, un primer gran ámbito de delincuencia en Internet que si bien abarca múltiples tipologías de conducta diferentes entre sí, todas ellas son parte del puzle requerido para lograr el fraude económico final. Posteriormente, cuando analicemos los perfiles del cibercriminal, volveremos sobre esta modalidad de cibercrimen para ocuparnos de las muchas clases de cibercriminales económicos existentes de entre las que empieza a destacar el importante protagonismo que ocupa desde hace unos cuantos años la delincuencia organizada.

3.2. El cibercrimen «social» en la web 2.0: redes sociales, desarrollo de la personalidad en el ciberespacio y nuevos cibercrímenes

Sin lugar a dudas la delincuencia económica en Internet ha sido la gran protagonista de los primeros años de la aparición del ciberespacio y, concatenado a él, del fenómeno de la cibercriminalidad. El protagonismo futuro, o por lo menos el papel compartido, lo adquirirá probablemente en muy poco tiempo la denominada criminalidad social. Y no porque Internet vaya a dejar de ser un ámbito para la transacción económica: seguirá siéndolo y aumentarán, mutando en nuevas formas y potenciándose la importancia de las actualmente vigentes, los intercambios económicos en el ciberespacio y el valor económico de los servicios y los bienes informacionales en él; sino porque junto a este desarrollo de lo económico Internet ya hace años que hemos entrado en la web 2.0, y el ciberespacio se ha convertido en un ámbito de comunicación social importantísimo, y es este aspecto el que más se está viendo potenciado últimamente, especialmente por parte de las nuevas generaciones nacidas con la total implantación de las TIC.

Desde un primer momento Internet, en particular, y las TIC en general, fueron un vehículo para la comunicación social. Desde la propia *www* hasta el correo electrónico pasando por otros sistemas de comunicación entre personas como los canales de chat o el muy popular hace unos lustros Messenger, el ciberespacio no sólo ofrecía nuevos instrumentos para el contacto entre las personas sino que abría la posibilidad de nuevas formas de comunicación social. La unión de la Red con la telefonía móvil ya auguraba nuevos tiempos para las relaciones personales caracterizados por la reducción de la importancia de la distancia espacial y temporal. El espaldarazo definitivo, sin

[222] Véase en este sentido sobre la influencia entre la adscripción a redes sociales y el haber sido víctima de *phishing,* el estudio de JAGATIC, T.; JOHNSON, N.; JAKOBSSON, M., y MENCZER, F., «Social Phishing», en *Communications of the ACM*, Bloomington, 12 de diciembre de 2005.

embargo, lo ha dado la popularización de las redes sociales. Aunque se dice que ya en 1997 había sitios web que permitían establecer perfiles de amigos y otras funcionalidades de las redes sociales actuales, no es hasta mediados de la década pasada con la popularización de Myspace, primero, y de Facebook y otras redes más localizadas geográficamente, después, cuando las páginas web que facilitan y fomentan las relaciones entre personas sin los límites espaciales y temporales tradicionales, se convierten en un elemento esencial de la vida social para muchas personas y muy especialmente para el sector de los jóvenes [223]. Aunque es difícil situar en uno solo los elementos clave del éxito de las redes sociales, se ha dicho con razón que gran parte del mismo deriva de haber logrado permitir la convergencia entre servicios de las TIC que hasta el momento estaban separados como el correo electrónico, la mensajería directa, los chat, la creación de webs, los diarios electrónicos, álbumes de fotos, selección de música, vídeos, etc. [224]. Esto permite a los usuarios controlar el nivel de comunicación con las personas y convierte a las redes sociales por una parte en esferas de desarrollo del ocio y de las relaciones sociales en las que el nivel de intimidad plasmado en la web puede llegar a ser muy alto, y por otra en un medio integral de gestión de la propia identidad, de su personalidad y de las relaciones sociales [225].

El papel que juegan y pueden desempeñar estas redes sociales en el desarrollo de las relaciones sociales es aún mucho más significativo en los jóvenes [226]. En la etapa adolescente y preadulta donde la construcción de la identidad propia ocupa una dimensión muy significativa, un instrumento para la comunicación y el contacto social como son las redes sociales puede desempeñar un papel crucial en la vida de los jóvenes. Según las investigaciones existentes los adolescentes usan Internet para comunicarse con los amigos, para buscar otros nuevos, para buscar pareja, para compartir información personal, etcétera [227].

Lo cierto es que las redes sociales en particular e Internet en general constituyen hoy en día un nuevo ámbito de desarrollo personal, un nuevo espacio vital en el que cada individuo pasa varias horas al día, se comunica con otros, crea relaciones, etc. Lo hace desde su casa o desde el trabajo si atendemos al espacio físico que ocupa, pero ese espacio no tiene ya relevancia alguna cuando el sujeto está en Facebook comentando una opinión política, en Tuenti hablando de un compañero o en su blog personal cargan-

---

[223] BOYD, D. M., y ELLISON, N. B., «Social network sites: Definition, history, and scholarship», en *JCMC*, vol. 13, núm. 1, 2007, pp. 1 y ss.

[224] LIVINGSTONE, S., «Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression», en *NMS,* 10(3), 2008, p. 396.

[225] *Ibid.,* p. 396. Señala la autora que son los jóvenes los que están en la vanguardia de la utilización de las redes sociales según muestran todos los estudios.

[226] SUBRAHMANYAM, K.; REICH, S. M.; WAECHTER, N., y ESPINOZA, G., «Online and offline social networks: Use of social networking sites by emerging adults», en *JADP,* 29, 2008, pp. 420 y ss.

[227] *Ibid.,* pp. 422 y ss.

do un vídeo concreto. El ciberespacio es para las relaciones sociales, en ese sentido, tan real como el *meatspace* [228], y todos los comportamientos socialmente identificables que no requieren de un contacto físico directo pueden realizarse en él del mismo modo que en el espacio físico [229]. A los efectos que nos interesan, por tanto, puede afirmarse que todas las esferas personales que, al relacionarse con los demás, pueden ser puestas en peligro, lo están también en el ciberespacio; y que todas las conductas criminales de ataque a las personas que no requieran de una inmediatez física también van a acabar realizándose por medio de Internet.

Las primeras manifestaciones de esta criminalidad social se dieron ya mucho antes de la aparición de las redes sociales, con el uso de algunos de los servicios de Internet como la propia *www* o el correo electrónico y su utilización para comunicarse con otros. Como cualquier otro medio de difusión de contenidos, Internet está sirviendo desde hace tiempo para la comisión de calumnias, injurias y amenazas que son ejecutadas por medio de *e-mails* o por su publicación en páginas web. También la violación de la intimidad personal, y no sólo como parte del cibercrimen económico como medio para la consecución del futuro fraude, sino con el mero fin de desvelar secretos personales y dañar la intimidad de la víctima, se muestra como conducta delictiva en el ciberespacio debido a la ingente cantidad de información personal que los particulares colocan en sus sistemas informáticos y comparten en sus correos electrónicos y que entran en riesgo al estar tales sistemas conectados en Red. Incluso la libre formación de la sexualidad de los menores también podía ser atacada, no sólo por medio de la pornografía infantil que suele utilizar el ciberespacio únicamente para transmitir los contenidos grabados de forma previa en el espacio físico, sino por parte de abusadores sexuales que utilizan las salas de chat o sistemas de comunicación como el Messenger para realizar proposiciones sexuales a menores que luego tratan de convertir en realidad mediante un contacto con sus víctimas.

Con la web 2.0, la popularización de las redes sociales especialmente para adolescentes y adultos jóvenes y la generalización de los sistemas de telefonía móvil que permiten su conexión con el resto de servicios del ciberespacio, el catálogo de comportamientos criminales en la Red que pueden afectar a las esferas más personales del individuo aumenta cuantitativamente y, en lo cualitativo, su dañosidad es significativamente superior. En realidad,

---

[228] Término utilizado para referirse al espacio físico frente al ciberespacio. FIELDING, A., «Cyber Space, Meat Space and a Sense of Place: Lessons from the interplay of the online and offline worlds». En Internet, en *http://www.walk21.com/papers/Andrew%20Fielding_Cyber%20Space,%20Meat%20Space%20and%20a%20Sense%20of%20Place.pdf* (última visita el 19 de junio de 2012).

[229] En realidad, del mismo modo sólo en lo cualitativo, pues obviamente en lo cuantitativo el ciberespacio también potencia la capacidad de las personas para el contacto social al derribar las barreras del espacio físico.

lo que está sucediendo es que prácticamente todos los comportamientos delictivos en el espacio físico están encontrando su referente en el ciberespacio conforme la vida social empieza también a desarrollarse en ese ámbito. Así, y en cuanto a lo primero, todas las formas de acoso de una persona o grupo de personas a otra se están comenzando a dar también en el ciberespacio: bien con el simple uso del correo electrónico o de otras formas de comunicación que sirvan para enviar mensajes ofensivos contra la víctima, o de forma algo más elaborada por medio de las redes sociales que permiten tanto la exclusión de un sujeto por parte de un grupo como la creación de perfiles falsos y la difusión de imágenes, vídeos y textos relativos a la víctima con el ánimo de ofenderla y dañar su imagen o su dignidad. Aunque esto ya está comenzando a darse en el ámbito laboral como parte de las dinámicas de *mobbing*, aún más usual es encontrarnos con acoso entre adolescentes, especialmente en el ámbito escolar y no sólo utilizándose el ciberespacio en estos casos como forma de reforzar el acoso de un grupo de menores contra otro que ya tiene lugar en el ámbito del colegio, con la publicación de imágenes difamatorias, de mensajes o similares, sino incluso constituyendo la principal o única forma de acoso pero con similar potencialidad lesiva a la ejercida en el ámbito «real». También la Red es un ámbito propicio para el *stalking* o acoso continuado a una persona con permanentes solicitudes de contacto que son continuamente rechazadas por la víctima. El autor del *cyberstalking* aprovecha las facilidades para la comunicación que ofrece Internet para sumar al típico acoso telefónico el envío masivo de correos electrónicos, la solicitud de ser agregado a las redes sociales en las que está la víctima (directamente por parte de ella o por parte de los amigos de ésta), la creación de blogs y webs en los que se narra la relación con la persona acosada entre otras posibles conductas.

También forman parte de esta categoría que hemos denominado cibercriminalidad social, las conductas de acoso sexual (especialmente a menores) y que, si bien pueden efectuarse por medio de mensajes de correo electrónico o en redes sociales, es más común que se den en salas de chat en las que la comunicación entre el agresor y la víctima es más directa. Según los estudios existentes, uno de cada siete jóvenes de 13 a 17 años en Internet ha recibido una proposición sexual en el ciberespacio [230]. Aunque sobre estas conductas se volverá más adelante cuando analicemos el denominado *online grooming* o acercamiento sexual a menores con el propósito de realizar posteriormente un contacto, sí se puede adelantar que las mismas no son precisamente llevadas a cabo por el mismo tipo de «depredador sexual» que abusa de menores de 11 a 13 años [231], sino más bien por otro tipo de

---

[230] KONTOSTATHIS, A.; EDWARDS, L., y LEATHERMAN, A., «Text Mining and Cybercrime», en VVAA, *Text Mining: Applications and Theory,* John Willey and Sons, 2010, pp. 1 y ss.

[231] Así, BLAKELY, B. A., «Cyberpower in International Relations», 2010. En Internet, en *http://www.bablakely.net/wp-content/uploads/2010/12/Blakely-504Term.pdf*, p. 1.

delincuente que desde la seguridad que le da el ciberespacio realiza proposiciones sexuales directas a menores de 14 a 17 años con los que trata de quedar en el espacio real.

Mención especial por la singularidad de esta conducta realizada entre menores, y por el concreto instrumento de las TIC utilizado, merece el ya analizado *sexting*, consistente como se ha dicho en el envío a otro menor por mensajería telefónica (aunque también por medio de correos electrónicos o sistemas de mensajería en redes sociales) de fotografías de desnudos, posturas eróticas o partes del cuerpo con intención de formar parte de algún mensaje de tipo sexual practicadas normalmente por un menor. No es ésta la única conducta de entre las que estamos calificando como cibercriminalidad llevada a cabo por menores en la que se utiliza el teléfono móvil, puesto que el mismo también sirve para el envío de mensajes dentro de las dinámicas del *cyberbullying*, etc. Su singularidad estriba, en cambio, en la dificultad de su consideración como ilícito, dado que en este caso es el propio menor el que se realiza la fotografía a sí mismo y en muchos casos la envía voluntariamente a otro menor.

Por último, el teléfono móvil como instrumento de grabación o realización de fotografías e Internet en general y las redes sociales en particular como vehículo para la difusión de lo grabado, convergen en otro tipo de conductas violentas en las que si bien el acto criminal principal se realiza en el espacio físico y no es propiamente un cibercrimen, sí que deben ser mencionadas dado que la utilización de tales imágenes en el ciberespacio puede tener una entidad lesiva singular y propia. Me refiero a las conductas realizadas por grupos de menores o jóvenes adultos consistentes en la grabación de comportamientos violentos o vejatorios contra otras personas, usualmente menores conocidos por los actores víctimas de *bullying,* pero también personas mayores o cualesquiera otros individuos que puedan ser objeto de violencia y burla.

Como ya he señalado, todos estos comportamientos criminales realizados en el ciberespacio no son más que la extensión a ese nuevo ámbito de intercomunicación personal de comportamientos criminales realizados en el espacio físico. Eso no significa que los perfiles de quienes realizan unos y otros delitos sean idénticos. Como luego se verá y ya se ha adelantado para algún crimen en concreto, los especiales caracteres del ciberespacio también cambian los perfiles de quienes cometen los delitos en él. Antes de entrar en ello, en todo caso, de definir la arquitectura del nuevo medio criminal y analizar cómo incide en el delito, es el momento de terminar con la última categoría de cibercrimen.

3.3. El cibercrimen político: ciberterrorismo, *hacktivismo* y otras formas de delincuencia política en el ciberespacio

Hay una tercera forma de cibercriminalidad que no tiene que ver ni con la voluntad de obtener beneficios patrimoniales ilícitos por parte de los criminales ni con las nuevas formas de relaciones sociales en el ciberespacio y los bienes personales que se pueden ver afectados por ello, sino más bien con otra gran dimensión del ciberespacio, la de constituir el más poderoso medio de comunicación así como una herramienta imprescindible para la aplicación de políticas por parte de Estados e instituciones. Internet puede convertirse por tanto en un instrumento para la lucha política o ideológica de muchas formas distintas: puede ser vehículo de transmisión de la información que a su vez puede ser una forma de captación ideológica muy poderosa, puede ser un medio para el ataque a servicios estatales o institucionales de todo tipo en un momento en el que todos los Estados dependen de alguna forma y en muchas de sus funciones del funcionamiento de Internet, y puede ser un medio sencillo de comunicación entre individuos o grupos separados geográficamente pero unidos por una misma finalidad política o ideológica.

Todo esto configura al ciberespacio como un ámbito en el que van a aparecer diversas formas de cibercriminalidad política, de entre las que resalta muy especialmente en la actualidad el ciberterrorismo, pero entre las que irá adquiriendo cada vez más protagonismo el *hacktivismo* político tal y como han demostrado los sucesos de la denominada «primavera árabe» y otros en los que las TIC, en general, y las redes sociales y los sistemas de comunicación móvil, en particular, jugaron un papel determinante en la revolución de los países árabes.

3.3.1. *El ciberterrorismo*

Popularmente, el término ciberterrorismo [232] suena a una hipotética, en realidad futurista, utilización de Internet para la realización de ataques terroristas que atenten contra la vida o salud de miles de personas en todo

[232] Recuerdan COLARIK, A. M., y JANCZEWSKI, L. J., «Introduction to Cyber Warfare and Cyber Terrorism», en JANCZEWSKI, L. J., y COLARIK, A. M. (eds.), *Cyber Warfare and Cyber Terrorism*, Hershey-London, IGI Global, 2008, p. 13, que el término *cyberterrorism* fue utilizado en 1996 por las Fuerzas Armadas de los Estados Unidos y ha sido posteriormente aceptado de forma general. Sobre el término ciberterrorismo y los distintos usos que se le han ido dando, véase el trabajo de BALLARD, J. D.; HORNIK, J. G., y MCKENZIE, D., «Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues», en *ABS,* vol. 45, núm. 6, 2002, pp. 990 y ss. En los últimos tiempos, sin embargo, se está generalizando el sentido de ciberterrorismo que se le ha dado en este trabajo de relación amplia entre terrorismo y uso de las TIC.

el mundo [233]. Aunque los expertos en el desarrollo de las TIC dicen que la posibilidad de ataques de este tipo «no es una cuestión de si, sino de cuándo» [234], la realidad aún es más prosaica [235], y esa imagen «casi cinematográfica» se asemeja parcialmente a lo que en realidad es el ciberterrorismo que ya existe en la actualidad: la posibilidad de la utilización de las TIC para la realización de ataques premeditados y políticos contra sistemas de información que sean un potencial objetivo, así como para la difusión de sus fines y logros, con la consiguiente puesta en peligro de los intereses individuales de las personas y la afectación de la paz social como en cualquier otra forma de amenaza terrorista [236].

En efecto, si bien el término ciberterrorismo se utilizó en un primer momento tanto para referirse a los ataques a sistemas informáticos con efectos tan graves que generaban un temor comparable al que produce el terrorismo tradicional [237], como para englobar los ataques a sistemas informáticos motivados políticamente y realizados para intimidar o coaccionar a los Estados a cambio de determinadas prestaciones [238]; hoy el mismo se utiliza, en sentido amplio, como forma de referirse a los efectos de riesgo social que conlleva la unión entre terrorismo global y nuevas tecnologías de la información y la comunicación [239], esto es, para englobar todo un grupo de comportamientos distintos llevados a cabo por organizaciones terroristas pero caracterizados todos ellos por la utilización de la Red para la difusión y comunicación de contenidos relacionados con la actividad de la banda armada [240] o para la

---

[233] En general, sobre las «mentiras» y exageraciones acerca del ciberterrorismo, véase GREEN, J., «The myth of ciberterrorismo», en *WM,* noviembre de 2002, pp. 8 y ss. Es inevitable, en todo caso, que se genere «terror» ante la aparición de noticias como la de finales de 2010 relativa al ataque informático del virus Stuxnet que afectó a unos 30.000 ordenadores en Irán, aparentemente creado para sabotear el programa nuclear iraní y que puso en riesgo, según la información, la seguridad de sus instalaciones nucleares. Véase la noticia en *http://www.elpais.com/articulo/internacional/Iran/sufre/ataque/informatico/instalaciones/nucleares/elpepuint/20100928elpepiint_8/Tes* (última visita el 28 de septiembre de 2010).

[234] PRUNCKUN, H., «"Bogies in the wire": Is there a need for legislative control of cyber weapons?», en *GC,* vol. 9, núm. 3, agosto de 2008, p. 262.

[235] BROWN, I., «The Law and Economics of Cybersecurity», en *LQR,* vol. 123, 2007, p. 173.

[236] Véase, extensamente, BROWN, I., y KORFF, D., «Terrorism and the Proportionality of Internet Surveillance», en *EJC*, vol. 6, núm. 2, 2009, pp. 119 y ss., especialmente pp. 121 y ss.

[237] CURRAN, K.; CONCANNON, K., y MCKEEVER, S., «Cyber terrorism attacks», en JANCZEWSKI, L. J., y COLARIK, A. M. (eds.), *Cyber Warfare..., op. cit.,* p. 1.

[238] ROLLINS, J., y WILSON, C., «Terrorist Capabilities for Cyberattack: Overview and Policy Issues», en *CRS Report for Congress,* enero de 2007, Library of Congress Washington DC Congressional Research Service, p. 3.

[239] Distingue SUBIJANA ZUNZUNEGUI, I. J., «El ciberterrorismo: una perspectiva legal y judicial», en *Eguzkilore*, núm. 22, San Sebastián, diciembre de 2008*,* pp. 172 y ss., entre una perspectiva medial y una perspectiva final del ciberterrorismo, la primera para referirse al aprovechamiento por los grupos terroristas de las posibilidades que brindan las TIC y la medial para hacerlo a las conductas de destrucción de información sensible contenida en sistemas telemáticos o informáticos.

[240] Aunque posteriormente volveremos sobre el concepto de ciberterrorismo baste ahora con aprovechar como definición la idea de ARIELY, G., «Knowledge Management, Terrorism,

realización de ataques informáticos directos tal y como ya han demostrado algunos estudios criminológicos [241].

En realidad, podría hacerse una triple clasificación de conductas de ciberterrorismo, tal y como se presenta en la siguiente tabla, según la actividad desarrollada: difundir el mensaje terrorista, ayudar a las actividades por medio de la difusión de información, o ayudar a la actividad terrorista por medio del ataque directo.

Tabla 2.5. Conductas de ciberterrorismo. Elaboración propia.

Uso de las TIC para difusión de información		*Ciberataques directos*
Incitación y propaganda terrorista	*Actividades de apoyo informacional*	*Ciberataques terroristas directos*
Webs de incitación	Solicitud de financiación	Ataques DoS
Webs de propaganda	Órdenes a las células	Infecciones de *malware* destructivo
	Adiestramiento en fabricación de bombas, etc.	Infecciones de *malware* intrusivo
	Reclutamiento de terroristas	

Y todas estas modalidades están especialmente relacionadas con el nuevo terrorismo yihadista. Pues, y aunque por causas (no total pero sí parcialmente) desconectadas, es cierto que en el mismo período de la historia (finales del siglo pasado y principios de éste) han aparecido dos fenómenos de importancia capital: el primero, del que ya hemos hablado, el de la popularización de las TIC y la aparición del ciberespacio como nuevo ámbito de intercomunicación personal; el segundo, la aparición del terrorismo global, término que comenzó a utilizarse a partir del 11 de septiembre de 2001 para referirse a aquel tipo de actividad terrorista caracterizada por ser transnacional, como ya lo era en parte el terrorismo internacional clásico, pero, también, por tener pretensiones políticas o desestabilizadoras a nivel mundial y, por tanto, afectar no a Estados concretos y particulares, sino a todos ellos en

---

and Cyber Terrorism», en JANCZEWSKI, L. J., y COLARIK, A., *Cyber Warfare and Cyber Terrorism,* Idea Group Inc (IGI), USA, 2008, pp. 7 y ss., cuando señala que el ciberterrorismo no es más que la convergencia, en todos sus sentidos y posibilidades, del terrorismo y el ciberespacio y está especialmente unido al terrorismo no virtual en general y al nuevo terrorismo global en particular.

[241] A lo cual se podría sumar otra modalidad, aportada por TOUNTAS, S. W., «Carnivore: Is the Regulation of Wireless Technology a Legally Viable Option to Curtail the Growth of Cybercrime?», en *WUJLP,* vol. 11, 2003, p. 362, que consistiría en el uso de las TIC para evitar la detección de las actividades terroristas por parte de los servicios de inteligencia. Señala el autor que éste fue uno de los primeros usos que el terrorismo internacional dio a las TIC.

general [242]. El terrorismo global está claramente protagonizado por el terrorismo islamista, como concepto englobador de los distintos grupos terroristas adscritos al islamismo radical, y muy en particular por Al Qaeda, que más que un grupo terrorista conforme a la comprensión tradicional del mismo, se puede considerar como una ideología organizada para el odio terrorista.

Lo cierto es que las TIC en general, e Internet muy en particular, se han convertido en un poderoso aliado para un gran número de grupos terroristas clásicos [243], pero muy especialmente para esta nueva forma de terrorismo que, por su carácter transnacional y por englobar, ideológicamente hablando, todo un conjunto de grupúsculos y de personas individuales unidas por el fundamentalismo ideológico radical y el odio a Occidente, requiere de formas de comunicación y de difusión de la información a nivel interno y externo, que superen los sistemas tradicionales anteriores a la aparición del ciberespacio.

Ese tipo de comportamientos, pues, conformarían el primer gran grupo de conductas de ciberterrorismo, el que entronca el fenómeno con los cibercrímenes de contenido, todas aquellas en las que se usan las TIC para difundir por Internet contenidos, genéricos o específicos, de difusión de mensajes de violencia y de incitación al terrorismo o, más generalmente, como «plataforma de adoctrinamiento y radicalización yihadista de cientos de miles de individuos musulmanes repartidos por todo el mundo que, por diversas razones, sienten la necesidad de defender al islam del yugo representado por occidente» [244].

En relación con estas modalidades de conducta el ciberterrorismo tiene especial relevancia en los últimos años debido a que ha venido unido al terrorismo yihadista o terrorismo global, en el que la falta de jerarquía directa entre las células separadas entre sí por grandes distancias geográficas se compensa con la existencia de un mensaje único que solamente tiene que ser transmitido a todos los pertenecientes a esa idea que es Al Qaeda [245]. Las TIC son, en este sentido, una magnífica herramienta para la comunicación inter-

---

[242] Véase al respecto los trabajos de REINARES NESTARES, F., *Terrorismo y antiterrorismo,* Barcelona, Paidós Ibérica, 1998, pp. 25 y ss.

[243] En este sentido señala WEIMANN, G., «The Psychology of Mass-Mediated Terrorism», en *ABS,* vol. 52, núm. 1, septiembre de 2008, p. 76, que en la actualidad prácticamente todas las bandas terroristas activas mantienen sitios web, entre las cuales señala las siguientes: Hamás, Hezbolá, las Brigadas Mártires de Al Aqsa, Ansar el Islam, el Frente Popular para la Liberación de Palestina, y otros muchos grupos dentro del mundo árabe radical; ETA, el Ejército Corso y el IRA, en Europa; Túpac Amaru, Sendero Luminoso, las FARC y el ELN en Iberoamérica, y Aum Shinrikyo, el Ejército Rojo Japonés, el Movimiento Islámico de Uzbekistán (IMU) y el movimiento rebelde del Cáucaso Norte, en Asia.

[244] CANO PAÑOS, M. Á., «Internet y terrorismo islamista: aspectos criminológicos y legales», en *Eguzkilore,* núm. 22, San Sebastián, diciembre de 2008, p. 68. Resulta especialmente interesante el análisis que realiza el autor de los diferentes perfiles de nuevos terroristas islamistas existentes y de la influencia que en ellos y en el propio proceso de reclutamiento, tiene el uso de las TIC.

[245] ARIELY, G., «Knowledge Management, Terrorism...», *op. cit.,* pp. 8 y ss.

na, para la difusión de mensajes entre los miembros de la organización [246] relativos a los objetivos, a la financiación o a cualquier otra actividad organizativa. Esta modalidad de uso de Internet para las organizaciones criminales y terroristas tradicionales resulta innecesaria e incluso peligrosa por las posibilidades de detección de las mismas por los servicios de inteligencia, pero que para organizaciones terroristas como Al Qaeda, que constituye más bien el conglomerado de los pequeños grupúsculos terroristas dirigidos por una ideología global de odio que marca objetivos y modelos de ataque, resulta esencial [247]. Siendo ésa la estructura y siendo las dimensiones del terrorismo yihadista transnacionales, el contacto entre jefes de células o entre los propios miembros resulta generalmente muy complejo, por lo que es mucho más sencilla y eficaz la transmisión a través de Internet, bien mediante mensajes globales definitorios de objetivos genéricos en determinados momentos, o bien de comunicados concretos a grupos o terroristas específicos. A ello hay que sumar la utilización de Internet para dar sensación de pertenencia [248], lo cual en este tipo de organizaciones con células disgregadas acaba siendo muy importante.

Dentro de esta forma de uso de Internet por parte del terrorismo islamista radical podrían abarcarse, pues, todas las formas de promoción externa de la organización, entre ellas, como señala Cano Paños, algunas de las siguientes: el uso de las TIC para llevar a cabo amenazas contra sujetos en particular, Estados, organismos o formas de organización social y cultural; como foro de propaganda del terrorismo islamista en el que se ensalcen y justifiquen sus actividades; etcétera [249].

Junto a estas actividades de ciberterrorismo que hemos denominado de incitación y propaganda, habría un segundo grupo de conductas también caracterizadas por el uso de las TIC para informar y comunicar; no obstante, éstas ya no consistirían en la incitación general a la actividad terrorista o en la propaganda de las actividades de la banda, sino en el aprovechamiento de las TIC para la difusión de mensajes internos, de órdenes explícitas o incluso para recaudar fondos a través de páginas web de supuestas asociaciones

---

[246] Recuerdan BROWN, I., y KORFF, D., «Terrorism and...», *op. cit.,* p. 123, que la estructura de las webs que transmiten este tipo de información es muy diversa, según se trate de organizaciones terroristas tradicionales, como Hezbolá, en la que la jerarquía es total y hay instrucciones directas para sus miembros, o Al Qaeda, webs mucho más interactivas por no ser propiamente organizaciones jerárquicas y en las que los mensajes son más abiertos.

[247] Véase en este sentido el análisis llevado a cabo por WEIMANN, G., «The Psychology...», *op. cit.,* p. 76, de la utilización por Al Qaeda de los distintos servicios que ofrece Yahoo, tales como las salas de chat, el correo electrónico y especialmente los grupos dedicados a un asunto específico y cerrado a los miembros del mismo modo que las redes sociales, cuya creación es gratuita, libre, rápida y muy sencilla, por lo que es usado por los partidarios y los propios terroristas de Al Qaeda para hacer la crónica de sus victorias o proporcionar material multimedia relacionado con la Yihad.

[248] BROWN, I., y KORFF, D., «Terrorism and...», *op. cit.,* p. 122.

[249] CANO PAÑOS, M. Á., «Internet y terrorismo islamista: aspectos criminológicos y legales», *op. cit.,* p. 69.

benéficas o de ONG; como forma de reclutamiento de futuros terroristas a través de foros, chats y canales IRC, visitados por individuos receptivos a tal ideología extremista [250]; como «campo de entrenamiento virtual» para los terroristas, con la transmisión de los conocimientos necesarios para realizar los atentados o para dotarse de los instrumentos requeridos para hacerlo [251].

En tercer lugar, y como segunda gran categoría, también es posible otro tipo de ciberterrorismo en el que las TIC jueguen un papel aún más predominante: se trataría de la realización de ataques informáticos, principalmente de denegación de servicio, contra objetivos sensibles del Estado al que se ataca, ya sea éste el objetivo directo, ya sea sólo una forma de impedir el ejercicio de los servicios de inteligencia o cualesquiera otros servicios necesarios para la defensa del Estado de que se trate. Así lo han hecho, según los datos de la inteligencia antiterrorista existente, organizaciones terroristas como Al Qaeda, Hezbolá o la insurgencia iraquí. También entrarían dentro de esta última modalidad el envío de *malware* o el propio acceso informático ilícito siempre que el objetivo sea dañar una estructura de defensa del «enemigo».

Este ciberterrorismo en sentido puro o estricto consistiría, pues, en la realización de ataques a través de la Red por parte de los terroristas a sistemas informáticos para dañarlos o lograr la inutilización operativa de sistemas de información, logísticos o de intervención [252]. Aunque es una posibilidad el que se utilice Internet para atacar los sistemas de información del «enemigo» y, así, debilitarle, no suelen ser las propias organizaciones terroristas yihadistas las que se ocupan de estas actividades, sino que más bien son jóvenes musulmanes radicales con conocimientos básicos de informática, los que pueden realizar ataques de este tipo, pero de potencialidad lesiva muy limitada. Aun así, la inteligencia norteamericana considera fiables algunas informaciones relativas a la creación, desde el extremismo islamista, de una

---

[250] Como ejemplo de lo sencillo que puede resultar crear un sitio web para la realización de todo ese tipo de actividades, podría citarse el caso recordado por WEIMANN, G., «The Psychology...», *op. cit.,* p. 75, de la primera página web permanente que utilizó Al Qaeda bajo la apariencia de una organización ficticia, el Centro Islámico de Estudios e Investigación, gracias a una simple cuenta de correo de Hotmail y al envío de 87 dólares a un banco de Malasia para pagar el hospedaje de la web durante un año. Sobre las actividades que desde Al-Neda llevó a cabo Al Qaeda, especialmente en lo relativo a la difusión del mensaje del terror, véase el extenso trabajo de KOHLMANN, E. F., «"Homegrown" Terrorists: Theory and Cases in the War on Terror's Newest Front», en *ANNALS,* núm. 618, julio de 2008, pp. 99 y ss.

[251] En este sentido, son múltiples las posibilidades de entrenamiento virtual relatadas por SPRING, T., «Al Qaeda's Tech Traps. Investigations, arrests highlight how technology aids and weakens terror network», en *PCWorld*, septiembre de 2004. En Internet, en *http://pcworld.about.net/news/Sep012004id117658.htm* (última visita el 9 de septiembre de 2010), tales como enseñanzas para crear un lugar seguro, disimular el aspecto, saber desaparecer, etcétera.

[252] CURRAN, K.; CONCANNON, K., y MCKEEVER, S., «Cyber terrorism...», *op. cit.,* p. 2, también, SIEBER, U., y BRUNST, P., *Cyberterrorism. The use of the Internet for terrorist purposes*, Strasbourg, Council of Europe Publishing, 2008, pp. 25 y ss.

«armada islamista de *hackers*» que perpetren ciberataques contra el gobierno de Estados Unidos y otros objetivos enemigos [253].

Si a todo lo señalado sumamos los caracteres intrínsecos del ciberespacio, especialmente la transnacionalidad de ese medio de comunicación, su popularización en todas las sociedades y en todos los estratos, las facilidades para el anonimato que el mismo otorga, y las dificultades para la persecución de tales actividades a nivel nacional, se puede comprender la preocupación existente por este nuevo contexto de la violencia terrorista que se ha denominado ciberterrorismo.

3.3.2. *La ciberguerra*

No sólo los grupos terroristas, sino también los propios Estados, aprovechan Internet para debilitar a sus enemigos, hasta el punto de que hay quienes apuntan que la guerra cibernética [254] no está tan lejana como puede parecer: esta amenaza ha tomado el lugar que ocupaba hasta hace poco la guerra nuclear [255]. Sin entrar a valorar la realidad de ese tipo de amenazas, lo que es innegable es que hoy Internet puede ser una poderosa arma para ser utilizada frente a Estados, instituciones y demás por parte de gobiernos de todo el mundo y en relación con cuestiones muy diversas. Dos ejemplos paradigmáticos de esto son el ataque de denegación de servicio de Rusia a

---

[253] Véase en este sentido el reportaje de WATERMAN, S., «Islamists Seek To Organize Hackers' Jihad in Cyberspace», en *WT,* agosto de 2005, p. 9.

[254] Para referirse a este tipo de ciberataques entre Estados se suele utilizar en inglés el término *cyberwarfare*, si bien la literatura especializada utiliza a veces de forma poco precisa indistintamente el término *cyberterrorism* y el de *cyberwarfare*. Colarick y Janckcewsky proponen una interesante diferenciación entre ambos conceptos: mientras que el ciberterrorismo serían los ataques premeditados y motivados políticamente de grupos nacionales o agentes clandestinos o los actos individuales contra terminales informáticas, programas y la información en ellos contenidos que se traduce en violencia contra objetivos no combatientes, el término *cyberwarfare* serviría para definir los ataques planeados por naciones o sus agentes contra sistemas informáticos, terminales y demás con la intención de causar daños en el enemigo, COLARIK, A. M., y JANCZEWSKI, L. J., «Introduction to Cyber Warfare...», *op. cit.*, pp. 13 y 14. Esa definición, en realidad, muestra que el *cyber warfare* no es más que una actualización al ámbito del ciberespacio del *information warfare,* definido tradicionalmente como las acciones destinadas a proteger, explotar, corromper, impedir o destruir información o recursos de información con la intención de producir una significativa ventaja o victoria sobre el adversario., KNAPP, K. J., y BOULTON, W. R., «Ten Information Warfare Trends», en JANCZEWSKI, L. J., y COLARIK, A. M. (eds.), *Cyber warfare and cyber terrorism,* Information Science Reference, 2008, p. 18. Aunque no comparto la definición de ciberterrorismo que dan los autores, puesto que el mismo no debe englobar tan sólo los ataques a la información o a los sistemas con el objetivo de dañar al enemigo sino, como se ha visto y se verá posteriormente de forma más detenida, todas las actividades de facilitación de los grupos terroristas en el ciberespacio, sí creo que puede aprovecharse la diferenciación que realizan para señalar que el criterio de distinción de los dos conceptos, es el protagonista de los ataques: grupos terroristas en el ciberterrorismo, Estados en la guerra cibernética como modernización a la sociedad de las TIC de la guerra de información.

[255] BLAKELY, B. A., «Cyberpower in International Relations», 2010. En Internet, en *http://www.bablakely.net/wp-content/uploads/2010/12/Blakely-504Term.pdf*, p. 1.

Georgia durante la guerra de Osetia y la infección del virus Stuxnet a los sistemas informáticos del programa nuclear iraní llevado a cabo por Israel.

En cuanto al primero, quizás el más claro ejemplo de guerra cibernética al venir unido a actos de guerra real, se produjo en agosto de 2008 cuando tropas militares rusas respondieron a lo que consideraron una provocación de Georgia por haber entrado en el territorio semiautónomo de Ossetia. No sólo atacaron con bombas y balas sino también con un ataque de DDoS que afectó a múltiples páginas web del gobierno de Georgia, dejando sin uso varios servicios de Internet y obstruyendo y dificultando la comunicación de varias de las oficinas con sus tropas y ciudadanos. Los ataques de denegación de servicio vinieron unidos a otros ataques de *hackers* en los que se modificaban las webs oficiales del gobierno de Georgia con mensajes de propaganda nacionalista rusa [256]. Aunque Georgia acusó al gobierno ruso de perpetrar un ciberataque contra ellos, Rusia negó el patrocinio o el apoyo de tales conductas alegando que provendrían probablemente de personas con un excesivo sentimiento nacionalista y como respuesta a la agresión de Georgia [257].

Precisamente con Rusia también tuvo que ver el ataque perpetrado contra Estonia en la primavera del año anterior, 2007, cuando se decidió retirar una estatua de bronce al «soldado soviético» de un parque del puerto marítimo de Tallin. Las autoridades del país esperaban protestas airadas de los rusos o de los habitantes de su país de origen ruso, pero no todo el conjunto de ciberataques, generalmente de denegación de servicio, que tuvo prácticamente paralizado durante varias semanas el ciberespacio de aquel país y que duró casi un mes hasta que el gobierno pudo estabilizar la situación [258]. Quizás lo más significativo del caso de Estonia, cuanto menos en lo que implica de toma de conciencia de la importancia de la amenaza, es que, como recuerdan Sommer y Brown en el informe para la OCDE [259], a partir de aquel momento la OTAN creó la CDMA (Cyber Defence Management Authority) con la intención de dar asistencia a los países miembros de la organización en el caso de que hubiera un ciberataque de este tipo [260].

---

[256] Ophardt, J. A., «Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow's battlefield», en *DLTR,* núm. 3, 2010, p. 3.

[257] No fueron éstos los únicos casos de ciberataques realizados como continuación a ataques armados previos, y no siempre es fácil saber si realmente es el gobierno el que está detrás de los mismos. Según relatan Colarik, A. M., y Janczewski, L. J., «Introduction to Cyber Warfare and...», *op. cit.,* pp. 14 y ss., inmediatamente después de que un avión militar americano cayera en la costa de China, *hackers* de ambos países comenzaron a perpetrar ciberataques contra webs del otro país; y también hubo ataques durante los conflictos de Pakistán con la India, Israel y Palestina y durante la guerra de los Balcanes.

[258] Jenik, A., «Cyberwar in Estonia and the Middle East», en *NS*, núm. 4, abril de 2009, pp. 4 y ss.

[259] Sommer, P., y Brown, I., «Reducing Systemic Cybersecurity Risk. Contribution to the OECD project Future "Global Shocks", 2011», disponible en *http://www.oecd.org/dataoecd/57/44/46889922.pdf* (última visita el 19 de junio de 2012, p. 74).

[260] La OTAN estableció un centro de excelencia en la capital de Estonia, Tallin, y está analizando opciones de cooperación futura en materia de ciberdefensa.

De diferente tipo es el otro caso de guerra cibernética, quizá el más llamativo, el del virus gusano Stuxnet, presuntamente creado por el gobierno de Israel y destinado a infectar los sistemas informáticos utilizados en el programa nuclear iraní. Aunque los ciberataques entre Israel y los países árabes o los *hackers* islamistas radicales (muy particularmente un grupo de *hackers* marroquíes pero también de otros países) existen desde 1999 cuando empezó una guerra de ataques cibernéticos que no ha parado [261], el capítulo de Stuxnet es distinto, pues supone un boicot informático de primer orden que habla por sí solo del poder del ciberespacio. Además lo cierto es que Stuxnet parece haber tenido éxito, al menos según las noticias que llegan a Occidente: este virus ha logrado, aprovechando una vulnerabilidad del sistema, tomar el control de parte del sistema operativo que debía ser de uso exclusivo de los iraníes para el control de su programa nuclear, y está retrasando éste de forma más que significativa.

A mi parecer, no es demasiado difícil prever que las posibilidades de ciberataques de este tipo entre Estados, entre organizaciones o de organizaciones criminales contra Estados irán en aumento en los próximos años conforme vayan aumentando los servicios que los distintos Estados vayan ofreciendo a sus ciudadanos a través del ciberespacio. Hoy todavía son pocos los recursos estatales en Internet, o cuanto menos no parece que el corte de cualquiera de los que hay pueda suponer algo catastrófico. Ahora bien, conforme vayan llegando al ciberespacio servicios sociales relacionados con la seguridad personal, la sanidad, la educación, etc., la importancia de los ciberataques irá en aumento. No parece absurdo imaginar la extorsión realizada contra Estados o gobiernos ante el «secuestro» de servicios básicos realizados a través de Internet en los que se pida algo a cambio de cesar el ataque. Este es el aspecto de la ciberguerra que más parece acercarse a lo previsible para muy pronto.

3.3.3. *El ciberhacktivismo*

También se puede considerar criminalidad política, aunque no se trate en este caso de lucha entre Estados, el que se ha venido en denominar *hacktivismo*. La unión de los términos activismo y *hacker* en este concepto, que cada vez está adquiriendo mayor relevancia mediática, sirve para englobar todo un conjunto de ataques llevados a cabo por *hackers* informáticos, pero no con una finalidad maliciosa de defraudar a las víctimas, de robarles información para traficar con ella o de causar daños para perjudicarles económicamente, ni siquiera con la mera voluntad de superación de barreras que parecía distinguir a *hackers* y *crackers*, sino con la intención de lanzar un

[261] Así se relata en este artículo que se ocupa especialmente de los ciberataques en Estonia. JENIK, A., «Cyberwar in Estonia and the Middle East...», *op. cit.,* p. 1.

mensaje ideológico, de lucha política y defensa de ideas generalmente relacionadas con la libertad en Internet [262], aunque teniendo cabida cualesquiera otras convicciones ideológicas.

Al fin y al cabo, y como señaló Alexandra Samuel, el *hacktivismo*, matrimonio del activismo político con la *hacking* informático, conlleva la búsqueda de soluciones en la tecnología, en general, y en Internet en particular a problemas sociales o políticos [263]. Esta mezcla entre la consecución de objetivos políticos fuera de la Red y la propia Internet como objetivo político principal del *hacktivismo* se muestra en el desarrollo de los primeros grupos hacktivistas, The Cult of the Dead Cow, y Electronic Disturbance Theater (EDT), el primero centrado esencialmente en la neutralidad en la Red y el segundo que utilizaba Internet para realizar acciones de desobediencia civil electrónica dirigidas contra el gobierno de México como forma de apoyo a los grupos zapatistas [264]. A partir de ahí el *hacktivismo* ha sido de muchos tipos y en muchos lugares, si bien como se verá al hablar de Anonymous más adelante, ha seguido manteniendo una mezcla entre la defensa de la filosofía libertaria de Internet y la búsqueda de que la misma, en lo que a juicio de los *hacktivistas* conlleva de defensa de la libertad, se expandiera al espacio físico.

Como ha señalado Jordan, además de los propios ataques *hackers* realizados para demostrar la capacidad individual de superar barreras de seguridad, en la actualidad hay activistas *hackers* que han convertido sus intrusiones en sistemas y redes en una actividad política dirigida contra los sectores de la industria y los estados que tratan de controlar el ciberespacio [265]. Y ésa es la característica esencial del *hacktivismo*: frente a los *hackers* de primera, segunda y tercera generación en los que el fin político no existía, era más bien indirecto, o estaba muy localizado, hay en la actualidad un grupo de *hackers* para los que la política es la auténtica razón de ser de su actividad [266].

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

---

[262] ALLEYNE, B., «Sociology of Hackers Revisited», en *TSR,* vol. 58, 2010, pp. 1-35. Señala el autor que en el caso de los *hacktivist* la, cuanto menos en lo ideal, barrera entre *hackers* clandestinos (*black hat* o aquí denominados *crackers*) y abiertos (*white hat*) se diluye significativamente, dado que si bien no actúan con un propósito criminal en su propio beneficio, tampoco se puede decir que los *hacktivistas* estén en el plano de la legalidad.

[263] SAMUEL, A. W., *Hacktivism and the Future...*, *op. cit.*, citada por FITRI, N., «Democracy Discourses through the Internet Communication: Understanding the Hacktivism for the Global Changing», en *OJCMT,* vol. 1, núm. 2, abril de 2011, p. 8.

[264] FITRI, N., «Democracy Discourses through the Internet...», *op. cit.,* p. 10.

[265] JORDAN, T., *Hacktivism and Cyberwars: Rebels with a Cause?,* London, Routledge, 2004.

[266] TAYLOR, P. A., «From hackers to hacktivists: speed bumps on the global superhighway?», en *NMS,* vol. 7, núm. 5*,* 2005, pp. 626 y ss.

por otros usuarios, e incluso, aprovechando la web 2.0 para la creación de blogs y webs o de grupos en las redes sociales más importantes en los que se informa de los objetivos políticos-ideológicos del *hacktivismo*, se organizan protestas y acciones y se definen los objetivos que se deben combatir [267].

En realidad y como se puede ver en el siguiente gráfico, el *hacktivismo* no hace más que aplicar en el ciberespacio algunas de las técnicas tradicionales utilizadas para el activismo político callejero [268]:

Tabla 2.6. Técnicas de *hacktivismo*. Elaboración propia.

Civil desobedience	*Hacktivism*
Sit-ins	*Web site defacements*
Barricades	*Web site redirects*
Political graffiti	*Site parodies*
Wildcat strikes	*DoS attacks*
Underground presses	*Information theft*
Political theater	*Virtual sit-ins*
Sabotage	*Virtual sabotage*
	Software development

Todas estas actividades se llevan a cabo, como se verá posteriormente con más profundidad, por grupos semiorganizados: pequeños grupos que lideran concretas incitativas y que permiten sumarse a quienes quieran otros *hackers* que compartan objetivos. En este sentido, y con ese único paralelismo, el *hacktivismo* se asemeja al ciberterrorismo de grupos como Al Qaeda: no hay una dirección jerárquica que defina las acciones de los *hackers* a nivel mundial, pero sí una filosofía política o ideológica común que une a todos aquellos que, desde cualquier parte del mundo, pretenden combatir el intento de la industria y de los estados por controlar Internet [269].

---

[267] Alleyne, B., «Sociology of Hackers Revisited...», *op. cit.,* p. 10.

[268] Fitri, N., «Democracy Discourses through the Internet...», *op. cit.,* p. 13.

[269] Lo cual no significa que no haya grupos concretos y más o menos amplios de ciberactivistas que funcionen de forma más o menos coordinada y que puedan tener cierta estructura jerárquica interna. El caso más significativo de esto sería, sin lugar a dudas el del grupo Anonymous, sobre el que se tratará a continuación. Su similitud con las células del terrorismo insurgente de Al Qaeda es implícitamente reconocida por los propios miembros de Anonymous en una interesante entrevista en el diario *El País*: «Salvando las distancias, es como una organización insurgente basada en células, compartimos una marca, Anonymous, pero somos gente independiente, que responde a una ideología común y que participa de cada acción particular de acuerdo con si coincide o no con sus convicciones». *El País,* «Somos Anonymus», 16 de enero de 2011. En Internet, en *http://elpais.com/diario/2011/01/16/domingo/1295153553_850215.html*. Sobre esto se volverá posteriormente en cap. IV.2.2.

Ése es, por otra parte, el gran fondo ideológico del *hacktivismo*, el código *hacker* en su esencia [270] y que se resume en la defensa de la libertad en, y la neutralidad de, Internet y en la lucha contra cualquier barrera que se pretenda imponer en el ciberespacio. Esto hace que los ciberactivistas hayan actuado contra el intento de algunos gobiernos por controlar Internet, contra las instituciones públicas y privadas que tratan de poner coto a la libre difusión de archivos en el ciberespacio. No obstante, es cierto que en algunos casos se ha ido más allá y los ataques de denegación de servicio han tenido que ver con otras cuestiones ideológicas lejanas de lo relacionado con Internet como las protestas estudiantiles en el Reino Unido, o en relación con la inmolación de un joven en Túnez a raíz de la crisis de gobierno que se produjo en enero de 2011 y que acabó con la huida del presidente de aquel país.

Evidentemente, en relación con el *hacktivismo*, y no sólo por estos comentados ataques de denegación de servicio perpetrados por el grupo Anonymous ante la persecución de Assange por parte de Estados Unidos, está el fenómeno Wikileaks, la página web que después de haber publicado antes información confidencial y haber desvelado las torturas de Abu Graib, saltó a la fama mundial el 28 de noviembre de 2010 al comenzar a publicar parte de más de 250.000 cables enviados por 274 embajadas de Estados Unidos al gobierno y en los que se informaba de secretos de política estadounidense así como de la visión de las embajadas de Estados y dirigentes de todo el mundo. De nuevo debemos matizar que por situarlo en esta categoría de la cibercriminalidad política no estamos afirmando que se trate de un comportamiento delictivo. Sólo sería así si se demostrase que la información publicada por esta página de Internet ha sido obtenida ilegalmente. Wikileaks, en todo caso, y por eso nos interesa aquí, muestra como pocos fenómenos la capacidad del ciberespacio para transformar determinados aspectos de la realidad social, en este caso el periodismo y el funcionamiento de la difusión de información política entre distintos organismos de los Estados, así como el enorme poder y capacidad disruptiva que tiene la información en el ciberespacio.

Como decía, el fenómeno Wikileaks no puede desligarse de la ética *hacker* y del *hacktivismo* pese a que la imagen pública de Julian Assange haya hecho que parezca el proyecto de una única persona [271]. De hecho el que está considerado su lema o principio fundacional, «la información quiere ser libre», no es más que parte de la declaración de la ética *hacker* junto con otras ideas esenciales relacionadas con Wikileaks como la voluntad de mantener Internet libre de censura [272]. Además de los propios ataques de denegación

---

[270] Véase *infra* cuando analicemos el código *hacker.*

[271] NAYAR, P. K., «WikiLeaks, the New Information Cultures and Digital Parrhesia», en *Economic & Political Weekly,* núm. 52, 25 de diciembre de 2010, pp. 1 y ss.

[272] Véase por ejemplo la declaración hacktivista de *The Cult of the Dead Cow* (CDC) en *http://www.cultdeadcow.com/cDc_files/HacktivismoFAQ.html*.

de servicio que pueden venir ligados o no a este fenómeno[273], Wikileaks demuestra que el *hacktivismo* también se puede llevar a cabo de muchas otras formas, por ejemplo, mediante la difusión de información en páginas web que puede ser más destructiva para algunos Estados que cualquier ataque de DDoS.

En todo caso, conviene matizar que la utilización de Internet con fines de divulgación política e ideológica no siempre, sino más bien excepcionalmente, se situará en el marco conceptual del cibercrimen. El activismo político en el ciberespacio es tan legítimo como fuera de él, si bien lo que sucede es que los Estados están mucho más preocupados y por tanto tentados de regular legalmente más allá de lo que permitiría el libre ejercicio de la expresión en un Estado democrático, por el inmenso poder de difusión de mensajes e ideas y de convocatoria de manifestaciones y reuniones que tiene el ciberespacio, que lo que estaban antes de su existencia. Así, sucesos como la Primavera árabe o las protestas del 11-M y Occupy Wall Street, no tratándose de cibercriminalidad, son *hacktivismo* que empieza en el ciberespacio y termina en las calles con miles de personas unidas gracias a las inmensas posibilidades que ofrece Internet.

[273] Hay que recordar que en el caso de Wikileaks no fue el grupo Anonymous el primero en realizar el ataque de DDoS, sino que la propia web de Wikileaks sufrió varios ataques de ese tipo. PRAS, A.; SPEROTTO, A.; MOURA, G. C.; DRAGO, I.; BARBOSA, R.; SADRE, R.; SCHMIDT, R., y HOFSTEDE, R., «Attacks by "Anonymous" WikiLeaks Proponents not Anonymous», *CTIT Technical Report 10.41,* 10 de diciembre de 2010. En Internet, en *http://eprints.eemcs.utwente.nl/19151/*, pp. 1 y ss. Ésa sería, al fin y al cabo, otra forma de cibercriminalidad política: una ciberguerra de ataques de denegación de servicio entre partidarios y enemigos de una determinada concepción ideológica de la Red.

SEGUNDA PARTE

CRIMINOLOGÍA DEL CIBERCRIMEN

CAPÍTULO III

CIBERESPACIO Y OPORTUNIDAD DELICTIVA

1. INTRODUCCIÓN

Ya hemos asumido que la nuestra es una sociedad nueva: la sociedad de la información, sociedad digital o sociedad red, caracterizada porque son las TIC las que impulsan múltiples cambios en la sociedad [1]. Vivimos, como ha señalado Castells, uno de esos raros intervalos de la historia «caracterizado por la transformación de nuestra cultura material», en este caso, por obra de un nuevo paradigma tecnológico organizado en torno a las TIC [2] que ha interaccionado, además, con otro factor insustituible en la dinámica de cambio social, político y económico, como ha sido la globalización económica [3]. La suma de evoluciones tecnológicas en el campo de la microelectrónica, la informática y las telecomunicaciones, entre otras, junto a la aparición del paradigma de innovación tecnológica que ha supuesto una mayor incidencia social, como ha sido Internet, que ha vuelto los mercados financieros transfronterizos, multiplicado las opciones de acceso a información de todo tipo, permitido transacciones económicas o personales transfronterizas y en tiempo real, creado nuevas formas de comunicación personal y modificado los contextos y sentido de cualquier forma de comunicación [4]; ha provocado múltiples cambios en lo económico, cultural y social [5].

A los efectos de lo que ahora nos interesa, las TIC, en general, e Internet como red global en particular, han supuesto la creación de un lugar

---

[1] Sobre la utilización del término «sociedad de la información», véase BRIGGS, A., y BURKE, P., *De Gutenberg a Internet. Una historia social de los medios de comunicación* (traducido por Marco Aurelio GALMARINI), Madrid, Taurus, 2002, pp. 32 y ss. El término «sociedad digital» fue acuñado por NEGROPONTE, N., *El mundo digital* (traducido por Marisa Abdala), Barcelona, Ediciones B, 1995; y el de «sociedad red» por CASTELLS en su trilogía: *La era de la información. Vol. 1. La sociedad red,* Madrid, Alianza Editorial, 2000 (2.ª ed.), pp. 41 y ss.

[2] CASTELLS, M., *La era de la información..., op. cit.,* pp. 59 y ss.

[3] Así, también, MORA MOLINA, J., «Globalización, Derecho y ciencias sociales: hacia una nueva teoría del conocimiento», en *AFD,* t. XVII, 2000, p. 105.

[4] MORA MOLINA, J., «Globalización, Derecho y ciencias sociales...», *op. cit.,* p. 105.

[5] Véase en general, la obra de CASTELLS, M., *La era de la información..., op. cit.,* vols. 1, 2 y 3.

de comunicación social transnacional, universal y en permanente evolución tecnológica que se ha venido en denominar ciberespacio [6], y respecto al cual nos interesa plantearnos si el mismo puede definirse como un nuevo ámbito de oportunidad delictiva, un contexto de riesgo criminal distinto al espacio nacional físico tradicional o, por el contrario, idéntico a éste en sus caracteres esenciales. Siguiendo la acertada metáfora de Grabosky, la cuestión es si el cibercrimen es *«old wine in new bottles»* [7], o por el contrario, constituye un tipo de delincuencia esencialmente nueva y respecto de la cual no son válidas las teorías criminológicas aplicables al delito llevado a cabo en el espacio físico-nacional. Al fin y al cabo, y como he señalado en otro lugar [8], son varios los sentidos que pueden atribuirse a la idea de que el cibercrimen es «vino viejo en botellas nuevas». Con ello se puede estar haciendo referencia, en primer lugar, y desde una visión más extrema, a que la ciberdelincuencia es un tipo de delincuencia nueva para la cual no son válidas las teorías tradicionales creadas para explicar el espacio físico. En el polo opuesto, con tal expresión que ha hecho fortuna en la literatura dedicada al estudio del cibercrimen, se puede estar afirmando que el ciberdelito es idéntico estructuralmente al delito cometido en el espacio físico, cambiando únicamente el aspecto del mismo, pero en ningún caso sus caracteres configuradores. Y también cabe una posición intermedia, conforme a la cual la cibercriminalidad comparte con la delincuencia todos los elementos definitorios del concepto de «crimen», pero dándose los mismos de una forma tal en el nuevo ámbito que es el ciberespacio, que puede influir significativamente en la explicación del delito y, por tanto, en su prevención.

Aunque esté anticipándome a las conclusiones, esta última parece ser la idea más acertada de una expresión que sería más precisa si fuera «es vino, pero se bebe de otra forma». Al fin al cabo todo evento social es distinto en

---

[6] En realidad, no son lo mismo Internet, la *www* y el ciberespacio. Este último es el espacio virtual, no físico, determinado por la interconexión de personas a través de redes telemáticas, y dentro de él, uno de sus principales catalizadores es Internet, sistema global de información y comunicación basado en el protocolo TCP que une ordenadores de todo el mundo y permite el acceso a cualquiera de ellos para obtener e intercambiar información de manera sencilla. De Andrés Blasco, J., «¿Qué es Internet», en García Mexía, P. (dir.), *Principios de Derecho de Internet,* Valencia, Tirant lo Blanch, 2002, p. 29. Dentro de Internet son muchos los servicios existentes, uno de los cuales es la *World Wide Web,* como conjunto de protocolos que permite acceder a información de forma remota, y que ha llegado a solapar como concepto al propio término de Internet, pese a que ésta incluye otros servicios aparte de la *www* como el correo electrónico, los canales IRC de conversación en línea, además de que son otras muchas las TIC que están integrándose hoy en Internet, como la telefonía electrónica o la televisión digital. En este libro se utilizan en muchos casos los términos ciberespacio, Internet y la Red, como equivalentes, cuando no es necesaria ninguna precisión de diferenciación entre estos conceptos.

[7] Grabosky, P., «Virtual Criminality: Old Wine in New Bottles?», en *SLS,* núm. 10, 2001, pp. 243 y ss., también Brenner, S. W., «Cybercrime Metrics...», *op. cit.,* pp. 1 y ss.

[8] Miró Llinares, F., «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen», en *RECPC,* 13-07 (2011).

Internet, un nuevo ámbito estructuralmente distinto al físico en el que sucedían las cosas hasta el momento. Y el crimen es un evento social que cambia en Internet. De hecho, la criminología no ha negado nunca que el ámbito incide en el delito. Si, como señalaran hace ya más de tres décadas Cohen y Felson [9], el crimen se produce cuando se unen en el espacio y el tiempo un objetivo adecuado, un delincuente motivado y la ausencia de un guardián capaz de darle protección al primero, es evidente entonces que los especiales caracteres del ciberespacio en los que se ven modificados los parámetros espacio-temporales, pueden incidir en una modificación de los condicionantes del delito. Esto ya tendría una gran relevancia, pues el descubrimiento de tales modificaciones será esencial para la comprensión, primero, del alcance real de esta criminalidad, y de las razones de su aparición y desarrollo, y para su prevención, después, por medio de la modificación de las reglas de la prevención situacional. Y eso, a la vez, no es incompatible con la afirmación de que el cibercrimen deba seguir siendo considerado un delito y explicado desde las teorías criminológicas.

2. ARQUITECTURA DEL CIBERESPACIO

Antes de entrar en consideraciones sobre los caracteres del cibercrimen derivados de los propios del nuevo ámbito de intercomunicación social en el que se comete, resulta esencial concretar estos últimos, es decir, analizar en qué cambia el ciberespacio con respecto al espacio físico, cuáles son las singularidades de ese nuevo espacio que conllevan que cualquier evento social en él se caracterice de forma distinta a como lo es en el otro espacio de comunicación social. Obviamente no se pretende realizar una definición antropológico-social del ciberespacio, pero sí identificar los caracteres de su arquitectura, de su construcción como ámbito relacional, especialmente en lo que se diferencian de los del ámbito espacial o físico en el que tradicionalmente se han cometido las infracciones.

Para ello hay que partir del propio concepto ciberespacio que, como ha señalado Graham, muestra la tendencia de las ciencias sociales para acudir a la geografía para utilizar metáforas sobre los nuevos ámbitos de comunicación surgidos en la sociedad de la información [10]. En realidad metáforas geográficas o sociales, como la del propio ciberespacio, sitio web, comunidad virtual o autopista de la información, ayudan a visualizar, en términos de funcionalidad social, lo que, en última instancia, no son más que circuitos de señales electrónicas que contienen información codificada. Tales palabras se convierten así en herramientas conceptuales utilizadas para entender

[9] COHEN, L., y FELSON, M., «Social change and crime rate trends: A routine activity approach», en *ASR,* vol. 44, núm. 4, 1979, pp. 588-608.

[10] GRAHAM, S., «The end of geography or the explosion of place? Conceptualizing space, place and information technology», en *PHG,* vol. 22, núm. 2, 1998, pp. 165 y ss.

el sentido y alcance funcional de una nueva tecnología; para traducir estas nuevas técnicas en términos de cuál es el uso social que se puede hacer de ellas, cuáles son los efectos de su desarrollo, y cuáles sus diferencias con las tecnologías anteriores. En el caso del término ciberespacio, el mismo sirve para poner de manifiesto que se trata de un lugar de comunicación que no tiene una naturaleza física primaria, sino esencialmente relacional.

Trataré, a continuación, de aclarar qué implica esto y cómo se configura ese nuevo ámbito con respecto a como lo hace el físico. Después de definir los caracteres intrínsecos y esenciales del ciberespacio me ocuparé de aquellos otros que, aunque podrían ser otros, definen hoy al ámbito de comunicación objeto de estudio.

2.1. Tiempo y espacio en el ciberespacio

Dice Gotved que toda sociedad se caracteriza por su posición en el tiempo y el espacio, de modo que los nuevos significados asignados a tales ideas son fundamentales para los cambios culturales [11]. Es lo que ocurre en la sociedad actual con el ciberespacio como ámbito social que tiene como caracteres intrínsecos una concreta configuración de las coordenadas espacio/tiempo diferente a la que tiene en el que podríamos denominar espacio real o físico.

Decimos que el ciberespacio es un espacio porque en él las personas se encuentran y relacionan, pero mientras que el espacio físico existe antes y seguirá existiendo después de que termine la relación (al menos mientras exista un observador), el ciberespacio agota su existencia en cuanto el mismo sirva para la comunicación entre los sujetos, dado que sin interacción no hay red [12]. Así, frente al espacio geotécnico como la tierra, que existe independientemente de los actos de la gente que tengan lugar en ella, y que sólo puede ser ocupado a la vez por un mismo ente, el ciberespacio existe en cuanto en él se interacciona y es posible que sea ocupado por muchos entes al mismo tiempo [13]. De hecho, se suele utilizar como sinónimo de ciberespacio el concepto de «espacio virtual», como antitético al espacio «real». La simultaneidad, la unicidad de momentos, puede llevar a la impresión de que el ciberespacio es la ausencia de espacio, quizás fruto del equívoco de asimilar la idea de espacio a la de distancia [14]. Evidentemente, el ciberespacio es real en el sentido de que existe, pero se trata de una «especie nueva» de espacio,

---

[11] Gotved, S., «Time and space in cyber social reality», en *NMS*, 2006, p. 467.

[12] Aguirre Romero, J. M.ª, «Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo xxi», en *EREL*, núm. 27, Universidad Complutense de Madrid, julio/octubre de 2004, en Internet en *http://www.ucm.es/info/especulo/numero27/cibercom.html* (última visita el 1 de octubre de 2010).

[13] Graham, P. W., «Space and Cyberspace: on the enclosure of consciousness», en Armitage, J., y Roberts, J. (eds.), *Living with cyberspace: technology & society in the 21st century,* London, Continuum International Publishing Group, 2002, pp. 156-164.

[14] Gutiérrez Puebla, J., «Redes, espacio y tiempo», en *AGUC,* núm. 18, 1998, p. 81.

invisible a nuestros directos sentidos y en el que las coordenadas espacio-tiempo adquieren otro significado y ven redefinidos su alcance y límites.

En realidad, la idea de la «virtualidad» del ciberespacio deriva de la tradicional identificación entre espacio (físico) y distancia. En el ámbito de comunicación configurado por Internet no hay distancias, pero sí espacio. Así, el ciberespacio supone la contracción total del espacio (de las distancias) y, a la vez, la dilatación de las posibilidades de encuentro y comunicación entre personas. Internet ha contraído el mundo acercando a un mismo lugar interactivo a personas que pueden estar en coordenadas espaciales separadas por miles de kilómetros [15]. El espacio se contrae, la intercomunicación se expande [16]. Y ello influye evidentemente en la configuración social. Como ha señalado Gutiérrez Puebla, mientras que el espacio de las sociedades tradicionales estaba dominado por la contigüidad, por las relaciones de proximidad a nivel familiar, vecinal, local y supralocal, en la sociedad actual las relaciones se canalizan a través de redes, lo cual favorece un desplazamiento de la información y de la comunicación mucho mayor [17]. Es a través de redes, pues, como se crean las nuevas comunidades virtuales entre personas que pueden estar separadas por el espacio físico, pero a las que les unen los intereses e inquietudes y que, por ello, se configuran como comunidades con una lógica distinta a las de las tradicionales comunidades físicas.

El ciberespacio, en todo caso, convive con el espacio físico o terrestre, y también tiene, en algunos aspectos, una relación directa con él que no debe ser obviada: las redes telemáticas que conforman el ciberespacio vienen a unir, de forma virtual pero también física, terminales o sistemas informáticos que están ubicados en espacios terrestres concretos en países nacionales determinados con contextos sociales de facilitación del acceso a Internet específicos [18], así como con regímenes jurídicos distintos que pueden afectar, por ejemplo, a las obligaciones de los prestadores de servicios respecto a la identificación de los titulares de las direcciones IP. Además también va cambiando la relación entre el espacio físico y el virtual: hace unas décadas era necesario un lugar físico fijo para entrar en el ciberespacio, mientras que hoy, gracias a las redes *wifi* y, en particular, a la nueva tecnología de la telefonía móvil, es posible conectarse desde prácticamente cualquier lugar físico del planeta y estando en movimiento [19].

---

[15] Gutiérrez Puebla, J., «Redes, espacio...», *op. cit.,* p. 65.

[16] Así, Green, N., «On the Move: technology, mobility, and the mediation of social time and space», en *IS*, vol. 18, núm. 4, 2002, p. 285, quien señala que hay una compresión espacio-temporal en el sentido de la reducción del tiempo necesario para cubrir una distancia, pero un estiramiento en el sentido de que aumenta el contacto entre las sociedades.

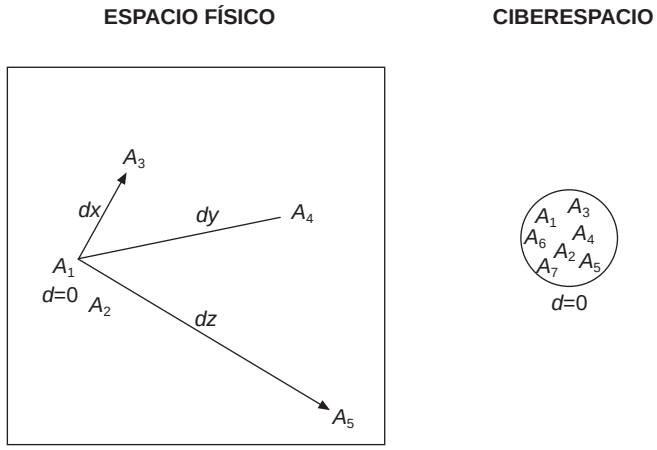
[17] Gutiérrez Puebla, J., «Redes, espacio...», *op. cit.,* p. 70.

[18] Así señala Kitchin, R. M., «Towards geographies of cyberspace», en *PHG,* vol. 22, núm. 3, 1998, p. 387, que las facilidades para la conexión al ciberespacio no están distribuidas de forma equitativa en el espacio físico y eso impide hablar de identidad de ciberespacio.

[19] Fielding, A., «Cyber Space, Meat Space and a Sense of Place: Lessons from the interplay of the online and offline worlds», pp. 3 y ss.

Pero ese espacio geográfico en el que se encuentran las terminales es irrelevante para la comunicación entre personas en el ciberespacio. Lo realmente importante es que mientras que para la comunicación en el espacio físico era necesaria una cercanía (en términos de distancia) entre emisor y receptor, la misma ya no es necesaria en el ciberespacio: ahora pueden hacerlo al mismo tiempo (o en tiempos separados, sobre lo que trataré después) y en el mismo (ciber)espacio, pero en distintos espacios geográficos (o a distancia).

Gráfico 3.1. Contracción de la distancia en el ciberespacio y expansión de la capacidad comunicativa: A1 necesita d = 0 para comunicarse con A2, A3, A4, etc. Elaboración propia.



La distancia deja de ser un obstáculo, por tanto, para la comunicación en el ciberespacio, de modo que esté donde esté el sujeto al que va dirigida la acción en Internet, el coste de realización es exactamente el mismo, dado que la distancia física no tiene relevancia en el ciberespacio.

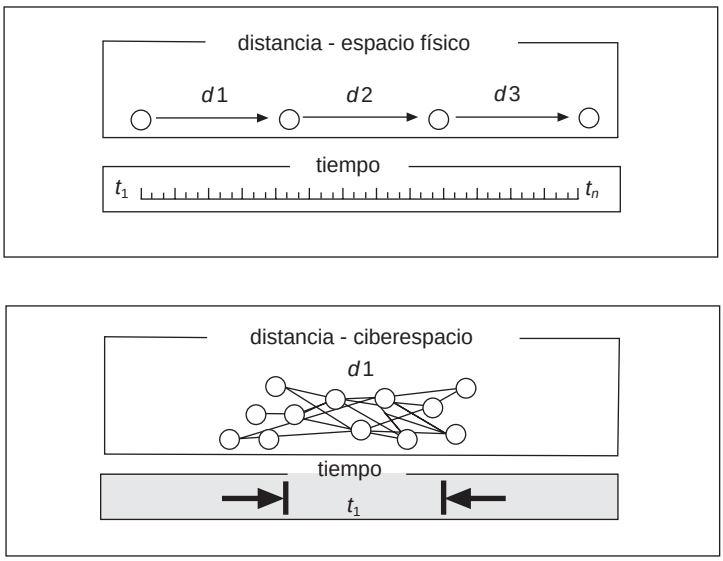
Al afirmar que el ciberespacio es un «nuevo espacio», estamos anticipando la respuesta sobre la incidencia del ámbito en la otra dimensión, el tiempo. Internet también cambia el tiempo, su percepción social, así como la forma en la que el mismo tiempo se organiza [20]. La contracción del espacio conlleva, en primer lugar, un aumento de la importancia del tiempo, y en segundo lugar, una compresión del tiempo necesario para la comunicación social [21]. El tiempo necesario para la comunicación entre dos personas separadas por un espacio físico también se contrae ante la ausencia de la distancia y la aparición de un espacio virtual de intercomunicación inmediata. Así,

[20] LEE, H., y LIEBENAU, J., «Time and the Internet at the turn of the millenium», en *TSoc.,* vol. 9, núm. 1, 2000, p. 44.

[21] KITCHIN, R. M., «Towards geographies of...», *op. cit.,* p. 386.

lo que en el espacio físico nacional exige mucho tiempo, puede ser llevado a cabo de forma inmediata en el ciberespacio, con la consiguiente «aceleración de la vivencia subjetiva del tiempo»[22], dado que en Internet los eventos suceden mucho más rápidamente que en la vida no virtual[23]. En todo caso, con el tiempo ocurre algo similar a lo que sucede con el espacio: la contracción en el sentido de reducción del tiempo necesario para llevar a cabo una determinada tarea, conlleva un estiramiento de las relaciones sociales, en cuanto que, como señaló Giddens, el avance de las tecnologías de la comunicación ha permitido salvar las «distancias temporales» entre las sociedades y acercarlas hasta convertir el contacto entre ellas en algo instantáneo[24]. Como se ve en el gráfico 3.2, al no requerirse en el ciberespacio recorrer una distancia para la comunicación, las posibilidades de contacto con múltiples sujetos aumentan y se reduce el tiempo necesario para ello. En última instancia puede decirse que Internet reduce los costes temporales exigidos en el espacio físico para cualquier tipo de comunicación entre personas.

Gráfico 3.2. Contracción del tiempo. El tiempo necesario para la comunicación disminuye al no existir distancias en el ciberespacio. Elaboración propia.



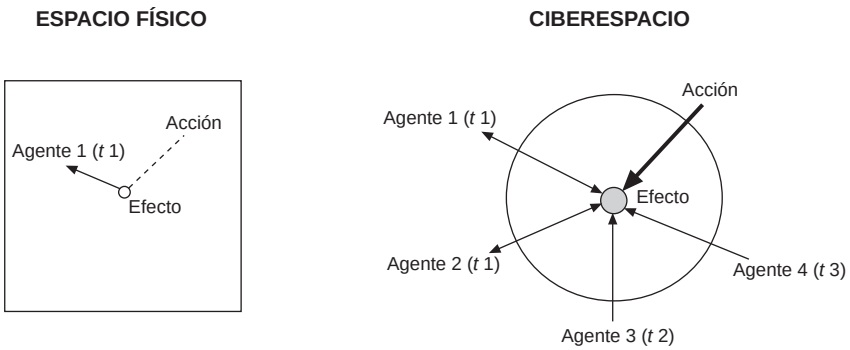
[22] GREEN, N., «On the Move...», *op. cit.,* p. 284.

[23] Me parece muy gráfico el ejemplo de WELLMAN, B., «Computer Networks As Social Networks», en *Science*, vol. 293, 14 de septiembre de 2001, p. 2034, cuando señala que *«an Internet year is like a dog year, changing approximately seven times faster than normal human time».*

[24] FUCHS, C., «Transnational Space and the "Network Society"», en *Paper Presented at the Association of Internet Researchers (AoIR) Conference: Internet Research 7.0, Brisbane, September 27-30, 2006,* en Internet en *http://aoir.org/files/fuchs_516.pdf*, p. 9 (última visita el 2 de diciembre de 2010).

Y no es el único cambio que podríamos asignar al «tiempo» en el ciberespacio. La configuración comunicativa de este nuevo ámbito de intercomunicación social puede hacer que acciones cuyos efectos se produjeran de forma instantánea pero caduca, tengan un funcionamiento temporal distinto: que los efectos se produzcan instantáneamente pero sean perceptibles de forma perenne. Así, las conductas ejecutadas a través del ciberespacio, especialmente aquellas consistentes en la publicitación de contenidos, pueden quedar fijadas durante un tiempo indeterminado y seguir desplegando efectos aunque su ejecución sólo haya durado un instante. La razón es la estructura comunicativa de Internet, de constituir un espacio vasto que puede expandirse y contraerse, en el que las cosas pueden estar en un sitio y luego en otro, y en el que la comunicación entre personas en el ciberespacio puede producirse en tiempos distintos, en el sentido de que el emisor puede enviar un mensaje comunicativo en un momento temporal determinado y no ser recibido hasta mucho después por el receptor. Así, y como se trata de reflejar en el gráfico 3.3, mientras que en el espacio físico las acciones producen efectos en un determinado momento, en el ciberespacio el efecto puede quedar fijado durante un tiempo indeterminado y afectar a un agente determinado en el momento en que se realiza, pero también en un momento posterior cuando otro agente interaccione con dicho efecto.

Gráfico 3.3. Fijación de los efectos en el ciberespacio. La acción se ejecuta en un momento *x*, pero A3 y A4 interaccionan con ella en momentos posteriores. Elaboración propia.



Es cierto que en el espacio físico esto también es posible. Pero qué duda cabe de que el ciberespacio modifica la capacidad de control por parte del agente del hecho en relación con el elemento temporal. Y lo mismo sucede con el elemento espacial: en el espacio físico el agente tenía, cuanto menos generalmente, un mayor dominio sobre las coordenadas espacio-temporales del hecho, en el sentido de que podía definir el ámbito geográfico en el que

iba a comenzar a producir efectos (aunque después éstos pudieran escapar a lo deseado), así como el momento o instante temporal en el que iban a comenzar a hacerlo. También era posible, en muchos casos, definir concretamente el espacio físico en el que el hecho del agente iba a terminar de producir efectos, al menos los más directamente derivados del mismo; y, de igual modo, el tiempo que iba a durar el hecho. En el ciberespacio es más difícil concretar el ámbito geográfico-espacial en el que el hecho va a desarrollarse: algunas acciones se pueden dirigir concretamente contra un usuario, un colectivo o una institución determinada, pero incluso en esos casos la propagación de los efectos es más sencilla al no necesitar «recorrer distancias». Otras acciones, además, son incontrolables en cuanto a su dimensión espacial: una vez se difunde un contenido en Internet o se propaga un *malware* a un colectivo indeterminado, es casi imposible saber quién, desde cualquier lado del mundo, se verá afectado por los mismos. Y si lo observamos desde la perspectiva contraria, la complejidad para la concreción de la causa a la que se puede atribuir el resultado o efecto es de similar entidad: mientras que la concreción del espacio geográfico donde se ha causado un determinado daño nos puede ayudar a identificar al responsable del mismo, en el ciberespacio la identificación geográfica y temporal de un efecto o consecuencia no nos asegura ningún tipo de cercanía espacial o de tiempo con la causa. No es que no haya transferencia, que la habrá, y por tanto huella, que será digital, sino que no habrá transferencia espacial: la seguridad (o alta previsibilidad) de que el criminal deberá estar en un espacio determinado simplemente por el hecho de que el daño se haya producido en un lugar concreto. Y lo mismo ocurrirá con el tiempo: que los efectos de una acción surjan en un determinado momento no asegura, en el ciberespacio, que el hecho se haya iniciado por parte del sujeto en ese instante temporal. Por el contrario, los agentes pasivos pueden convertirse en activos en el ciberespacio: es posible que un agente realice algo y «deje» el ciberespacio, y que sea otro sujeto el que interaccione con lo hecho por el primero posteriormente e independientemente de la voluntad del primero.

Lo relevante, en todo caso, es que en el ciberespacio las coordenadas espacio-temporales se ven significativamente modificadas: por una parte, se comprimen las distancias y el tiempo que cuesta recorrerlas; por otra, y derivado de lo anterior, se expanden las posibilidades comunicativas entre las personas y los efectos de los hechos que apenas se ven limitados espacial o temporalmente. Simbólicamente, acudiendo de nuevo a la geografía para explicar el efecto de todo esto, se podría afirmar que el ciberespacio es un espacio mayor, más amplio, y también más duradero, de percepción de los efectos más dilatada en el tiempo, que el espacio físico. Lo que esto quiere decir es que cualquier agente en el ciberespacio, salvo el impedimento del contacto físico directo, tiene menos restricciones espaciales y temporales para sus actos que en el espacio físico. También, que los efectos de las con-

ductas, las consecuencias plasmadas en unas coordenadas espacio-temporales determinadas, ofrecen menor información en el ciberespacio que las coordenadas espacio-temporales del acto al que se deben atribuir las mismas y, por ello, del agente causante, que en el espacio físico.

Por supuesto todo esto va a influir en la configuración del (ciber)crimen, como evento social que es. Y si la criminología desde siempre ha tratado de explicar este fenómeno, especialmente en los últimos tiempos en los que ya no se focaliza únicamente en el agente del mismo sino que atiende también al entorno en el que actúa, presuponiendo como constantes inmutables una arquitectura del espacio y del tiempo en la sociedad que, en cambio, no sirven como columnas de un nuevo ámbito de intercomunicación social en el que también pueden producirse eventos criminales, es evidente entonces la necesidad de replantear la vigencia de esas teorías para este nuevo tipo de delitos o, cuanto menos, de adaptar sus desarrollos a los nuevos presupuestos que definen el ciberespacio.

Antes de ello, sin embargo, conviene explicar otro tipo de caracteres que configuran también el ciberespacio y, por ello, van a determinar cualquier fenómeno social que tenga lugar en él.

Gráfico 3.4. Caracteres del ciberespacio. Elaboración propia.

2.2. El ciberespacio transnacional, universal, neutro, abierto al cambio, etcétera

La configuración espacio-temporal del ciberespacio es intrínseca al mismo, en cuanto que Internet está definido en sus coordenadas espacio-tempo-

rales de forma distinta al espacio físico. Pero no son éstos, como he desarrollado en otro lugar, los únicos caracteres que configuran este nuevo ámbito de comunicación y relaciones sociales [25]. Junto a tales caracteres intrínsecos hay otros que, siendo extrínsecos, se consideran hoy absolutamente definitorios, si bien podrían ser distintos a los que son. Así, hoy parece intrínseco al ciberespacio su carácter desregulado, pero en algunos países del mundo se está haciendo lo posible porque no sea así. Hoy asumimos, también, un ciberespacio universal y popularizado, si bien la realidad política de algunos Estados y las enormes desigualdades económicas en todo el mundo impiden poder afirmar que ello es un carácter intrínseco del mismo. Y lo mismo, el que se trata de caracteres extrínsecos, se va a poder afirmar de los que voy a analizar a continuación y de muchos otros que se vienen asociando a este nuevo contexto de relaciones económicas y sociales [26].

Todos estos elementos que vamos a analizar configuran aquello que definimos como ciberespacio. Sin la transnacionalidad del ciberespacio, esto es, con un ciberespacio en el que existieran fronteras y hubiera que pasar de uno a otro; sin su descentralización, sin su carácter universal y abierto o sin el efecto de mutación constante que sobre sus funcionalidades causa el desarrollo tecnológico, Internet no sería lo que es. Y obviamente todos y cada uno de los fenómenos que se desarrollan en él se ven afectados y configurados no sólo por el cambio espacio-temporal que el ciberespacio supone, sino también por toda una serie de caracteres que, por tanto, nos debieran ayudar a comprender las diferencias del fenómeno criminal y de su prevención cuando se comete en el ciberespacio.

A ello me voy a dedicar a continuación, de forma breve, centrándome, eso sí, en los caracteres que van a tener una mayor influencia en el concreto fenómeno que nos interesa, la cibercriminalidad.

2.2.1. *El ciberespacio transnacional*

Uno de los caracteres básicos que acertadamente se suelen atribuir a Internet es el hecho de que la misma esté deslocalizada. El ciberespacio, podríamos decir, no está situado en un sitio en concreto, sino que, en sentido funcional, está en todos a la vez pero, en sentido físico, en ninguno. En realidad éste no es ningún carácter extrínseco al fenómeno, sino algo intrínseco al ciberespacio: es su propia esencia como fenómeno (no) espacial, y que hemos analizado anteriormente. No puede negarse, sin embargo, que tal carácter no tendría la importancia que tiene si no viniera unido a otro elemento que podríamos denominar accesorio, en cuanto que podría imaginarse un

[25] MIRÓ LLINARES, F., «La oportunidad criminal...», *op. cit.,* pp. 10 y ss.

[26] Véanse los citados por CAPELLER, W., «Not such a neat net: some comments on virtual criminality», en *SLS,* núm. 10, 2001, p. 233.

ciberespacio configurado sin él, pero esencial y definitorio de lo que, para todo el mundo, constituye en la actualidad ese nuevo ámbito social que es Internet. Me refiero, obviamente a la transnacionalidad del ciberespacio, a la inexistencia de fronteras o distancias [27], ni aparentes ni reales, en un ámbito digital de interacción social que no pertenece a ningún Estado nacional concreto, pero que, a la vez, permite el acceso a sus servicios desde cualquiera de ellos.

La transnacionalidad del ciberespacio se traduce, a los efectos que nos interesan, en la total ausencia, para la comunicación e interacción entre individuos, de barreras que no sean impuestas o configuradas por el propio sujeto. Desde cualquier Estado nacional es posible acceder a cualquier Estado nacional, y un contenido vertido en una página web localizada en un servidor de un Estado concreto y colgada por un sujeto de un determinado Estado, puede ser vista por cientos de personas en cientos de sitios distintos en el mundo. Desde una perspectiva sociológica es obvio que la transnacionalidad del ciberespacio lo configura como un ámbito de intercomunicación social nuevo que contrasta con las posibilidades de comunicación extranacional en el espacio físico. En el ciberespacio la trasnacionalidad se mezcla con la localidad, en el sentido de que ya no es necesario, para tener un contacto o comunicación con un Estado, región o localidad, distinta a la propia, realizar un traslado físico, sino que puede accederse a lo trasnacional desde lo local, incluso desde lo personal o íntimo que, por tanto, puede quedar ya, tan sólo dependiendo de la decisión del propio individuo, al acceso de muchas más personas de lo que era posible anteriormente. Aumentan por tanto, en el ciberespacio, las facilidades para la multicomunicación social (transnacional), y disminuyen, así, los impedimentos para la comunicación entre personas, cuanto menos el que la misma se limitaba a las personas que se hallasen físicamente próximas. Lo mismo ocurre con los bienes: ya no es necesario, en el ciberespacio, un contacto físico entre agente y bien para que exista el acceso, y desde luego no es necesario que se esté en el momento del intercambio o de la adquisición (lícita o ilícita) en el mismo lugar físico, sino que es posible que un sujeto desde un Estado nacional acceda a otro y acceda a un bien, digitalizado, pero con valor económico. En otras palabras, la exigencia de distancia física como obstáculo natural para la comunicación entre personas (entre las que está la delictiva) desaparece en el ciberespacio, en el que sólo funcionan los obstáculos artificiales que deberán ser puestos por el propio titular de los bienes.

[27] PÉREZ LUÑO, A. E., «Impactos sociales y jurídicos de Internet», en *ART,* núm. 1, 1998, pp. 33 y ss.

2.2.2. *La neutralidad en la Red*

Otro carácter extrínseco de la máxima importancia es la neutralidad en el ciberespacio, que implica la libertad del usuario a la hora de transitar por el mismo sin fronteras pero también sin censuras de acceso por parte de nadie. El carácter neutro de Internet deriva de la imposibilidad de bloquear conexiones entre nodos en la Red, lo que permite que una vez tengan acceso a Internet, ni siquiera el propio operador pueda impedir el acceso a una web o a un servicio elegido por el usuario [28]. Aunque se trata de un carácter extrínseco, dado que podrían establecerse restricciones por medio de una reconfiguración de Internet que permitiera, por ejemplo, bloquear la capacidad de un usuario para emitir información o para acceder a un sitio web, es consustancial al ciberespacio que conocemos su carácter neutro, dado que no hay más restricciones que las impuestas por el propio usuario. Es obvio, precisamente por ello, que el control de informaciones y contenidos, por parte de quien quiera llevarlo a cabo, es complejo en el ciberespacio, aunque es discutible que lo sea más que en el espacio físico. La dificultad de controlar las comunicaciones entre usuarios particulares en el ámbito real puede ser incluso mayor al no quedar, como en el ciberespacio, constancia o huella de lo comunicado. Lo que sí es mayor, sin lugar a dudas, es la capacidad de la información para difundirse en un espacio universal y popularizado, y eso es lo que aumenta su importancia, también su valor y, en algunos casos, su capacidad para causar daño a bienes esenciales no puede negarse, lo cual puede servir de razón o de excusa para Estados o algunas organizaciones para tratar de crear un ciberespacio distinto, con nodos conectados que en su parte central dependan de alguien y que, por ello, le permitan impedir el acceso a determinadas webs o la navegación a usuarios específicos.

2.2.3. *El ciberespacio no centralizado (más bien distribuido)*

En relación con la transnacionalidad y el carácter neutro de la Red también podríamos citar como carácter extrínseco pero configurador del ciberespacio, su descentralización o, quizá mejor, su no centralización y concretamente su carácter distribuido, dado que en la estructuración de Internet no existen nodos centrales pero tampoco nodos que actúen como centros locales, sino que se trata, como ha señalado gráficamente Alcántara, de una malla «en la que ningún nodo tiene el poder de aislar a otro, en la que ningún nodo tiene el poder de decidir qué conecta con qué», y en la que, por tanto, la caída de un nodo no imposibilita que la información siga fluyendo [29].

---

[28] Alcántara, J., *La neutralidad en la Red, y por qué es una mala idea acabar con ella*, Madrid, Biblioteca de Las Indias, 2011.

[29] Alcántara, J., *La neutralidad en la Red..., op. cit.,* pp. 10 y ss. Advierte con razón que no sólo el diseño de Internet no lo hace centralizado, sino que tampoco es correcto hablar de que es

Por otra parte, y relacionado con ello, no existe en Internet autoridad centralizada alguna, ni siquiera órganos o instituciones de control de la información circulante que puedan establecer algún tipo de censura sistemática o control de los contenidos [30]. Internet no está sometida a las leyes nacionales de un único país, ni a unas normas propias aceptadas por todos los que la conforman, y esto conlleva que los controles gubernamentales resulten poco efectivos, al existir variadas formas de evitar los que van imponiendo los Estados nacionales. Es obvio, sin embargo, que la existencia de este espacio transnacional, neutro y distribuido, con las consecuencias que conlleva, produce una tensión, en este caso en el plano jurídico, con la casi contradictoria existencia de Estados nacionales con legislaciones distintas reguladoras de éste u otro fenómeno. Si bien no existe un control global de la Red, los gobiernos nacionales han comenzado a tratar de regular Internet ante el potencial riesgo que supone y su popularización en todas las escalas sociales. Estos controles van desde el propio acceso a Internet hasta el control de los contenidos, con normas dirigidas a los servidores que buscan responsabilizarles de lo publicado en este gran medio de comunicación, y sobre las que trataremos más adelante. En todo caso, la adopción de decisiones nacionales apenas soluciona el problema, como es obvio. El potencial riesgo que supone la transnacionalidad del cibercrimen y que le convierte en uno de los mayores desafíos planteados en la actualidad, deriva de lo complejo que resulta responder localmente a riesgos globales. Y mientras que el mundo parece encogerse y el crimen cometido desde «el edificio de al lado» se perpetra hoy desde otro continente, los Estados, sus normas y las instituciones que las aplican aún se diferencian entre sí y no logran conjugar lo que no puede más que considerarse un «problema común» [31].

Desde la perspectiva criminológica que ahora nos interesa podríamos afirmar que esto es conocido por los cibercriminales, en el sentido de que son conscientes de que pese a realizar conductas que en el Estado en el que producen efectos pueden resultar delictivas, el hecho de hacerlo desde un Estado distinto complicará enormemente la persecución penal por las mismas. Además, y como señalan acertadamente Goodman y Brenner, esta transnacionalidad y carácter distribuido del ciberespacio unidas a la existencia de múltiples normas distintas en diferentes Estados, y a la característica que después analizaremos relativa a la permanente revolución tecnológica que se produce en este nuevo ámbito social conlleva que, al contrario de lo que suele suceder en el espacio físico, no sea nada sencillo determinar para algunas conductas si las mismas son socialmente adecuadas o incluso

---

descentralizado puesto que ello podría venir a significar que hay nodos locales que se unen en red entre sí; por ello propone utilizar el término «distribuido», que sirve mejor para expresar la naturaleza con la que se construye Internet.

[30] Romeo Casabona, C. M., «De los delitos informáticos...», *op. cit.,* p. 3.

[31] Grabosky, P., «Virtual Criminality: Old Wine in New Bottles?», *op. cit.*, p. 247.

legales o no lo son [32]. El ciberespacio difumina la apariencia de legalidad de las conductas.

2.2.4. *La universalidad y popularización del ciberespacio*

El segundo carácter a destacar del ciberespacio como ámbito de riesgo consiste en su carácter universal, y no en este caso en el sentido de transnacional, sino en el de global, colectivo o popular. Al fin y al cabo, son las gigantescas dimensiones de ese nuevo espacio de comunicación social las que le otorgan una dimensión de riesgo que, en el caso de tener un ámbito más reducido, no tendría.

En el mundo podemos hablar de aproximadamente mil millones de usuarios y por tanto, de millones de objetivos sobre los que pueden actuar los criminales. Y es que si bien hubo un momento en que los sistemas informáticos eran únicamente utilizados por empresas o instituciones públicas y el acceso a los mismos era muy limitado, en las últimas décadas se ha producido una popularización de la informática, un aumento de las facilidades para adquirir o acceder a terminales y, muy especialmente, la interconexión entre todas ellas en un espacio de comunicación global que también se ha generalizado [33]. Además, y pese a que se creyó durante los primeros años que Internet sería de uso esencial para empresas e instituciones, la evolución de las tecnologías para el acceso a la Red ha hecho que hoy en día sean usuarios particulares los que principalmente usen Internet como vehículo de comunicación personal. Y aunque el perfil de usuario más general sigue siendo el de adulto de veinte a cuarenta años y con fines profesionales, el auge de las redes sociales y la mejora de la educación en el uso de las TIC desde la infancia ha llevado a que todos, los menores desde los nueve años, hasta los mayores de sesenta y cinco años, sean usuarios de una red que, también en ese sentido, es global.

2.2.5. *El ciberespacio anonimizado*

La universalización de Internet, su popularización como espacio de intercomunicación personal, también tiene que ver, además de con su bajo coste, con el anonimato que confiere [34]. Pese a que desde algunos sectores se está intentando construir algún tipo de sistema que permita la identificación de los usuarios en la Red, parece, al menos de momento, difícil de imaginar un ciberespacio en el que todos o la mayoría de los que intervienen en él

---

[32] GOODMAN, M. D., y BRENNER, S. W., «The emerging consensus on criminal conduct in cyberspace», en *IJLIT*, vol. 10, núm. 2, Oxford University Press, 2002, p. 7.

[33] CLOUGH, J., *Principles of Cybercrime..., op. cit.,* p. 6.

[34] LÓPEZ ORTEGA, J. J., «Libertad de expresión..., *op. cit.,* p. 119.

estén identificados. Tal y como lo conocemos en estos momentos, el ciberespacio es un ámbito que favorece el anonimato del sujeto que interviene en él, por lo menos en comparación con el otro ámbito de comunicación social, el físico. Así, aunque no parezca tan compleja actualmente la determinación del sistema informático que navega por el ciberespacio, sí lo es por el contrario la concreción del sujeto que ha utilizado el mismo para realizar la infracción, especialmente cuando existen múltiples cibercafés desde los que comunicarse en el ciberespacio, redes *wifi* que permiten acceder desde sitios abiertos, etc. A ello hay que sumar los proveedores de servicios gratuitos que no exigen la identificación de los usuarios [35], los múltiples sistemas que permiten enviar correos electrónicos de forma anónima [36] y, ya más en el ámbito del evento criminal, las posibilidades actuales de infectar un determinado sistema informático para convertirlo en un robot (*bot* o *zombie*) y utilizarlo para realizar la actividad criminal logrando que ni siquiera sea posible la identificación de la IP desde la que, en realidad, se ha generado el ataque, así como otros factores relevantes, como la transnacionalidad y la diversidad de prestadores de servicios que operan en Estados con regímenes jurídicos distintos, que no siempre obligan a la identificación de las terminales en red.

Aunque se diga, pues, por parte de algún autor, que el anonimato no es ya una característica de Internet al ser cada vez más sencilla la identificación de las direcciones IP [37], lo cierto es que sigue siendo en la actualidad más compleja, pese a los rastros digitales del delito, la identificación de los autores de estas conductas que la de otros sujetos que cometen similares infracciones pero en el mundo real [38]. Y todas las teorías criminológicas aseveran, como luego se argumentará, que la percepción de que la actuación se realiza en el anonimato conlleva un aumento de la sensación de impunidad y ésta, a su vez, un incremento del riesgo de que el agente acabe por ejecutar el delito.

2.2.6. *El ciberespacio, sujeto a revolución permanente y abierto al cambio*

El tercer carácter que convierte a las TIC en general, y al ciberespacio en particular, en un ámbito de riesgo penal, es que la sujeción a una evolución tecnológica permanente. Las TIC se caracterizan por sufrir modificaciones importantes de forma casi constante, de forma tal que los modos de comunicación social, de intercambio económico, de difusión de contenidos, o

---

[35] *Ibid.*

[36] Véanse los detallados por Pittaro, M. L., «Cyber stalking...», *op. cit.,* p. 1815.

[37] Wall, D., «Cybercrime and the culture of fear: Social Science fiction(s) and the production of knowledge about cybercrime», en *ICS*, vol. 11, núm. 6, 2008, pp. 874 y ss.

[38] Zheng, R.; Qin, Y.; Huang, Z., y Chen, H., «Authorship Analysis in Cybercrime Investigation», en VVAA, *Lecture Notes in Computer Science,* Berlin-Heidelberg, Springer Verlag, 2003, p. 59. También, De la Mata Barranco, N. J., «Ilícitos vinculados al ámbito informático: la respuesta penal», en De la Cuesta Arzamendi, J. L. (dir.), *Derecho penal informático, op. cit.,* p. 19, nota 10.

cualesquiera otros que se utilizan en un determinado momento, pueden ser sustituidos en muy poco tiempo por evoluciones que pueden ir desde una pequeña modificación hasta una auténtica revolución del sistema.

Así, la evolución de Internet parece imparable, tanto en la aparición de nuevos servicios, como en la mejora y modificación de las formas de acceso. En cuanto a lo primero, junto a los ya clásicos servicios de uso de la propia web, del correo electrónico, de los canales IRC o de la mensajería instantánea, aparecen ahora nuevas formas de comunicación relacionadas con el uso de la telefonía digital, las consolas de videojuegos y los sistemas de juego *online* que cada vez ocupan un espectro de mercado más amplio, o la televisión digital.

La importancia que esto tiene es más que evidente: por una parte, las barreras de protección, del tipo que sean, para los intereses personales y sociales que parecen en un determinado momento eficaces, pueden dejar de serlo en muy poco tiempo, y bienes que parecen intocables frente a las TIC, pueden pasar a ser susceptibles de ataque en un instante; por otra, aunque sobre esto se tratará más adelante, el derecho camina totalmente «a remolque» de un contexto social que va cambiando, y las soluciones jurídicas de hoy parecen obsoletas y de ayer cuando entran en vigor. En el espacio físico esto puede suceder, y es perfectamente posible que la aparición de nuevos intereses o de nuevas técnicas e instrumentos convierta en obsoletos los sistemas de control o de tutela de bienes y personas. Pero es obvio que en el ciberespacio, donde la evolución tecnológica se muestra como revolución imparable, la necesaria actualización de los sistemas de protección se hace imprescindible pero compleja.

Por otra parte no hay que despreciar la importancia que tiene que el ciberespacio esté sometido a cambios procedentes de los propios usuarios. Como ha señalado Castells, son los usuarios los que han hecho de Internet lo que es, y son ellos los que constantemente modifican y crean. Y esto se debe, no sólo a que la interacción social con cualquier tecnología incida en su propia estructura, sino a que Internet es una tecnología muy flexible y dúctil que «permite el efecto de retroacción en tiempo real»[39]. Internet está configurando un espacio abierto en el que, al contrario que en otros sistemas, los cambios y modificaciones devienen de la propia intervención del conjunto de usuarios, y no de un ente central[40]. Incluso aquellos que no tienen experiencia en la utilización de los sistemas informáticos, y por supuesto quienes poseen estos conocimientos y tienen inquietudes relacionadas con el mundo virtual, pueden, mediante sus creaciones (véanse los casos de Youtu-

---

[39] CASTELLS, M., «Internet y la sociedad red», en *Conferencia de Presentación del Programa de Doctorado sobre la Sociedad de la Información y el Conocimiento. Universitat Oberta de Catalunya, 7.10.2000.* En Internet, en *http://www.mvdenred.edu.uy/download/destacados/castells.pdf* (última visita el 2 de diciembre de 2010, pp. 1 y ss.).

[40] CAPELLER, W., «Not such a neat net...», *op. cit.,* p. 233.

be o Facebook), o sus usos (los mismos) cambiar la forma de comunicación social en el ciberespacio.

Esta relación directa entre el usuario e Internet, entre su configuración y uso con el agente, es más poderosa que en la realidad del espacio físico debido probablemente a otros de los factores que hemos mencionado antes como la descentralización y la popularización del medio. Lo importante, en todo caso, es el efecto que produce: el usuario se siente parte definitoria del ciberespacio y, por tanto, parte decisoria del mismo, especialmente en su configuración como espacio de libertad. En el espacio físico-geográfico, determinado por unas fronteras y bajo la autoridad de un concreto Estado, el ciudadano tiene fijadas muy estrictamente sus posibilidades democráticas: puede elegir a los representantes políticos o directamente a los gobernantes, puede proponer de forma más o menos directa la aprobación de normas jurídicas, etc.; y también puede configurar los usos sociales, si bien al estar ellos generalmente definidos con la evolución de la sociedad resulta complicado para el ciudadano una influencia directa en ellos. En el ciberespacio es distinto. En cuanto a la participación en procesos formales de decisión democrática, la misma no es posible en el ciberespacio y, sin embargo, su democratización (o la apariencia de ella) es mucho mayor porque, al no existir autoridades y ser universal y popular, es el conjunto de los ciudadanos de Internet el que acaba decidiendo cuáles son las normas sociales básicas de funcionamiento interno. Es evidente que esto no es Derecho en un sentido estricto, pero también que son usos sociales que, en un ámbito como el de Internet donde son los intereses económicos y personales los que mandan, acaban convirtiéndose en reglas de conducta válidas para el funcionamiento de las relaciones. Además, y precisamente por ser un ámbito social nuevo, cambiar y definir las normas (llamémoslas así) éticas del mismo es mucho más sencillo para el usuario pues no hay unas normas sociales impuestas, sino que se van creando con la interacción de todos los nuevos.

Las consecuencias de esto para el entorno social del ciberespacio, a los efectos que nos interesan, son variadas, pero destaca el hecho de que en el mismo no está tan definida la ética o moral imperante como en el espacio físico sujeto a una soberanía nacional, básicamente porque los propios usuarios, con sus conductas, la pueden cambiar. Es posible, y de hecho es lo que está sucediendo con instituciones como la propiedad intelectual, pero no sólo con ella, que las reglas que rijan para el espacio físico se consideren, por parte de los usuarios, no aptas para ese nuevo ámbito que ellos acaban definiendo con su actuar. Esto no significa que el Derecho deje de regir, pero sí que su capacidad de influencia reguladora puede disminuir: a mayor correspondencia entre lo normado y lo aceptado socialmente, mayor cumplimiento de las normas.

Es obvio que todos estos factores, intrínsecos y extrínsecos, de ese nuevo ámbito que es el ciberespacio van a determinar todos los fenómenos que

en él se produzcan, entre ellos el que nos ocupa, el crimen. Es el momento de comprobar cómo, desde el *approach* de las teorías de la oportunidad delictiva.

3. ¿ES EL CIBERESPACIO UN NUEVO ÁMBITO DE RIESGO DELICTIVO? LA OPORTUNIDAD DELICTIVA EN EL CIBERESPACIO

3.1. Introducción: teoría criminológica y cibercrimen

A mi parecer, es algo sorprendente, y para otros también criticable [41], que la criminología apenas haya explotado todavía el estudio de la relación entre la evolución tecnológica y la modificación actual de la delincuencia. En gran parte de los tratados y manuales criminológicos, incluso entre los posteriores al inicio del nuevo siglo, aún se obvia esta cuestión quizá como reflejo de que el cibercrimen aún no se percibe como un fenómeno criminal de gran relevancia. Sea por lo que fuere, las primeras aproximaciones de la criminología al fenómeno del cibercrimen se centraron en la discusión acerca de las motivaciones del *hacker*, quizás por lo atractivo que resultaba ese personaje que cometía delitos y que, sin embargo, parecía tan alejado del prototipo de delincuente, pero también por focalizarse en aquellos momentos la criminología en el sujeto criminal, en la comprensión de los condicionantes de su conducta y sus modalidades, y no tanto en el crimen como evento, completo y complejo [42], que conlleva la constatación de un espacio de oportunidad criminal cuya identificación y análisis puede ser esencial a efectos preventivos.

---

[41] Así MCQUADE III, S. C., «Cybercrime», en TONRY, M. (ed.), *The Oxford Handbook of Crime and public policy,* New York, Oxford University Press, 2009, p. 476, quien señala que es necesario etiquetar y definir el fenómeno criminológico del cibercrimen y de la influencia de la evolución tecnológica en el delito, criticando que se sigan utilizando para estos delitos constructos basados en la categoría de la criminalidad de cuello blanco de Sutherland.

[42] En los últimos años ha sido frecuente la referencia al delito como evento, generalmente para expresar la necesidad de no obviar el factor lugar y el factor víctima en la explicación del delito. Así, es esencial el trabajo de MEIER, R. F.; KENNEDY, L. W., y SACCO, V. F. (eds.), «Crime and the criminal event perspective», en MEIER, R. F.; KENNEDY, L. W., y SACCO, V. F. (eds.): *The Process and structure of Crime. Criminal events and Crime analysis,* en *ACT*, vol. 9, New Jersey, Transaction Publishers, 2001, pp. 3 y ss., en el que se argumenta la utilización de esa expresión como forma de enlace de las teorías del crimen con las teorías de la criminalidad. Al fin y al cabo, y como han señalado Branthingham y Branthingham, la criminología tradicional seguía situando el foco en las motivaciones y las conductas de los criminales hasta el punto de excluir en la mayoría de los casos cualesquiera otras consideraciones, siendo, por tanto, el avance el permitir abrir la criminología al estudio de todos sus componentes, entre otros el rol criminógeno desempeñado por las propias víctimas y objetivos, por guardianes y gestores, etc. BRANTHINGHAM, P. J., y BRANTHINGHAM, P., «The implications of the criminal event model for crime prevention», *ibid.,* pp. 277 y ss. Aunque la idea del crimen como evento se atribuye a autores como Meier, Sacco, Kennedy, Gibbs, Van Brunschot o Ekblom, es evidente que la misma debe mucho a la teoría de las actividades cotidianas de Cohen y Felson, como reconocen entre otros. KENNEDY, L. W., y GIBBS VAN BRUSCHOT, E., «Routines and the criminal event», *ibid.;* así BRANTHINGHAM, P. J., y BRANTHINGHAM, P., «The implications

En esto último es en lo que la criminología parece estar centrando, sin embargo, sus esfuerzos los últimos años. Así, y si bien podemos encontrar en los últimos diez años interesantes estudios de criminología aplicada a la cibercriminalidad en las que se manejan teorías como la del autocontrol [43],

---

of the criminal...», *op. cit.,* p. 278. Merece especial interés, en todo caso, el trabajo de Serrano Maíllo en el que se adopta la perspectiva del crimen como evento si bien, desde la base del filósofo analítico Donald Davidson (DAVIDSON, D., *Essays on actions and events,* Oxford, Clarendon Press, 1980) por medio de lo que él denomina «metateoría» que entiende que no es posible integrar (ni interaccionar entre sí) la motivación y la oportunidad en una teoría, dado que ambos elementos no son más que descripciones de un mismo evento, el evento criminal o, en otras palabras, una misma cosa bajo distintas descripciones. SERRANO MAÍLLO, A., *Oportunidad y delito, op. cit.,* pp. 200 y ss., especialmente 205, también 210 y ss., y 220 y ss., concretamente 224. Sin entrar en una valoración de la metateoría de Serrano Maíllo, lo que sí puede afirmarse es que con la misma no se niega, en ningún momento, que no haya que analizar el evento criminal desde una perspectiva múltiple; más bien se señala que el delito como evento, como todo, dependerá en última instancia «también» de la motivación que, conforme a lo señalado por el autor, no puede separarse de la oportunidad ni ésta de aquél. Es decir, que la oportunidad es también dependiente del agresor motivado lo cual lleva al autor la conclusión de que el centro de la teoría criminológica, en cuanto teoría para la explicación del crimen, está en la motivación y en los condicionantes de la misma. De hecho esto es compatible con el enfoque de la prevención situacional que, en última instancia, también hace depender la prevención de las percepciones (o motivaciones) del propio criminal. Ahora bien, que la oportunidad también sea el evento criminal y que no pueda analizarse sin la motivación no implica que sólo podamos, para prevenir el delito, situar el foco de las políticas en la motivación general, abstracta o concreta, de los ciudadanos. Lo interesante de las teorías del crimen como evento, del enfoque de las actividades cotidianas y de la prevención situacional, es que permiten pensar en elementos externos a la propia motivación del sujeto a la hora de prevenir el crimen, esto es, antes de que el mismo suceda, si bien es obvio, que finalmente, el mismo sólo se podrá explicar en relación con la concreta motivación del concreto delincuente. Así es evidente, como señala en un par de ocasiones Serrano Maíllo citando a Akers y Sellers, que la teoría de las actividades cotidianas es sólo indirectamente una teoría de la comisión de comportamientos criminales siendo principalmente una teoría de la victimización,. De hecho es la visión de la relevancia del «*Suitable Target*» en la ecuación del delito y lo que ello supone de la incidencia de la víctima en su propia victimización lo que acerca esta teoría a la que siempre ha venido siendo considerado una teoría de la victimización criminal como es la de los estilos de vida de HINDELANG, M. J.; GOTTFREDSON, M. R., y GAROFALO, J., *Victims of Personal Crime, op. cit.,* pp. 240 y ss. Es decir, que aquello que aporta la teoría de las actividades cotidianas, y es algo ya de por sí bastante relevante, es el análisis de en qué medida, y desde una perspectiva *ex ante,* independientemente de la motivación del criminal, puede evitarse aquello que, al interaccionar *ex post,* con su motivación, acabará convirtiéndose en un crimen. En otras palabras, es evidente que motivación y oportunidad van unidas en el evento criminal (analizado *ex post),* de forma que sin la motivación no es posible explicar el mismo; pero también lo es que, desde una perspectiva *ex ante,* la única relevante a los efectos de la prevención de la criminalidad, no sólo debe atenderse a la motivación criminal (lo cual no puede dudarse en ningún) sino a otros factores relacionados con ella pero también singulares como la conducta de la víctima, los gestores y guardianes o el espacio. Todo ello, para acabar conformando un crimen, interaccionará con la motivación pero, para no hacerlo, debe analizarse también, si bien, para una visión completa del fenómeno, en relación con ella.

[43] HIGGINS, G. E.; FELL, B. D., y WILSON, A. L., «Low Self-Control and Social Learning in...», *op. cit.,* pp. 339 y ss. Aunque sea para un fenómeno delictivo muy concreto, este trabajo es especialmente interesante porque también utiliza y compara, para el caso de la piratería intelectual la teoría del aprendizaje social. Véase también al respecto, y en sentido prácticamente idéntico, HIGGINS G. E., y MAKIN, D. A., «Does Social Learning Theory Condition the Effects of...», *op. cit.,* pp. 1 y ss.

la decisión racional [44], la del aprendizaje social [45], el control social [46] o el etiquetamiento [47], gran parte de los estudios criminológicos que tratan de comprender el crimen en Internet y de, incluso, definir los caracteres particulares de este evento por el hecho de llevarse a cabo en el ciberespacio, toman en consideración para su estudio, tal y como he analizado en un trabajo reciente [48], la teoría de las actividades cotidianas [49] de Cohen y Felson [50].

En realidad, tiene sentido si tomamos en consideración que la teoría de las actividades cotidianas [51], como parte del germen de todas las actuales teorías de la oportunidad o del día a día [52] que en los últimos años parecen

---

[44] En realidad, y por motivos obvios derivados de la relación entre la teoría de la elección racional y las teorías de la oportunidad, la mayoría de los trabajos en los que se analiza la incidencia del cibercrimen en el modelo teórico de la decisión racional, llevan a cabo su análisis junto con el de otras teorías como la de las actividades cotidianas o referidas a la prevención situacional. Así ocurre, por ejemplo, con BEEBE, N. L., y RAO, S. V., «Using Situational Crime Prevention Theory to...», *op. cit.,* pp. 1 y ss.

[45] YOUNG, R., y ZHANG, L., «Factors Affecting Illegal Hacking Behavior», *op. cit.,* pp. 1 y ss., donde también se tiene en cuenta el enfoque del control social.

[46] SVENSSON, J. S., y BANNISTER, F., «Pirates, sharks and moral crusaders...», *op. cit.,* pp. 1 y ss.

[47] En el *labeling approach* se basa el estudio de TURGEMAN-GOLDSCHMIT, O., «Meanings that Hackers Assign to...», *op. cit.,* pp. 382 y ss.

[48] MIRÓ LLINARES, F., «La oportunidad criminal en el ciberespacio...», *op. cit.*

[49] Véanse así, YAR, M., «The novelty of "cybercrime"....», *op. cit.,* pp. 407-427; CHOI, K., «Computer Crime Victimization and Integrated Theory:...», *op. cit.*, pp. 308 y ss.; HUTCHINGS, A., y HAYES, H., «Routine Activity Theory and Phishing Victimisation:...», *op. cit.*, pp. 433 y ss.; HOLT, T. J., y BOSSLER, A. M., «Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization», en *DB*, vol. 30, núm. 1, enero de 2009, pp. 1 y ss.; HOLT, T. J., y BOSSLER, A. M., «On-line Activities, Guardianship, and...», *op. cit.,* pp. 400 y ss.; YUCEDAL, B., «Victimization in cyberspace:...», *op. cit.,* pp. 26 y ss. Como se puede observar ya sólo en los títulos de los artículos, gran parte de ellos centran el estudio en las implicaciones victimológicas de esta teoría. No es de extrañar si tenemos en cuenta que hay quienes la conciben esencialmente así, y si tenemos en cuenta que su aporte de la oportunidad sitúa al *suitable target* en el centro de la problemática criminológica. Esto hará que posteriormente, cuando analicemos las consideraciones victimológicas de la cibercriminalidad, volvamos sobre algunas de estas referencias y sobre la «Routine Activities Theory» (RAT), traducido como Teoría de las Actividades Cotidianas, en adelante, TAC.

[50] COHEN, L., y FELSON, M., «Social change and crime rate trends...», *op. cit.,* pp. 588-608. El enunciado esencial de la teoría sería que el crimen se produce durante las actividades cotidianas del día a día, cuando se unen en el espacio y el tiempo un objetivo adecuado, un delincuente motivado y sin un guardián capaz de darle protección al primero.

[51] Como ya expliqué en otro lugar, al que remito las explicaciones, me parece preferible la traducción «Teoría de las actividades cotidianas», que la tradicionalmente utilizada «teoría de las actividades cotidianas». MIRÓ LLINARES, F., «La oportunidad criminal en el ciberespacio...», *op. cit.*, p. 07:3.

[52] Se suelen considerar como grandes hitos de las teorías de la oportunidad dos trabajos publicados a finales de los años setenta en Londres y Estados Unidos: por una parte el trabajo monográfico de MAYHEW, P.; CLARKE, R.; STURMAN, A., y HOUGH, M., *Crime as opportunity,* London, Home office Research Study 34, 1976, y por otra el ya citado trabajo de COHEN, L., y FELSON, M., «Social change and crime rate trends...», *op. cit.* Al respecto señala TILLEY, N., *Crime Prevention*, Collumpton, Willan Publishing, 2009, p. 120, que las dos teorías surgieron al mismo tiempo, debiendo considerarse el desarrollo de la teoría de las actividades cotidianas independiente del británico al no existir en aquellos momentos referencias del trabajo realizado al otro lado del Atlántico. Lo cierto es que si bien el planteamiento era diverso, ambas convergían en las bases de las que partían (la decisión racional) y en la voluntad de situar el acento de la prevención y de la explicación del delito no

estar en el centro de los principales debates criminológicos superando las expectativas que se marcaban para la criminología ambiental [53] y que han dado lugar, en conjunción con la teoría de la decisión racional [54], a los desarrollos sobre la prevención situacional del delito [55], partió, como una de sus premisas fundamentales, de la idea de que la modernidad, y en ella la evolución tecnológica, llevaba implícita el aumento del contacto entre potenciales autores, potenciales víctimas y, en algunos casos, la disminución de guardianes capaces de evitar el crimen, con el consiguiente aumento en las tasas de criminalidad [56]. Lo cierto es que si en el momento en que se enunció esta teoría, ello se apoyaba en evoluciones tecnológicas como el automóvil y sociales como la igualdad entre hombre y mujer, que habían modificado la relación entre el ofensor motivado, el objetivo y la ausencia de mecanismos de defensa; hoy, la aparición de un nuevo espacio de comunicación personal transnacional, universal y sujeto a revolución permanente, como es el ciberespacio, anticipa, si no un aumento de la criminalidad, lo cual tendrá que evaluarse a más largo plazo, sí por lo menos, la existencia de un nuevo contexto de oportunidad criminal que coexistirá en el tiempo con el de la realidad física, y que pudiendo compartir con éste el que el delito dependerá de la relación entre victimario, víctima y mecanismos de protección, divergirá en la manifestación concreta de estos mismos factores, fruto de la especialidad del medio en que convergen.

---

sólo en el criminal sino también en el espacio y el tiempo en el que actúa, como demuestran trabajos posteriores en los que se unen Clarke y Felson como en CLARKE, R. V., y FELSON, M., «Introduction: Criminology, routine activity, and rational choice», en CLARKE, R. V., y FELSON, M. (eds.), *Advances y criminological theory, 5. Routine activity and rational choice,* New Brunswick, NJ, Transaction books, 1993. Tampoco habría que desdeñar la importancia en el paradigma de la oportunidad de uno de sus primeros antecedentes, incluso anterior a la teoría de las actividades cotidianas de Cohen y Felson, si bien restringida al papel de la víctima y centrada en la explicación de su victimización a partir de factores demográficos, como es la teoría de los estilos de vida de Hindelang, que vino a ser la primera que incorporó al análisis del crimen el tópico de la víctima. La misma ya argumentaba que las elecciones individuales de la víctima tales como con quién se reunía y por dónde, qué tipo de ocio frecuentaba, etc., influían en el riesgo de victimización (HINDELANG, M. J.; GOTTFREDSON, M. R., y GAROFALO, J., *Victims of Personal Crime..., op. cit.,* p. 242). Como se ha dicho, en España se ha publicado un trabajo sobre la oportunidad en la criminología de SERRANO MAÍLLO, A., *Oportunidad y delito, op. cit.*, donde, superando la consideración de las teorías de la oportunidad como teorías criminológicas integradas, analiza el tópico y lo trata de incluir como parte de la explicación del delito como evento.

[53] Véase sobre la *«environmental criminology»,* su aparición en relación con la Chicago School of Sociology y su desarrollo en múltiples áreas de entre las que destaca el *«opportunity approach»* para la explicación del evento criminal y, dentro de él, la teoría de las actividades cotidianas, el clarificador trabajo de BOTTOMS, A. E., y WILES, P., «Environmental Criminology», en MAGUIRE, M.; MORGAN, R., y REINER, R., *The Oxford handbook of criminology*, New York, Oxford University Press, 1997 (2.ª ed.), pp. 305 y ss., y especialmente en lo que más nos interesa, pp. 320 y ss.

[54] CLARKE, R., y FELSON, M. (eds.), «Routine activity and rational choice», en *ACT,* vol. 5, New Brunswick, New Jersey, Transaction Publishers, 1993, pp. 25 y ss.

[55] GARRIDO, V.; STANGELAND, P., y REDONDO S., *Principios de Criminología,* Valencia, Tirant lo Blanch, 2006 (3.ª ed.).

[56] SERRANO MAÍLLO, A., *Oportunidad y delito, op. cit.,* pp. 36 y ss.

En todo caso, a mi parecer, lo que hace especialmente apta esta teoría, otras como la de los estilos de vida que será analizada especialmente en el capítulo dedicado a la victimización por el cibercrimen, y en general todos aquellos enfoques enmarcados en el tópico de la prevención situacional, para el estudio del cibercrimen, es el hecho de que las mismas ponen el foco de análisis del evento criminal, no tanto en el agresor o criminal, como en el propio espacio y en cómo el mismo puede incidir en la aparición del delito. El nacimiento de un nuevo ámbito de comisión delictiva como el ciberespacio con caracteres intrínsecos y extrínsecos significativamente distintos al espacio físico donde se siguen cometiendo el mayor número de delitos, conlleva que sea oportuno partir de aquellas teorías que prestan atención al lugar de comisión delictiva para comprobar los nuevos caracteres del evento criminal en el ciberespacio.

Y hay un último punto de unión entre el enfoque de la oportunidad y el cibercrimen, que tiene que ver con la necesidad de acudir para la prevención de esta nueva forma de delincuencia a aquellas teorías que pongan la mayor atención posible en el control no formal debido a la probada ineficiencia del control formal, y especialmente de las normas jurídicas nacionales, frente a este tipo de crimen. En efecto, y como advirtió Garland, las que él denomina *new criminologies of every day life*, dan de alguna forma por sentado que el Sistema de la Justicia Penal tiene una capacidad limitada para lograr efectos preventivos, por lo que centran su atención en el mundo de cada día para intentar actuar en él y prevenir así el delito [57]. En palabras esta vez de Medina Ariza, «la prevención del delito es una responsabilidad de todos y no solamente de las agencias de control social formal o el sistema de justicia penal» [58]. Es obvio que este enfoque tiene especial sentido ante un tipo de criminalidad como el que nos ocupa que, debido a que es realizada en el ciberespacio transnacional y anonimizado contra el que, de algún modo, van a chocar la administración de justicia y el sistema penal nacional en general, requiere poner el foco de atención para su prevención no sólo en lo normativo y lo formal sino, más allá de ello, en lo ambiental y en el propio actuar cotidiano de quienes acceden e interactúan en Internet.

Todo lo anterior no supone, por supuesto, ni la consideración de que el enfoque de la oportunidad sea más válido como pensamiento criminológico que el de las tradicionales teorías criminológicas o del delincuente con el consiguiente rechazo de las múltiples críticas dirigidas al *opportunity approach* [59],

---

[57] Garland, D., *The Culture of Control. Crime and Social order in contemporary society,* New York, Oxford University Press, 2001, p. 128.

[58] Medina Ariza, J. J., «El control social del delito a través de la prevención situacional», en *RDPC*, 2.ª época, núm. 2, 1998, p. 281.

[59] Si bien no procede aquí ni una completa revisión de todas las críticas a las teorías de la oportunidad y al enfoque de la prevención situacional, ni su valoración, sí que debe destacarse que su utilización no es pacíficamente aceptada, especialmente por la teoría criminológica más tradicional

ni que sea el único posible para la cibercriminalidad. Simplemente sirve para explicar la decisión tomada de utilizar este enfoque para comprobar la importancia del cambio del entorno espacio/temporal en el fenómeno criminal y, así, analizar el evento cibercrimen. Es evidente la potencial capacidad de algunas de las tradicionales teorías de la criminalidad o del delincuente para la explicación de muchas modalidades de cibercriminalidad, así como que esta visión es perfectamente compatible con una intervención en el ámbito de la oportunidad [60], pero también lo es que aquellas teorías que ponen más énfasis en la relación de lo ambiental o espacial con la propia motivación

---

y por la nueva criminología sociológica, que especialmente intuye problemas éticos y de legitimidad en su utilización que fueron puestos de manifiesto y recopilados en el libro colectivo de VON HIRSH, A.; GARLAND, D., y WAKEFIELD, A., *Ethical and social perspectives in situational crime prevention*, Oxford, 2000, y en otros trabajos posteriores como en GARLAND, D., *The Culture of Control..., op. cit.,* pp. 130 y ss., donde siguiendo con la línea argumentativa de sus dos artículos en el citado libro, GARLAND, D., «Ideas, Institutions and Situational Crime Prevention», en VON HIRSCH, A.; GARLAND, D., y WAKEFIELD, A., *Ethical and Social Perspectives on Situational Crime Prevention,* Oxford-Portland, Hart Publishing, 2000, y GARLAND, D., «The new criminologies of Everyday life: Routine Activity Theory in Historical and social context», en VON HIRSCH, A.; GARLAND, D., y WAKEFIELD, A., *Ethical and Social...», op. cit.,* pp. 1 y ss., y 215 y ss., señala que frente al tratamiento del crimen por la criminología tradicional como un problema con dimensiones sociales, temporales y psicológicas, el modelo de la decisión racional lo hace como una cuestión de precio, lo cual puede conllevar una legitimación de políticas duras en los que la eficacia de la intervención se sobrepone a otros valores. En España estas cuestiones las analizó primero MEDINA ARIZA, J. J., «El control social del delito...», *op. cit.,* p. 286, y lo ha hecho más recientemente en un libro colectivo. Sin entrar en una, imposible aquí, evaluación de las críticas y sus argumentos, lo cierto es que el riesgo del enfoque situacional y, en general, de las teorías de la oportunidad estriba en no prestar atención, desde una perspectiva global y para la prevención del crimen, a los aspectos sociológicos y psicológicos del delito, al igual que algunas teorías criminológicas se centran demasiado en lo explicativo y no aportan auténticas soluciones para la prevención del crimen en contextos determinados. También es evidente que la aplicación de mecanismos de prevención situacional sin sometimiento a los principios y límites de la intervención penal y de la aplicación de políticas públicas de un Estado social y democrático de Derecho, resulta inaceptable, como lo es la aplicación de medidas de intervención social y psicológica a partir de los presupuestos de cualquiera de las teorías criminológicas tradicionales sin el respeto a los citados principios. Pero nada de ello deslegitima el enfoque de la prevención del crimen en el día a día sino que, más bien, las sitúa como parte del análisis que debe realizarse para la prevención de la delincuencia y siempre en el marco de los límites que marca el estado democrático en el que vivimos. Y esto es obviamente también así para la cibercriminalidad: ni pretendo explicar el cibercrimen como evento desde el único marco de la teoría de las actividades cotidianas, ni creo que cualquiera de las medidas posibles para la prevención situacional del delito en el ciberespacio tenga que ser implantada sin antes realizar un análisis de legitimidad de la intervención. Pero sí considero que el enfoque no sólo es el más adecuado para la explicación de las especialidades del crimen en ese nuevo ámbito de intercomunicación personal que son las TIC y, por tanto, también para la prevención de muchas de las conductas nocivas para diversos bienes jurídicos, sino que, en términos de legitimidad, será el que menos restrinja en muchos casos la libertad de las personas, por lo menos en comparación con el tradicional sistema de creación de normas que impidan la realización de comportamientos en el ciberespacio pese a ser prácticamente imposible su real aplicación en Internet.

[60] Y ello tanto desde la visión de la relación entre la oportunidad y la motivación de las teorías integradoras, como por ejemplo la del Triple Riesgo delictivo de Santiago Redondo [REDONDO ILLESCAS, S., «Individuos, sociedades y oportunidades en la explicación y prevención del delito: Modelo del triple Riesgo Delictivo (TRD)», en *Revista Española de Investigación criminológica*, pp. 1 y ss.], como desde la de quienes niegan la integración al entender que motivación y oportu-

del criminal reflejarán mejor los cambios que puede suponer para el crimen como evento el que el lugar de realización sea el ciberespacio.

Esta opción por el enfoque situacional para el análisis criminológico de la cibercriminalidad queda reforzada cuando se comprueba que es la visión más aceptada para su análisis también a nivel comparado. De hecho han sido ya varios los criminólogos anglosajones que, partiendo de los aparentemente sencillos presupuestos de la teoría de las actividades cotidianas, han planteado la posibilidad de que el ciberespacio sea un nuevo ámbito de riesgo criminal, o un evento criminal distinto, en el que se vean modificados algunos de los condicionantes relacionados con el delito [61].

Evidentemente, y como se señaló con anterioridad, no se está diciendo con ello que las teorías que tratan de explicar el evento delictivo no puedan hacerlo ahora con el cibercrimen, como tampoco, obviamente, puede afirmarse que el crimen en Internet no sea un delito tal y como el mismo ha venido siendo discutido y definido por la criminología. Como lo indica el

---

nidad son descripciones distintas de lo mismo, como SERRANO MAÍLLO, A., *Oportunidad y delito, op. cit.,* p. 230.

[61] En este sentido se manifiesta Capeller, quien después de señalar que algunas de las características de Internet, tales como la transnacionalidad, su fugacidad, la volatilidad de sus contenidos y las estrategias de los operadores en la comunidad virtual, tienen un impacto directo en materia penal, concluye que el impacto de dichos cambios en tal ámbito obliga, no sólo a una revisión del derecho sino también, de la teoría criminológica, que debería transitar hacia lo inmaterial para adaptarse al siglo XXI y evitar seguir «frente a un estado de caos virtual». CAPELLER, W., «Not such a neat net...», *op. cit.,* pp. 237 y ss., especialmente 240 y 241. Frente a ello es menos «tremendista» Grabosky (GRABOSKY, P., «Virtual criminality...», *op. cit.,* p. 248), quien reconoce un cambio en el factor oportunidad (que él viene a identificar con el objetivo o víctima de la visión tradicional de la teoría de las actividades cotidianas), pero no en los sistemas de protección ni en el autor motivado, respecto al cual señala, de forma muy gráfica que «si bien las tecnologías pueden cambiar rápidamente, no así la naturaleza humana. Los diez mandamientos son tan relevantes hoy como lo eran en tiempos bíblicos. La emoción del engaño que caracterizó la introducción del caballo de Troya, sigue vigente en la creación de sus descendientes digitales». Véase en sentido similar, en GRABOSKY, P., y SMITH, R., «Telecommunication fraud in the digital age: the convergence of technologies», en WALL, E. (ed.), *Crime and the internet*, London, Routledge, 2001, p. 37; y de forma mucho más amplia aunque con similares argumentos, en GRABOSKY, P., «Computer crime: a criminological overview», en *Presentation at the Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Treatment of Offenders,* Vienna, 15 de abril de 2000, pp. 2 y ss. También analiza la cuestión PEASE, K., «Crime futures and foresight: Challenging criminal behaviour in the information age», en WALL, D. (ed.), *Crime and the Internet*, London, Routledge, 2001, p. 23, que compara el *cyberspace* con el *meatspace*, señalando que mientras que en el último el número de víctimas está limitado por la velocidad en la que pueden situarse «frente al agresor», esto ya no ocurre en el ciberespacio donde muchas víctimas pueden ser dañadas a la vez. Precisamente Pease ya había publicado un interesante trabajo sobre la evolución del crimen en el futuro en el que ya apuntaba algunos de los cambios criminológicos que podrían producirse en el ciberespacio como por ejemplo, la diferente relación entre agresor y víctima, fruto de la inexistencia de un contacto visual directo de uno con otra, DAVIES, R., y PEASE, K., «Crime, technology and the future», en *SJ*, núm. 13, abril de 2000, p. 61. Algunas de estas y otras referencias son apuntadas por YAR, M., «The novelty of "cybercrime":...», *op. cit.,* pp. 407-427, quien, a mi parecer, realiza el análisis más completo sobre la validez de los tópicos de la criminología clásica para la comprensión de unos crímenes aparentemente nuevos como los cometidos en el ciberespacio.

propio término, el cibercrimen es un crimen, un delito que debiera poder ser analizado y comprendido por cualquier teoría que trate de abarcar el fenómeno delictivo de forma completa. De hecho nada parece indicar que los presupuestos básicos de la teoría de las actividades cotidianas o, en general, del paradigma criminológico de la oportunidad, no sean válidos para la cibercriminalidad, en la misma medida en que lo sean para cualquier otro tipo de delito. Más bien al contrario lo que sucede es que tales parámetros, tales elementos definitorios del evento criminal, deben ser revisados con nuevos ojos al ser distinto el entorno o ámbito en el que se comete el delito [62]. Al igual que ocurre con tantas otras ciencias y técnicas sociales, la criminología fue construyendo sus desarrollos a partir de un objeto con unas características determinadas; es obvio que el cambio en las mismas, siempre que no modifique la esencia del objeto pero sí elementos configuradores del mismo, obligue a un replanteamiento teórico que, a mi humilde parecer, todavía no está siendo realizado con la profundidad que merecería por la doctrina criminológica. El ciberespacio no cambia los caracteres esenciales que hacen que a determinados eventos se les pueda seguir denominando crímenes, pero sí modifica los parámetros espacio/tiempo en los que el crimen tiene lugar, por lo que es lógico que ello exija un replanteamiento de las teorías criminológicas que tratan el crimen como evento y que, por ello, prestan especial atención al contexto espacial y temporal en el que el mismo se produce.

Esto no significa, tampoco, que estas teorías de la oportunidad y los desarrollos de la prevención situacional ya no sean acertadas para explicar «el crimen», como concepto englobador de todos y cualquiera de estos eventos: sólo dejarán de serlo, por no dar cabida al cibercrimen, en cuanto exijan como presupuesto para su existencia como evento la realización del hecho en un espacio físico y en un tiempo determinado conforme a la concepción tradicional [63]. Lo cual se hacía, implícita, pero no explícitamente, con la teoría de las actividades cotidianas que es perfectamente apta para explicar el evento cibercrimen como se verá a continuación.

3.2. El triángulo del cibercrimen: el ciberespacio, nuevo ámbito de oportunidad criminal

La teoría de las actividades cotidianas afirma que el delito se produce en un tiempo y un lugar pero no exige que sea físico, aunque implícitamente lo estuviera presuponiendo [64]. Por supuesto, el lugar de comisión de un crimen

---

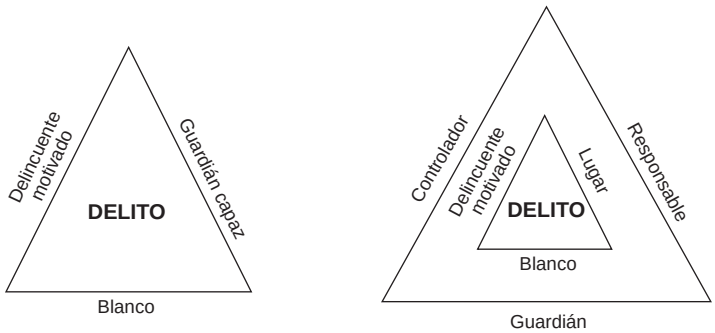
[62] En idéntico sentido, YUCEDAL, B., «Victimization in...», *op. cit.,* p. 43.

[63] Y en ese caso sólo dejarían de ser válidas las teorías o desarrollos de las mismas para el cibercrimen, pero no para la criminalidad en el espacio físico.

[64] Esto es obvio en COHEN, L. E., y FELSON, M., «Social change and crime rate trends..., *op. cit.,* p. 590, y en posteriores obras de Felson, como FELSON, M., «Routine activities and crime prevention», en *Studies on Crime and Crime Prevention: Annual Review,* 1, pp. 30 y ss. Por el con-

puede ser el ciberespacio que, como hemos visto, difiere en su arquitectura del espacio físico en el que sólo podían cometerse los delitos hasta hace unas décadas. Pero si en el ciberespacio puede cometerse un delito, en él tendrán que darse también los caracteres que se asignan al mismo. Es decir, si el crimen, como evento, depende de la presencia de un delincuente capacitado y motivado para el delito, un objetivo o víctima adecuado y la ausencia de un guardián capaz, en la primera fórmula de la TAC, así como de los demás elementos incorporados en las siguientes fórmulas [65], lo mismo deberá poder decirse del cibercrimen. Eso sí, al cambiar la configuración espacio-temporal del ciberespacio será distinto el modo en que confluirán tales elemento, será distinto. El triángulo del crimen seguirá existiendo como tal y con los mismos elementos, aunque quizás los «ángulos», valga la expresión, sean distintos. O en otras palabras, el lugar «ciberespacio», no alterará los factores del crimen, pero sí la concreta expresión de los mismos y, por tanto, de múltiples elementos que deberían ser tomados en consideración en aras a la prevención del delito.

Gráfico 3.5. Triángulo del crimen de Cohen y Felson, en su primera versión. El triángulo de la derecha se confeccionó tras las aportaciones de Eck y otros autores.



trario, en la última edición de *Crime and everyday life*, Felson, ya viene a reconocer implícitamente el ciberespacio como espacio del delito. FELSON, M., y BOBA, R., *Crime and everiday life,* Thousand Oaks, CA, Sage, 2009 (4.ª ed.).

[65] A los tradicionales elementos se pretendió añadir posteriormente un cuarto elemento, la ausencia de una persona que controle las actividades del ofensor motivado (*personal handler*), y después el gestor del lugar. FELSON, M., «Linking criminal choices, routine activities, informal control and criminal outcomes», en CORNISH, D. B., y CLARKE, R. V. (eds.): *The reasoning Criminal, Rational choice perspectives on offending*, New York, Springer-Verlag, 1986. Véase también sobre ello, ADLER, F.; MUELLER, G. O. W., y LAUFER, W. S., *Criminology and the Criminal Justice System*, New York, McGraw Hill, 4.ª ed., 2001, p. 241, y también TILLEY, N., *Crime prevention, op. cit.,* p. 120. Así, los tres elementos que conformaban el delito en un primer momento, agresor, objetivo y ausencia de guardián, mutaron primero en la sustitución del guardián por el lugar en el primer triángulo, y después con la incorporación de un segundo triángulo superpuesto al primero en el que el guardián capaz tutela el objetivo adecuado, el *personal handler* al agresor motivado y el gestor del lugar al espacio en el que se produce el ataque.

Para analizar las razones de los diferentes ángulos que conforman la interacción del agresor motivado con el objetivo adecuado en el lugar ciberespacio, hay que contrastar tales elementos con los caracteres intrínsecos y extrínsecos del ciberespacio, definiendo, así, los rasgos más singulares de ese nuevo ámbito de oportunidad delictiva y en comparación con el otro ámbito de oportunidad criminal, el del espacio real. El resultado de tal comparación deberá servirnos para comprender las peculiaridades del cibercrimen que deben ser tomadas en consideración para definir los instrumentos de prevención del mismo.

Por otra parte, y pese a que todos los elementos del evento criminal se explican al venir unidos entre sí, voy a analizar el mismo estudiando de forma separada la incidencia del ciberespacio en cada uno de los elementos que conforman el triángulo del delito (tal y como quedaría con la primera configuración de Cohen y Felson), añadiendo a los gestores del lugar que se incorporan en el segundo triángulo y eliminando, por motivos obvios, el lugar (que es el propio ciberespacio). Ello no significa que crea que se trate de elementos separados: a mi parecer la TAC aporta la idea de que para la comprensión del delito no sólo hay que mirar al agresor, sino también otros elementos del evento, pero es obvio que todos los que lo conforman están interrelacionados, de modo tal que la propia motivación del agresor depende de los demás factores, así como el objetivo es definido como adecuado por la conducta del agresor, etc. El estudio separado de los elementos es, por tanto, meramente a efectos didácticos. El cibercrimen, como el delito en el espacio físico, es la confluencia de las partes en el todo.

3.2.1. *El ciberagresor motivado*

He señalado en otro lugar que los caracteres intrínsecos del ciberespacio, su propia esencia como ámbito virtual en el que las coordenadas ya no son definidas en términos de distancia, sino, más bien, de posibilidades de comunicación, producen como primer efecto de mutación del ámbito de oportunidad criminal, el incremento significativo de los márgenes potenciales del evento criminal [66]. Obviamente, el agresor en el ciberespacio sigue motivándose sobre un determinado objetivo y en un lugar, y el evento, analizado «*ex post commissio*», seguirá, al igual que el ejecutado en el espacio físico, conformado por tales elementos concretados en una víctima y un ámbito de localización. Pero, desde una perspectiva «*ex ante*», el campo de oportunidad de un agresor motivado (en abstracto) es muy amplio en el ciberespacio debido a la inexistencia de la distancia física como barrera o, dicho de otra forma, a la no necesidad de

[66] Miró Llinares, F., «La oportunidad criminal...», *op. cit.*

cercanía entre agresor y víctima para la (ciber)delincuencia [67] tal y como sí se requería generalmente en el espacio físico [68]. Mientras que lo usual en la criminalidad suele ser que el delincuente realice el delito cerca de su propia residencia [69], o cuanto menos que no se desplace a largas distancias, salvo en el caso de que el incentivo derivado del ataque al objetivo adecuado sea especialmente valioso, en la cibercriminalidad no hace falta salir de casa para atacar a bienes jurídicos que se encuentran físicamente muy lejos [70].

Es cierto que ya existían tecnologías que posibilitaban que el ataque criminal se realizara desde un lugar y los efectos se produjeran a miles de kilómetros de distancia. Pero también es claro que han sido las TIC las que han creado el ciberespacio en el que la distancia física deja de ser una barrera infranqueable para muchos delitos [71], constituyéndose en un ámbito de oportunidad más amplio (siempre en términos potenciales): aumenta considerablemente el número de personas que pueden contactar entre sí como agresores y objetivos adecuados [72], expandiéndose, por tanto, el ámbito potencial de oportunidad criminal [73]. En otras palabras, y refiriéndonos a los elementos del triángulo del delito: al no existir distancias que actúen como barreras y dificulten el contacto entre las personas y sus bienes, entre los agentes motivados y los objetivos adecuados, el potencial número de los que pueden acabar siendo unos y otros aumenta.

Lo más relevante de lo señalado, en todo caso, y desde la perspectiva del agresor motivado, es que la compresión del espacio que supone el ciberespacio incrementa las «posibilidades de motivación» de un potencial agresor motivado. Lo hace al menos por dos razones. La primera porque incrementa los objetivos potenciales sobre los que puede tomar la decisión de cuál es el adecuado, sin que la distancia ni el tiempo sean elementos esenciales de la decisión. La segunda porque reduce el coste espacio-temporal

---

[67] JONES, B. R., «Comment: virtual...», *op. cit.*, pp. 610 y ss.

[68] MIRÓ LLINARES, F., «La oportunidad criminal...», *op. cit.* Al fin y al cabo, y como han señalado Brenner y Clarke, en el mundo real (físico), el autor y la víctima generalmente están próximos, en términos de distancia física, cuando se produce el delito: no sólo no es posible la violación o el homicidio si agresor y víctima no están juntos en el momento del ataque, sino que gran parte de los fraudes se producen debido a que ha existido un contacto, hasta el punto de que en un mundo no tecnológico no es posible robar o defraudar la propiedad si el ladrón y la víctima se encuentran en diferentes países o ciudades. BRENNER, S. W., y CLARKE, L. L., «Distributed Security: preventing cybercrime», en *TJMJCIL,* Summer 2005, p. 3.

[69] BOTTOMS, A. E., y WILES, P., «Environmental Criminology», *op. cit.,* p. 323.

[70] KSHETRI, N., «The Simple Economics of...», *op. cit.*

[71] Así señalan ADLER, F.; MUELLER, G. O. W., y LAUFER, W. S., *Criminology and the Criminal..., op. cit.,* p. 351, que en el ciberespacio, los movimientos físicos son reemplazados por los «viajes electrónicos», por lo que los agresores ya no necesitan estar al lado de las víctimas.

[72] JONES, B. R., «Comment: virtual...», *op. cit.*, p. 610.

[73] En este sentido también, MCQUADE, S. C., «Cybercrime», en TONRY, M. (ed.), *The Oxford Handbook of Crime and Public Policy,* New York, Oxford University Press, 2009, p. 481.

que supone prácticamente siempre cometer un delito, tanto en términos de llegar al objetivo como en el de asegurarse la huida una vez el delito se ha cometido.

El que no exista un desplazamiento espacial y que el sujeto pueda «ahorrarse tal coste, no significa que no haya un coste temporal para la realización de un ataque en el ciberespacio. Siempre lo habrá, y será mayor o menor dependiendo del tipo de cibercrimen. En el caso de los económicos en particular, el desarrollo de programas y técnicas o la propia búsqueda de vulnerabilidades exige a los *hackers* mucho tiempo, al igual que para el ladrón se exige preparación en el espacio físico. En realidad es este tiempo, el de preparación del ataque y de selección de los objetivos, el que se convertirá en el auténtico protagonista, en términos de coste, del ataque en el ciberespacio. De hecho, la selección de objetivos es la clave, como se ha visto, de gran parte de la cibercriminalidad económica, especialmente del *phishing,* tanto por medio de la búsqueda de vulnerabilidades en los sistemas para ser infectados como *bots,* como de la búsqueda de destinatarios finales a los que defraudar. Eso sí, se trata de un proceso de selección, y sobre ello se volverá más adelante, en el que interviene mucho la víctima, pues lo que hará el ciberagresor en muchas ocasiones es crear el *software* y el lugar en el que lo deja, y será la víctima con la vulnerabilidad *x* la que, al interaccionar, será infectada y «atacada». En todo caso, costes temporales relacionados con la preparación y ejecución del crimen, los hay tanto en el ciberespacio como *offline.*

En lo que sí variará es en los costes de desplazamiento y de huida que están presentes en el crimen en el espacio físico, pero no en el cibercrimen.

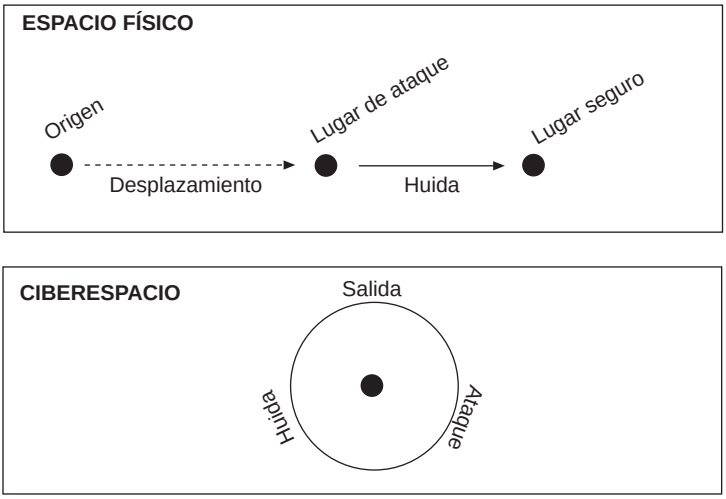
Tabla 3.1. Costes del crimen en términos de tiempo y distancia. Construcción propia.

Espacio físico				
Selección	Preparación	Desplazamiento	Ejecución	Huida
Ciberespacio				
Selección		Preparación		Ejecución

Así, mientras que el criminal en el espacio físico tiene que tener en cuenta el coste, en términos de distancia y tiempo, de la huida del lugar desde el que ha cometido el delito a un lugar seguro (como tiene que tener en cuenta la distancia y tiempo desde su lugar de origen a aquél en el que comete la infracción), el cibercriminal «se ahorra» estos costes.

También en relación con el agresor y la incidencia en él de la arquitectura del nuevo ámbito en el que actúa como es el ciberespacio, hay que

Gráfico 3.6. Costes del crimen en el espacio físico y en el ciberespacio en términos de distancia. Elaboración propia.



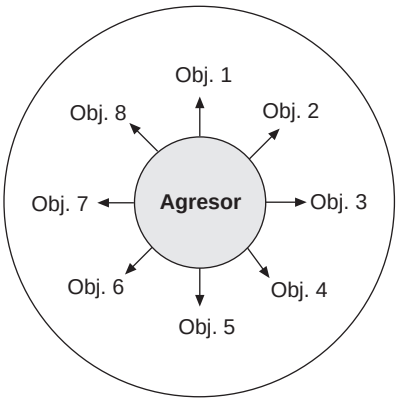
señalar que las TIC pueden actuar como un «multiplicador de fuerza» [74] que hace que personas con mínimos recursos puedan generar grandes daños para múltiples personas y bienes en el ciberespacio [75]. Además, la expansión del ámbito comunicativo al que puede acceder un agresor motivado que supone el ciberespacio conlleva una multiplicación de la potencialidad lesiva de una conducta por comparación con lo que ocurre en el espacio físico. Me explico. Aunque hay armas sofisticadas que permiten causar daños a múltiples bienes en el espacio físico y real, lo general es que la producción de daños a bienes existentes en lugares distintos (y desde luego en países distintos sería también válido como excepción para las armas) requiera de un tránsito del cibercriminal de un lugar a otro que, en el ciberespacio, no es necesario. Esto ya ocurría con los delitos «de palabra» en relación con la televisión y otros medios de comunicación. En el ciberespacio aún es más significativo: como se ve en el siguiente gráfico, el agresor puede no sólo seleccionar entre muchísimas víctimas potenciales sino que puede atacar a varias de ellas en el mismo instante y desde el mismo espacio, aunque ellas se encuentren en lugares situados a miles de kilómetros de distancia entre sí; e incluso aunque los efectos de los ataques no se desplieguen (o sí) en el mismo momento.

Además, el ciberespacio no sólo permite al agresor motivado seleccionar entre varias víctimas el objetivo de su ataque, sino que la contracción de las distancias le ofrece la posibilidad de atacar a varias con una única conducta.

---

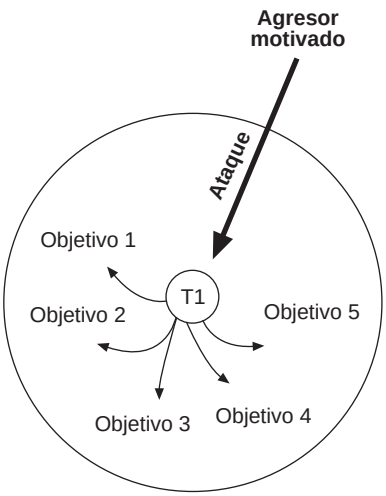
[74] YAR, M., «The novelty of "cybercrime"...», *op. cit.,* p. 411.
[75] También, PEASE, K., «Crimefutures...», *op. cit.,* p. 23.

Gráfico 3.7. Multiplicidad de objetivos para un mismo atacante. Un agresor actúa a la vez sobre varios objetivos. Elaboración propia.



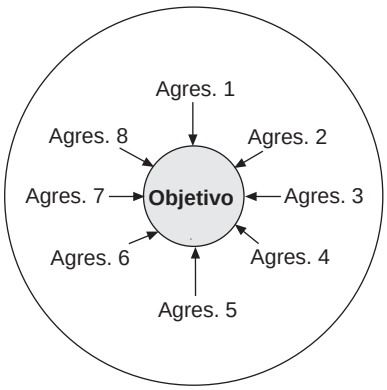
Esto también es posible en el caso de la criminalidad llevada a cabo en el espacio físico-real, si bien las facilidades para ello en el ciberespacio son mucho mayores, especialmente en el caso de la modalidad de cibercrímenes en los que la ilicitud deviene del contenido y en los que la mera publicitación de una página web con contenido nocivo o prohibido (ciberterrorismo, *hate speech,* pornografía infantil, piratería intelectual, etc.) ya supone la afectación de múltiples bienes jurídicos o del mismo bien supraindividual pero con una mayor dimensión en la lesión.

Gráfico 3.8. Ataque múltiple. Con la misma acción se atacan diversos objetivos (y al mismo tiempo). Elaboración propia.



También es perfectamente posible en el ciberespacio que una misma víctima sea atacada de forma simultánea y en el mismo espacio que ocupa por múltiples agresores distintos.

Gráfico 3.9. Multiplicidad de atacantes para un mismo objetivo. En el mismo (ciber)espacio pero desde espacios (físicos) distintos y en momentos temporales que pueden ser idénticos en cuanto al despliegue de efectos pero no tienen por qué serlo en cuanto al momento del ataque. Elaboración propia.

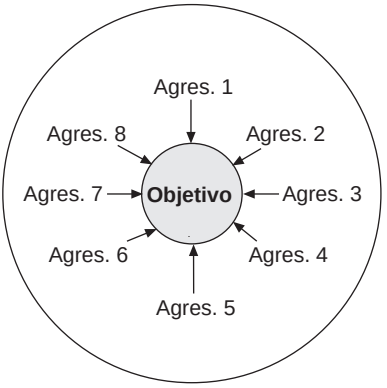


Por último, el agresor puede utilizar uno o múltiples sistemas informáticos situados también en múltiples lugares (redes *hotnet*) desde los que realizar ataques que pueden ocurrir de forma simultánea o secuencial y contra un único objetivo o contra objetivos que pueden ser múltiples e incluso indeterminados, sin que sea necesario para ello hacer ningún esfuerzo de traslado [76].

Y todo eso, por supuesto, ejecutado por el agresor desde y sobre cualquier parte del mundo [77]. Al fin y al cabo, la compresión o contracción de las distancias y la consiguiente expansión comunicativa en el ciberespacio, no sería tan relevante si el mismo no fuera transnacional y se hubiera popularizado de la forma que lo ha hecho. En el ciberespacio, los ofensores con inclinaciones criminales pueden serlo de y desde cualquier Estado nacional y pueden actuar sobre víctimas de (y hacia) otros distintos, reduciéndose las barreras que el espacio suele imponer para ello. Pero además, al aumentar la cantidad de personas que utilizan Internet, también lo hace el número de potenciales delincuentes [78], y al unir el ciberespacio a miles de millones

[76] McQuade, S. C., «Cybercrime», *op. cit.,* p. 482.
[77] Pease, K., «Science in the service of crime reduction», en Tilley, N. (ed.), *Handbook of crime prevention and community safety,* UK, Willan Publishing, 2005, p. 181.
[78] Hutchings, A., y Hayes, H., «Routine Activity Theory...», *op. cit.,* p. 435.

Gráfico 3.10. Multiplicidad de lugares en el ciberespacio que utiliza el agresor para atacar a la víctima situada en un único punto en el espacio físico. Elaboración propia.



de ciudadanos en un «lugar común» en el que hay relaciones comerciales y personales, aumentan también los «objetivos adecuados» y, por tanto, las posibilidades de contacto entre unos y otros con el consiguiente potencial aumento de la criminalidad [79]. En este sentido, el ciberespacio es, desde una perspectiva cuantitativa, un espacio de riesgo criminal con un «potencial» efecto multiplicador sin precedentes en la historia [80].

Además, y como se ha adelantado, la reducción de la distancia conlleva una reducción del tiempo como coste. Todos los ataques a uno o varios objetivos pueden realizarse en el mismo momento, sin que sea necesario el tiempo requerido para transitar la distancia que separa a los objetivos para que todos se vean afectados. Además, y siguiendo en el análisis de la incidencia de las nuevas condiciones ambientales en el factor «agresor motivado», pero prestando ahora atención al factor temporal, las especiales características del ciberespacio y de determinados instrumentos de comisión de los ciberataques como los virus, permiten que en determinadas condiciones la presencia del agresor motivado tenga lugar en un momento de tiempo anterior al perfeccionamiento del ataque. A esto es a lo que, a mi parecer, se refiere Alshalan cuando señala que en el ciberespacio puede desaparecer el agresor motivado de la ecuación del delito en el caso de los ataques con virus [81]. Propiamente el agresor motivado no desaparece, sino

---

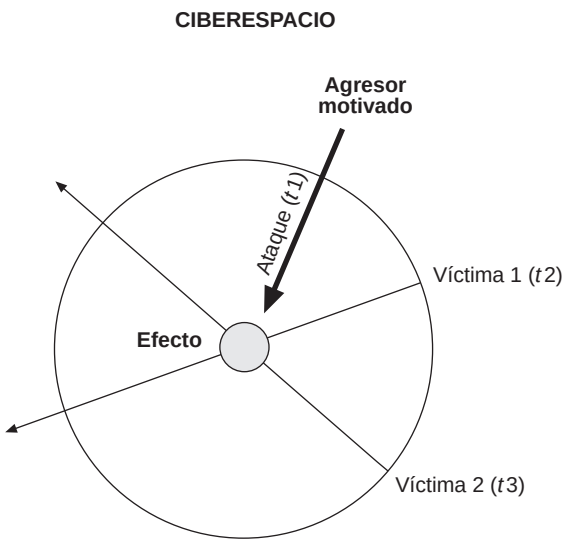
[79] En el mismo sentido, entre otros, GRABOSKY, P., «Virtual Criminality...», *op. cit.,* p. 248, y NISBETT, C., «New directions on Cybercrime», White Paper, Qinetiq, en Internet en *http://apps.qinetiq.com /perspectives/pdf/EP_White_Paper3_Cyber%20Crime.pdf*, p. 2.

[80] CLOUGH, J., *Principles of Cybercrime, op. cit.,* p. 5.

[81] ALSHALAN, A., *Cyber-Crime Fear and Victimization: An Analysis of A National Survey,* Mississippi State University, 2006, p. 146, al señalar que «En el ciberespacio el lugar es Internet, y el

que simplemente su ataque se produce en un ámbito (y en un momento temporal) en el que la concreción del mismo ya no dependerá tanto de la propia conducta de éste como de la de la víctima. Esto ocurre especialmente en el caso de los virus que son subidos a una determinada página web de descargas bajo la falsa apariencia de archivos de música o vídeo. El agresor motivado realiza su ataque dejando en el ciberespacio el instrumento del mismo como algo estático que espera a la conducta de la víctima para que el ataque termine perfeccionándose. Pero esto no significa que no haya agresor, sino que el mismo puede actuar multiplicando su capacidad lesiva en Internet sin las tradicionales limitaciones temporales y espaciales definidas por el espacio físico. Lo hará, eso sí, siempre que la víctima interaccione o, mejor dicho, con la víctima que interaccione con el efecto por él diseminado.

Gráfico 3.11. Fijación del ataque e interacción de la víctima. El ataque deja un efecto fijo en el ciberespacio, siendo la víctima la que interacciona con él. Elaboración propia.

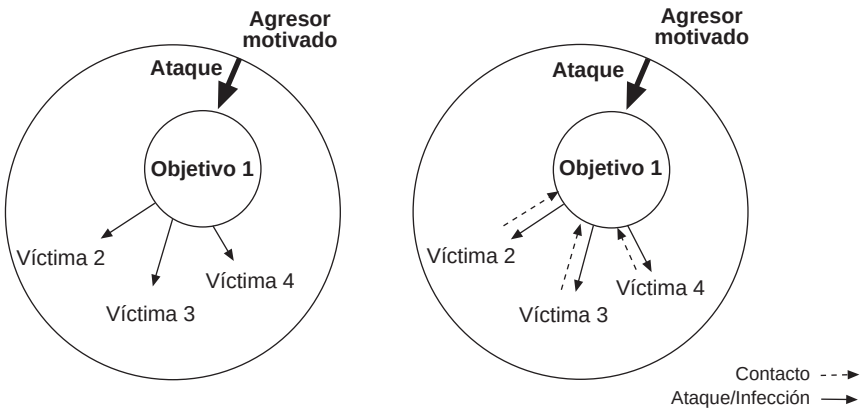


Y es que la contracción del espacio también puede tener importantes consecuencias en relación con los efectos del delito, muy en especial con alguno de los tipos de criminalidad en el ciberespacio caracterizada por la dinámica consistente en que la víctima-receptora del mismo se convierte inmediatamente, y sin quererlo, en emisor de un nuevo ataque en una cadena

tiempo eventualmente proporciona virus o *spyware,* no dependiendo el crimen de la presencia de un agresor».

sucesiva que ni siquiera es controlada por el propio autor del crimen. Esto ocurre con la transmisión de virus, también con el envío de *spam,* e incluso, aunque de forma diferente dado que en este caso es el receptor del mensaje el que tiene que acceder a la comunicación, con la transmisión de contenidos ilícitos o nocivos (pornografía infantil, obras protegidas, *hate speech*, etc.) en páginas web. Si los contenidos o los mensajes se transmitieran de forma física, la distancia entre emisor y receptor complicaría la multidifusión del ilícito. En el ciberespacio es distinto, pues la contracción del espacio y la interconexión de todos los sistemas hacen que la multiplicación de los efectos de la conducta sea prácticamente inmediata [82]. En la criminalidad realizada en el espacio físico-real es difícil encontrar algo semejante, a menos que se trate de la contaminación alimentaria o algunas formas de delincuencia ambiental, excepciones a la regla de que el delito produce sus efectos dañosos de forma controlada y dependiente esencialmente del actuar del criminal.

Gráficos 3.12 y 3.13. La víctima como instrumento de difusión del ataque. En la 3.12 la víctima difunde el ataque a sus contactos, y en la 3.13 son las víctimas las que, al interaccionar con ella, se infectan. Elaboración propia.



Por último, se ha relacionado acertadamente el aumento del riesgo criminal derivado de la potenciación del factor «agresor motivado», con el anonimato en Internet, que otorga una sensación de seguridad al infractor, al ofrecerle un refugio aparentemente seguro en el que ocultarse [83], lo cual a su vez le permite reinventarse y adoptar nuevos personajes virtuales con

[82] También reconoce la multiplicación de los efectos de los ataques en el ciberespacio AGUSTINA SANLLEHÍ, J. R., «La arquitectura digital de Internet como factor criminógeno», en *IeJCS,* art. 4, núm. 3, 2009, p. 9.

[83] PITTARO, M. L., «Cyber stalking...», *op. cit.,* p. 181.

los que, quizá, cometer delitos [84]. Con el anonimato ocurre, por tanto, algo muy similar a lo que relatábamos en relación con la transnacionalidad, que incide en la desaparición del temor a ser identificado y en la consiguiente minimización del temor a ser detenido [85], frenos de la motivación criminal que le convierten en un *motivated offender* [86]. Desde la perspectiva de la teoría de la decisión racional, por tanto, el ciberdelincuente incluiría dentro de los riesgos potenciales que tiene que sopesar frente a los beneficios de su agresión la enorme dificultad que plantea hoy en día la identificación, en términos judiciales probatorios, del cibercriminal [87]. Porque no sólo se trata de la identificación de la dirección IP, sino de la posterior concreción del usuario concreto del sistema informático al que se ha concedido la misma. Es obvio que existen medios para evitar estos riesgos. Así, los mecanismos electrónicos de identificación, como el ID (identificador) de usuario, sistemas automatizados de control del acceso o cámaras de vigilancia, pueden servir como elementos de disuasión al aumentar el riesgo percibido de ser detenidos [88]. De momento, sin embargo, ello no parece posible, pues el anonimato no sólo sirve a propósitos criminales, sino también a otros lícitos relacionados con la sencillez de la accesibilidad al ciberespacio que difícilmente sería compatible con otros sistemas de identificación que, además, podrían ser sencillamente falseados.

3.2.2. *Objetivos adecuados en el ciberespacio: del VIVA al IVI*

En realidad, lo que se ha afirmado hasta el momento del agresor motivado tiene consecuencias directas en el elemento «objetivo adecuado»: el crecimiento del ámbito de riesgo no es sólo por el agresor, sino por las víctimas potenciales que también son muchas más al no ser necesaria una inmediatez temporal y una cercanía física entre agresor y objetivo; del mismo modo las dinámicas de los ciberataques y la potenciación de las facilidades para la agresión que conlleva el ciberespacio inciden en el objetivo adecuado de la misma, y lo mismo puede decirse de los efectos del ciberdelito. Al fin y al cabo, ya se ha dicho que la separación entre agresor motivado y objetivo adecuado tan sólo es figurativa: no hay motivación sin objetivo y viceversa.

---

[84] YAR, M., «The novelty of "cybercrime"...», *op. cit.,* p. 421.

[85] También en este sentido, Mestre Delgado cita como una de las tres leyes del cibercrimen la ocultación de los autores «por los anchos dominios de la aldea global», junto con la optimización de la eficacia del esfuerzo criminal y la minimización de los riesgos para el agresor derivados de la relación personal con la víctima. MESTRE DELGADO, E., «Tiempos de cibercrimen», en *LL,* núm. 37, año IV, abril de 2007, p. 3.

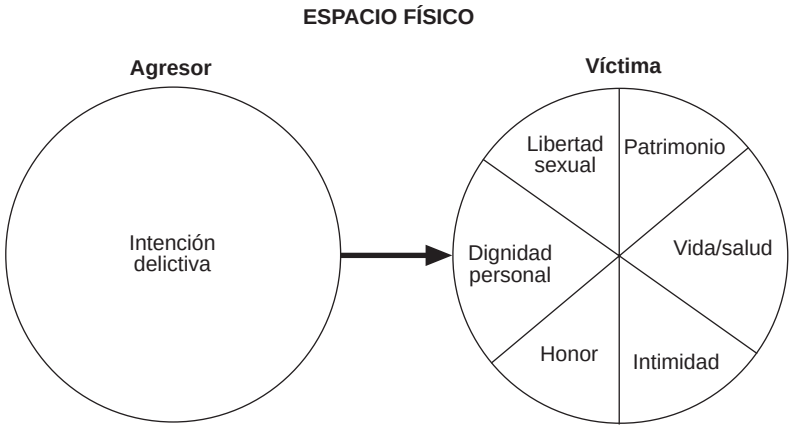
[86] PITTARO, M. L., «Cyber stalking...», *op. cit.,* p. 181.

[87] *Ibid.,* p. 189.

[88] LONGE, O. B.; MBARIKA, V.; KOUROUMA, M.; WADA, F., e ISABALIJA, R., «Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities», en *IJCSIS,* vol. 6, núm. 3, 2009, p. 127.

En todo caso, debe precisarse lo que supone el incremento potencial de las posibilidades de contacto entre agresor y víctima en el ciberespacio. El contacto entre objetivo y agresor en el espacio físico es, generalmente, un contacto físico directo e inmediato, en el que todos los bienes personales de la víctima y los patrimoniales que lleve con ella están expuestos y se convierten en potenciales objetivos adecuados para el ataque del agresor. Es cierto que la víctima potencial puede determinar en gran parte aquello que puede convertirse en objetivo adecuado, seleccionando los bienes con valor económico que lleva consigo, etc.; pero no puede eliminar del ámbito de contacto con las personas otros bienes personalísimos que van indisolublemente unidos a ella. Prácticamente todo lo que ella es como persona, todo lo que forma parte de ella, se pone en contacto con el agresor en el espacio físico.

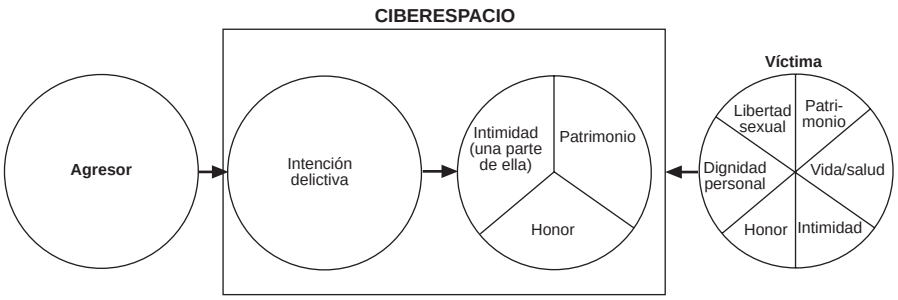
Gráfico 3.14. Contacto en el espacio físico. Agresor contacta con la víctima (con todos sus bienes) y selecciona los bienes a los que quiere afectar de todos los que posee. Elaboración propia.



En el espacio virtual o ciberespacio, el contacto entre personas es distinto: no es la persona física la que se comunica directamente, en un contexto espacio-temporal determinado, con otra persona, sino una representación de la misma, en lo más esencial por ella definida, la que contacta en ese ámbito comunicativo que es Internet. La persona no entra con todos sus bienes y valores en el ciberespacio, sino básicamente con aquellos que ella elige de entre los que pueden hacerlo. Al fin y al cabo, el primer límite que tiene la víctima para comunicarse con otra o para contactar en el ciberespacio es que no puede poner a disposición de otros su entidad física, de modo que los ataques a la persona que se dirijan directamente contra bienes como la vida o la salud, no podrán ser llevados a cabo en Internet. Además, y pese a que la persona puede ver atacados algunos bienes personalísimos aunque

ella no quiera ponerlos a disposición de terceros en el ciberespacio (como ocurre con la libre formación de la sexualidad de los menores, que puede ser atacada al recibir una imagen de contenido sexual o similar), en otros bienes como los relacionados con la privacidad o el propio patrimonio es la víctima la que decide, al incluir información personal en el ciberespacio o compartirla con otros, realizar actividades económicas y demás, situar tales bienes en ese ámbito de riesgo nuevo.

Gráfico 3.15. Contacto en el ciberespacio. La víctima no entra en toda su integridad en el ciberespacio, sino que lo hace con algunos bienes introducidos por ella, que son los que pueden ser atacados según la intención del agresor. Elaboración propia.



Los usuarios del ciberespacio pueden, por tanto, eliminar del ámbito de ataque aquellos bienes que no incorporen al ciberespacio. Apoyándonos en uno de los elementos del acrónimo CRAVED, utilizado por Clarke para definir los bienes preferidos por los ladrones (*Concealable, Removable, Available, Valuable, Enjoyable and Disposable*) [89], podríamos decir que si una víctima no introduce un bien en el ciberespacio, el mismo no estará disponible (*not available*) y no podrá ser objeto del ataque. El crimen, por tanto, en cuanto al objetivo concreto sobre el que se dirige, puede ser evitado por la propia víctima en el ciberespacio desde el momento que no sitúa el mismo en el espacio virtual. Independientemente de su valor, si la víctima no se incorpora al ciberespacio, el objetivo no existe y, por el contrario, la introducción de elementos en Internet conlleva inmediatamente el riesgo de que puedan ser victimizados. En este sentido, por ejemplo, podríamos citar los estudios empíricos que demuestran la relación entre la entrega de información personal *online* y la victimización por los delitos más relacionados con los jóvenes como víctimas como el *cyberbullying* y el ciberacoso sexual

[89] CLARKE, R. V., «Hot products: understanding, anticipating and reducing demand for stolen goods», *Paper núm. 112,* London, Police Research Series, British home Office Research Publications, 1999, pp. 23 y ss.

a menores [90]. En este último caso, hay estudios que constatan que prácticamente todas las modalidades de ataque se configuran en torno a una similar dinámica en la que el paso inicial suele ser el previo envío (la introducción), por parte de la víctima, de información personal a personas desconocidas [91]. Ahora bien, y como se profundizará después, la mera introducción del objeto no es per se peligrosa, sino que constituye un primer paso que, si se une a la interacción de la víctima en el ciberespacio, ya puede conllevar riesgo de victimizacion. En efecto, los estudios victimológicos existentes sobre el *online grooming* parecen demostrar que mientras que el mero hecho de colgar información personal en páginas web o redes sociales [92] no es un factor que incida en el aumento de riesgo de recibir un ataque de *grooming,* sí lo es el enviar directamente información personal a desconocidos.

La introducción de un objetivo en el ciberespacio, sin embargo, no siempre es voluntaria. En ocasiones, se trata de un proceso casi fortuito: el mero hecho de disponer de un sistema informático y de utilizarlo, implica la introducción de elementos relacionados con la privacidad que, sin quererlo, pueden conllevar afectaciones a la intimidad o al propio patrimonio. La respuesta a un correo electrónico con el número de una cuenta bancaria supone la introducción del patrimonio disponible en esa cuenta en el ciberespacio, y del mismo modo el acto de compartir una foto familiar en Facebook o información sobre un viaje reciente, acarrea el riesgo de que sea utilizado en contra de la dignidad o la intimidad de la persona.

En todo caso, el primer condicionante para que un objetivo sea adecuado a los efectos de la fórmula del cibercrimen, es su introducción en el ciberespacio. A partir de que un objetivo se introduce en el ciberespacio, voluntaria o involuntariamente, el mismo puede convertirse en adecuado dependiendo de su valoración por parte del agresor motivado. Encontramos aquí, pues, la primera divergencia de las condiciones que hacen adecuado un objetivo para el cibercrimen, con las que, con el acrónimo VIVA [93], Felson definió como condiciones o criterios que reflejan la adecuación del objetivo para el delito: el valor del objetivo del crimen, su inercia, la visibilidad física del mismo y su accesibilidad [94]. La diferencia estriba en que previamente a todo ello,

---

[90] Así, además de los citados, el de Marcum, C. D., «Adolescent online victimization and Constructs of Routine Activities theory», en Jaishankar, K. (ed.), *Cyber Criminology. Exploring Internet crimes and criminal behavior,* Boca Ratón, CRC Press, 2011, p. 269.

[91] Wolak, J.; Finkelhor, D.; Mitchell, K. J., e Ybarra, M. L., «Online "Predators..."», *op. cit.,* p. 112.

[92] *Ibid.,* p. 114.

[93] Correspondiente a *Value of crime target, the Inertia of crime target, the physical Visibility of crime target, Accessibility of crime target* (VIVA). Felson, M., *Crime and everyday life,* 2.ª ed., Thousand Oaks, CA: Pine Forge Press, 1998, pp. 54 y ss.

[94] Esto lo ha hecho con profundidad, aunque a mi parecer no con total acierto, Yar, M., «The novelty of "cybercrime"...», *op. cit.,* pp. 419 y ss. Posteriormente también relaciona el VIVA con los objetivos del ciberespacio Choi, K., «Computer Crime...», *op. cit.*, p. 312.

la introducción del objeto por parte de la propia víctima en el ciberespacio es condición primera y principal para su adecuación al cibercrimen.

Ahora bien ¿y los demás caracteres del acrónimo VIVA? ¿Son válidos para el cibercrimen? Trataré a continuación de analizar cada uno de ellos para, en el caso de que los mismos no sean suficientemente expresivos y definitorios de la distinta capacidad de adecuación de los objetivos, sustituir el acrónimo VIVA por otro más apropiado al nuevo ámbito de intercomunicación social en el que se puede producir el delito.

Pues bien, el primer elemento a analizar es el del valor del objetivo. Independientemente del tipo de objetivo de que se trate (patrimonial, intimidad, libertad sexual, etc.), en el ciberespacio se da la particularidad de que cosas con poco valor por sí mismas pueden adquirir un valor muy importante gracias a la facilidad para obtener información, relacionarla con la obtenida y convertirla en un objeto de riesgo. Así, cuatro dígitos parecen no ser valiosos, pero si a ellos, por medio de la minería de datos, se asocia el concepto «*pin*», y se relaciona con un determinado usuario, y si después se hace lo mismo con los números de una cuenta bancaria, etc., finalmente tales números acaban por tener mucho valor. En todo caso, es evidente que a mayor valor del objetivo, mayor es la posibilidad de ataque [95], y esto será igual en el ciberespacio: los números de 20 dígitos son más buscados que los de 40, y las empresas más valiosas serán más buscadas por sus secretos comerciales que las no conocidas, por poner un ejemplo, y el cibercriminal decidirá según el valor que él mismo otorgue al objetivo.

Es más discutible, por el contrario, que los restantes elementos del acrónimo VIVA sean válidos para la fórmula de la adecuación de los objetivos en el ciberespacio. Comenzando por la inercia, Felson la definía como las propiedades intrínsecas de los objetivos que pueden hacer que la misma ofrezca distinto grado de resistencia al ataque [96]. Sin entrar en la discusión sobre la difícil separación entre inercia y accesibilidad, lo cierto es que en el ciberespacio los objetivos ofrecerán generalmente poca resistencia, ya que se trata de bienes informacionales que pueden ser descargados fácilmente sin resistencia alguna. Yar ha tratado de mantener el elemento al considerar que lo anterior no implica que no haya inercia de los bienes en el ciberespacio, pues una reflexión más profunda muestra que incluso la información conserva las propiedades de inercia en algún grado, en relación, por ejemplo, con el volumen de los datos (cuanto mayor sea, mayor es la dificultad de la descarga) o el sistema informático utilizado [97]. A mi parecer, el intento de Yar es vano. La evolución actual de las TIC contradice lo que afirma, y salvo en singulares casos excepcionales los bienes en el ciberespacio apenas se dife-

---

[95] FELSON, M., *Crime and..., op. cit.,* p. 55.
[96] *Ibid.,* pp. 55 y s.
[97] YAR, M., «The novelty of "cybercrime"...», *op. cit.,* p. 420.

renciarán entre sí por sus mayores o menores condiciones intrínsecas (y no relacionadas con los guardianes, tema distinto), esto es, por la denominada inercia, para ser adecuados a recibir un ataque.

Algo similar ocurre con la accesibilidad, definida por Felson como la habilidad de un agresor para contactar con un objetivo y llevárselo de la escena del crimen [98]. Como se puede comprender, dada la contracción de la distancia en el ciberespacio, todos los objetivos que entren en el ciberespacio son, en ese sentido, accesibles. Puede haber, como ha señalado Yar, observación del delincuente por medio de sistemas de rastreo o de señalización [99], pero eso no convierte al objetivo en menos adecuado, sino al gestor del lugar (o al guardián si deviene de la propia víctima el sistema e impide el ataque) en más eficaz. Si a ello unimos que, en realidad, esta característica está más asociada al agresor que a las particularidades del objetivo, podemos afirmar que la misma no es condicionante de la adecuación de un objeto en el cibercrimen.

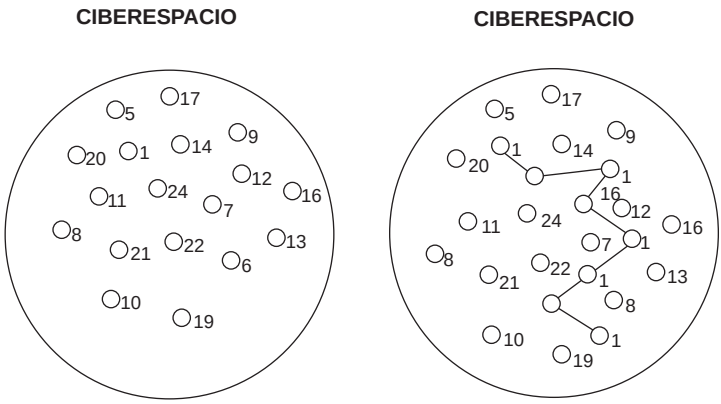
Cuestión similar, pero no idéntica, es la que Felson denomina visibilidad del objetivo, dado que si algo no es percibido por el agresor no puede ser blanco suyo [100]. Señala Yar que es esencia del ciberespacio su carácter público, por lo que todo en él está visible a nivel mundial [101]. A mi parecer, esto sólo es así parcialmente. Es indudable que la entrada en el ciberespacio conlleva la irrupción en un espacio público, pero eso no significa que se sea «visible», pues puede ocurrir que alguien acceda a Internet y nadie, excepto quienes le proveen el acceso, se aperciba de ello. El ciberespacio es tan ingente y tan universal, que es difícil hacerse visible, hasta el punto de que todos los usuarios conforman una maraña en la que es difícil distinguir a unos y otros. Hay algo, sin embargo, que hace visibles a los sujetos en el ciberespacio, su interacción con otros sujetos y con otros servicios. La interactividad sí es la esencia de Internet, y a mayor interacción con otros agentes, con diferentes páginas web, con variados servicios, mayor posibilidad de ser percibido (ser visible) por parte de otros.

La relación entre la mayor interacción de un sujeto en el ciberespacio con la probabilidad de ser victimizado podría darse por probada a partir de varios de los estudios empíricos de victimización en el ciberespacio. Así, adelantando algunas de las cuestiones que se estudiarán con mayor profundidad en el apartado victimológico [102], Alshalan [103] logra relacionar la victimización por virus informáticos por una parte, y por otra por cibercrímenes tales como el ciberfraude en sus múltiples formas, *identity theft*, *phishing*, fraudes de seguridad, *cyberstalking*, *cyberharassment*, extorsión y *hacking* [104],

---

[98] Felson, M., *Crime and..., op. cit.,* p. 58.
[99] Yar, M., «The novelty of "cybercrime"...», *op. cit.,* p. 421.
[100] Felson, M., *Crime and..., op. cit.,* p. 56.
[101] Yar, M., «The novelty of "cybercrime"...», *op. cit.,* p. 420.
[102] Véase *infra* cap. V.
[103] Alshalan, A., *Cyber-Crime Fear..., op. cit.,* p. 123.
[104] *Ibid.,* pp. 47 y ss.

Gráficos 3.16 y 3.17. Visualización de objetivos en el ciberespacio e interacción. Los objetivos se diluyen en el ciberespacio (3.16), pero el objetivo 1 se hace más visible cuando interacciona y se mueve por Internet (3.17). Elaboración propia.



con la interacción de la víctima en el ciberespacio concretada en su frecuencia de acceso y el tiempo pasado en Internet. En efecto, a partir de la hipótesis de que el comportamiento de la víctima en el ciberespacio es un importante predictor de su victimización, Alshalan concluye por medio de este estudio empírico de regresiones logísticas que a mayor frecuencia de acceso a Internet, mayor riesgo de victimización; y lo mismo sucede con el mayor tiempo conectado en el ciberespacio, así como con la realización de actividades en Internet que conllevan la divulgación de datos personales de tipo financiero [105] y, exclusivamente para la infección por virus, con el hecho de tener hijos que acceden al ciberespacio [106]. Por su parte, Yucedal, quien examina los factores que inciden en la victimización por conductas de *spyware* y *adware* a partir de los presupuestos de las citadas teorías, concluye que el comportamiento cotidiano en relación con el uso de Internet es un elemento determinante de la victimización por estos delitos que exigen, generalmente, que sea el propio sujeto el que al visitar una determinada web o al descar-

[105] *Ibid.,* p. 126.

[106] En efecto, tener hijos resulta un factor determinante del riesgo de victimización por infección de virus, pero no para el resto de la cibercriminalidad. ALSHALAN (*ibid.,* p. 127), plantea dos posibles explicaciones al fenómeno: la primera, que los niños desconozcan las amenazas potenciales de algunos sitios web y, por eso, se descarguen archivos con virus. La segunda, apoyada por la TAC, sería que cuando los encuestados contestan que tienen niños con acceso a Internet, quieren decir que lo utilizan, por lo que la frecuencia y duración de la utilización de Internet aumentaría. Quizás sea en realidad una mezcla de ambas: los menores utilizan Internet y, además, realizan muchas más actividades en el ciberespacio que los adultos. En todo caso, todas las explicaciones certificarían la tesis de que a mayor interacción en el ciberespacio, mayor adecuación del objetivo.

garse un programa cargue involuntariamente el virus [107]. Finalmente, Choi realiza una interesante identificación entre los comportamientos cotidianos en Internet y la teoría de los estilos de vida y la utilización de sistemas de protección con varios tópicos relacionados con la TAC [108]. También por medio de un estudio empírico de ecuaciones estructurales para la evaluación de la relevancia de variables como el estilo de vida en Internet y la utilización de sistemas informáticos de protección, Choi llega a la conclusión, después confirmada por Yucedal, relativa a que el *hacking* es más factible en personas con ordenadores personales que utilizan mucho Internet y que realizan conductas de riesgo en línea [109].

Y esto es así con otro tipo de cibercrímenes. Así, en un estudio de Ybarra y Mitchell, se relaciona de forma significativa el uso frecuente de Internet o el uso de salas de chat con una mayor exposición a la pornografía por parte de menores de edad [110], y ya hemos visto anteriormente que también había una intensa relación entre la interacción de la víctima en chats y demás con la victimizacion por *online grooming* o delitos similares.

En el ciberespacio, por tanto, a mayor interacción de un sujeto, plasmada en mayor tiempo en línea o mayor variedad de actividades en Internet (descarga de archivos, entrada en plataformas P2P, realización de compras en línea, creación de perfiles en redes sociales, etc.), mayor aptitud para ser objetivo adecuado. Es obvio que esto debe ser precisado y concretado de forma empírica y diferenciando cada una de las actividades. Pero también lo es que sólo con la interacción se producirá el contacto (necesario para el delito) en el vasto ciberespacio entre el agresor motivado y la víctima, dependiendo también su producción de que ésta «se mueva» por Internet, especialmente si recordamos que muchos de los ataques en Internet quedan estáticos a la espera de que sea la propia víctima la que al entrar en la página o descargar el archivo se convierta con su conducta en objetivo adecuado.

Podemos concluir, pues, que las condiciones para la adecuación del objetivo del crimen VIVA no son transportables al ciberespacio [111], excepto

---

[107] La medición del estilo de vida como determinante del riesgo de victimización lo realiza Yucedal a partir de un modelo de medida de dos factores consistentes en la realización de actividades *online* básicas o de ocio. En las actividades básicas se incluyen comportamientos relativamente seguros (en relación con la infección por *adware* o *spyware*) realizados en Internet, tales como la lectura de correos electrónicos, crear o leer blogs, o la compra *online*; mientras que en las actividades *online* de ocio se incluyen conductas más peligrosas, como la descarga de música, de vídeos o de programas que pueden contener *software* de este tipo o el juego *online.* YUCEDAL, B., «Victimization in...», *op. cit.,* pp. 113 y ss.

[108] CHOI, K., «Computer Crime...», *op. cit.,* p. 321.

[109] *Ibid.,* p. 321. Frente a la forma de medición de Yucedal, la variable del estilo de vida *online* es medida por medio de tres variables distintas: actividades vocacionales y de ocio, actividades de ocio peligrosas, y actividades vocacionales de riesgo.

[110] YBARRA, M. L., y MITCHELL, K., «Exposure to Internet Pornography among Children and Adolescents: A National Survey», en *CpB,* vol. 8, núm. 5, 2005, pp. 473 y ss.

[111] Lo admite, aunque mucho más tenuemente y tratando finalmente de incorporar las condiciones a la ecuación, Yar, al no poder sino reconocer que las variables inercia, visualización y

en el caso del «Valor». Éste deberá sumarse a la primera y esencial condición, y es que el objetivo haya sido «Introducido» en el espacio virtual. A ellos deberá sumarse la «Interacción» del titular del objeto en el ciberespacio como esencial condicionante de la victimización. Sumando las tres nos quedaría el acrónimo IVI, como definitorio de las condiciones que determinarán que una persona o alguno de sus bienes pueda ser objetivo adecuado de un cibercrimen: que el bien o la persona haya sido introducido en el ciberespacio; que tenga un valor que lo haga apetecible para el cibercriminal; y que la persona con la titularidad del bien interaccione en Internet de forma que se haga en él visible y pueda contactar con el agresor motivado. Es hora de analizar otros factores del evento criminal en el ciberespacio.

3.2.3. *Guardianes capaces y gestores del lugar «ciberespacio»*

No podemos finalizar esta abstracción teórica para la revisión del crimen en el nuevo ámbito de oportunidad criminal que es el ciberespacio sin analizar la incidencia del mismo, con sus caracteres intrínsecos y extrínsecos, con el otro factor de la ecuación del delito conforme a la definición de la TAC de Cohen y Felson. Me refiero a la ausencia del guardián capaz, sin la cual no hay delito, y que en el ciberespacio también ve ampliado sus límites, esto es, disminuye la capacidad potencial del guardián de evitar el crimen. La unión de los factores que hemos analizado, la compresión espacio-temporal para la comunicación entre personas, la popularización y el nivel transnacional de dicho ámbito, etc., dificultan en el ciberespacio la actuación del guardián (que debe ser) capaz de proteger a la víctima, lo cual, a su vez, interacciona con el factor agresor motivado al percibir tal reducción de obstáculos y disminuir la percepción de riesgo de ser cazado que va a tener el (ciber) criminal. En otros términos, la transnacionalidad puede incidir en una disminución de la eficacia de los elementos de protección de la víctima frente al ofensor capaz y dispuesto, con el consiguiente riesgo de victimización que supone la inexistencia de mecanismos de tutela [112], y al mismo tiempo puede ayudar a que el criminal se motive hacia la comisión del delito al percibir como compleja y alejada su identificación, la persecución judicial del mismo y los efectos negativos que de ello se derivarían [113].

---

accesibilidad «presentan una considerable divergencia entre su valor en el mundo real y el virtual». YAR, M., «The novelty of "cybercrime"...», *op. cit,* pp. 407 y ss.

[112] También destacan la relación entre la victimización en el cibercrimen y la ausencia de un *capable guardian* físico, GRABOSKY, P., y SMITH, R., «Telecommunication fraud...», *op. cit.* p. 37, aunque más que referirse a los medios institucionales, se refieren a los sistemas de protección físicos, tales como antivirus, etcétera.

[113] En sentido similar, pero no aludiendo específicamente a la transnacionalidad, sino a la dificultad de identificación de los criminales en Internet y a la posibilidad de que ello motive la realización de cibercrímenes, YAR, M., «The novelty of "cybercrime"...», *op. cit.,* pp. 407-427.

Como señalaron Farrell y Pease, la noción de guardián capaz se convierte en importante, pero también compleja, cuando pensamos en el cibercrimen [114]. Quizá en este sentido, sea más útil la diferenciación entre el mánager o gestor del lugar y el guardián que opera directamente sobre la víctima o el objetivo potencial, conforme a la segunda versión del triángulo del delito. La ausencia de mecanismos centrales de concesión de los servicios de Internet, así como de sistemas de control formal supranacional que tomen decisiones relativas a los servicios que estén por encima de las legislaciones estatales, conlleva la imposibilidad de unos «gestores centralizados» que vigilen el ciberespacio de forma global, y así, protejan a las potenciales víctimas [115]. No es que no haya policía en Internet, ni que no haya gestores de sitios en algunos de ellos, sino que los mismos están muy focalizados y su ámbito de incidencia es muy reducido. No obstante, es indudable que en determinados sitios web como las redes sociales los gestores pueden y deben funcionar tutelando la interacción de los usuarios de las mismas. Tales dificultades de gestión de un lugar tan vasto, por otra parte, son perfectamente conocidas por los usuarios de Internet, que perciben que «navegar por el ciberespacio» es una actividad en la que la intervención de los medios de control formal está mucho más diluida.

Distintos a los gestores del lugar son, en el triángulo del delito, los guardianes de los objetivos adecuados. Éstos lo pueden ser cualesquiera otros sistemas personales o no, ajenos a la propia víctima o impuestos por ella misma, que sirvan como forma de protección. Como han señalado Bossler y Holt, al igual que los sistemas de seguridad físicos, tales como alarmas, cerrojos especiales, etc. se han mostrado eficaces frente a la criminalidad, también pueden serlo aquellos otros que ejercen la misma función en el ciberespacio, tales como los antivirus o cualesquiera otros sistemas de seguridad [116].

Los estudios empíricos demuestran que tales sistemas pueden ser muy eficaces para evitar la victimización por el cibercrimen. Así, Yucedal constata que el uso de instrumentos digitales de seguridad, tales como cortafuegos, antivirus o programas *antispyware* como guardianes capaces, determina el riesgo de victimización [117], y a las mismas conclusiones llega Choi respecto al que él considera elemento esencial de la TAC [118].

Pero se trata, en todo caso y a mi parecer, de unos guardianes capaces íntimamente ligados con el elemento objetivo adecuado: no son sistemas

---

[114] Farrell, G., y Pease, K., «Criminology and Security», en Gill, M. (ed.), *The Handbook of Security,* Perpetuity Press, 2005.

[115] Así, también, Yar, M., «The novelty of "cybercrime"...», *op. cit.,* pp. 407-427.

[116] Holt, T. J., y Bossler, A. M., «On-line Activities...», *op. cit.,* pp. 1 y ss.

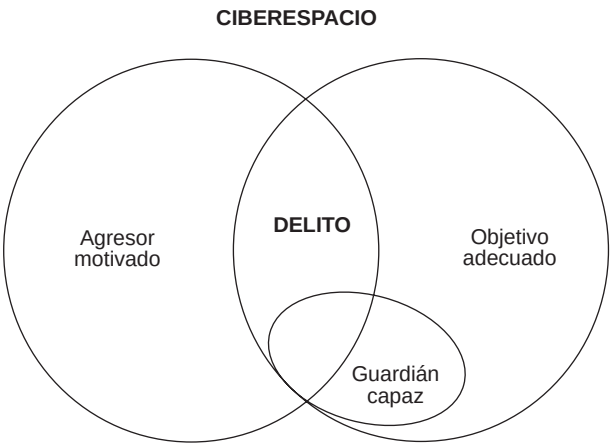
[117] Yucedal, B., «Victimization in...», *op. cit.,* pp. 117 y ss. En el caso de la incorporación de sistemas de autoprotección, el estudio utiliza como variables la tenencia de cortafuegos y de antivirus.

[118] Choi, K., «Computer Crime...», *op. cit.*, p. 321.

de protección incorporados o que funcionen de forma autónoma al comportamiento del propio sujeto al que protegen, sino que, por el contrario, todos los elementos de protección citados dependen de la propia víctima para su funcionamiento y actualización. Los que Cohen y Felson definían como guardianes capaces, generalmente eran cercanos a la víctima (vecinos, ciudadanos anónimos, etc.) [119], pero no «parte de ella», como sí lo es el *software* que la víctima pone en su ordenador. En el caso del ciberespacio es la propia víctima, y por tanto el propio objetivo, el que debe incorporar sus guardianes capaces.

Lo relevante, en todo caso, no es situar los antivirus, cortafuegos y demás en el lado del triángulo del objetivo adecuado o de la ausencia de guardián capaz, sino reconocer que en la conjunción de estos elementos, y por tanto, en la propia prevención del delito, la víctima juega un papel preponderante en el caso del cibercrimen, dado que de ella depende en parte, no sólo su adecuación como objetivo (las dos íes, Introducción e Interacción), sino también su propia autoprotección, pues será ella la que defina los guardianes capaces que la protegerán al tener sistemas antivirus, al actualizarlos, al incorporar otros sistemas de detección de *software* de riesgo, al actualizar el sistema siempre que se pueda, etc. El guardián capaz, en el ciberespacio, es prácticamente un autoguardián que depende de la propia víctima.

Gráfico 3.18. Triángulo del cibercrimen. El guardián capaz depende del propio objetivo, pues apenas hay guardianes externos, por lo que el efecto reductor del delito es menor. Elaboración propia.



[119] COHEN, L., y FELSON, M., «Social change...», *op. cit.,* p. 590; y también FELSON, M., *Crime and..., op. cit.*, p. 53.

Es cierto que los sistemas de autoprotección impuestos por la víctima no son los únicos que pueden desarrollar su eficacia en relación con los cibercrímenes. En otros delitos dirigidos contra menores pueden ser interesantes otros vigilantes capaces como son el control familiar sobre la actividad en Internet, la creación de perfiles específicos que impidan el acceso a determinados recursos web, etc. A ello deberán sumarse, en el futuro, medios de control y protección institucional, dado que la seguridad en el ciberespacio, como ha señalado Grabosky, exige una intervención y esfuerzo plural de instituciones y usuarios [120]. En todo caso esto parece más lejano. Ante la inexistencia actual de formas de control formal más institucionalizadas, como las fuerzas policiales, cuya función preventiva (que no la reactiva) parece imposible en el ciberespacio, la autodefensa sigue siendo, frente a estos crímenes, como quizás también frente a los otros, la mejor forma de protección [121].

Por último, merece la pena destacar que el hecho de que las TIC estén en constante evolución y que los usos sociales y comerciales del ciberespacio, vigentes hoy, no tengan por qué ser los del mañana, también tiene consecuencias en términos de oportunidad delictiva, muy especialmente en relación con la «capacidad» del agresor y en la «incapacidad» del guardián y de la propia víctima para asegurar su propia defensa. Así, la evolución permanente del ciberespacio, de sus tecnologías y sus servicios, complica la eficacia de los protectores, que son capaces para los riesgos que conocen, pero no para los nuevos, y tanto en relación con la aparición de nuevos medios de ataque a objetivos adecuados tradicionales, como en el propio surgimiento de nuevas oportunidades correspondientes a nuevos bienes aparecidos a la luz de las nuevas relaciones sociales en el ciberespacio. En cuanto a lo primero, es obvio que la rapidez con la que evoluciona la tecnología hace enormemente compleja la eficacia de los mecanismos de control y protección de los intereses socialmente esenciales. La actualización de los instrumentos y herramientas de los criminales va a ser aún mayor en el ciberespacio que en la criminalidad física que, de hecho, está aprovechándose ya de las TIC para mejorar en eficacia y eficiencia. Además, el carácter abierto del ciberespacio, el hecho de que sean los propios usuarios los que puedan hacer evolucionar el mismo, conlleva la posibilidad, para los que tengan grandes conocimientos informáticos, de cambiar protocolos y usos para su propio interés, que también puede ser criminal. Por otra parte, y en segundo lugar, esta misma mutación constante de las TIC y de la interacción social con las mismas, conlleva la aparición de nuevos intereses sociales o de nuevas dimensiones de valor de los existentes que, precisamente por no existir o no expresarse previamente de la forma en que lo hacen ahora, tampoco pueden ser convenientemente protegidos.

---

[120] Grabosky, P., «Virtual Criminality:...», *op. cit.,* p. 248.
[121] *Ibid.*

4. OPORTUNIDAD DELICTIVA EN EL CIBERESPACIO Y PREVENCIÓN DEL CIBERCRIMEN

4.1. La importancia de la víctima en el evento «cibercrimen»

Si bien hemos insistido en que lo relevante en el delito como evento no es cada uno de los elementos del mismo tanto como su confluencia, ésta, cuando se produce en el ciberespacio, parece reflejar un mayor protagonismo, no frente a los otros elementos pero sí frente a la que tiene generalmente en el espacio físico, del objetivo o víctima del delito. Generalmente el elemento central para la visión y comprensión del crimen es el agresor, dado que en su motivación está también definido el objetivo sobre el que se producirá el ataque y las condiciones de defensa que tiene el mismo. Esto podría hacer pensar que el agresor elige completamente a su víctima independientemente del actuar de ésta y que, para ella, el serlo es algo aleatorio (*the random fallacy*) [122]. Pero si eso no es así en el espacio físico, aún parece serlo menos en la cibercriminalidad. Son muchos los ciberataques que se realizan en el ciberespacio sin un objetivo determinado, siendo el concreto interactuar de la víctima el que la convierte en objetivo adecuado y no la voluntad del cibercriminal, y esto es así porque el ciberespacio es un ámbito de oportunidad nuevo (distinto).

La principal diferencia de la «botella» del crimen en el ciberespacio es que debido a que el mismo es un ámbito comunicativo vasto e inmenso, sin barreras ni dimensiones, en el que el contacto depende de las voluntades de interacción entre sujetos de modo tal que sin interacción de los dos no habrá contacto por más que uno quiera, el agresor ya no es el único y principal que define, desde su intención, el ámbito de riesgo [123]. Lo hace, sin duda, al actuar con una voluntad criminal, pero lo hará únicamente sobre aquel objeto (para él valioso) que esté en el ciberespacio, que interaccione con él y que no esté protegido, todo lo cual convierte a la víctima en un elemento explicativo (a posteriori) del evento delictivo muy expresivo.

En efecto, a mi parecer, son tres los factores que hacen que la víctima adquiera una especial importancia para la explicación y prevención del delito en el ciberespacio. El primero, y como se ha visto, es que la víctima potencial del ciberdelito tiene, en primer lugar, gran capacidad para dejar fuera del ámbito de riesgo aquello que no quiere que se vea afectado por el mismo: ella misma determina, desde un primer momento, al incorporar determinados bienes y esferas de su personalidad al ciberespacio, los márgenes genéricos del ámbito de riesgo al que va a estar sometida. Si no entra en el

---

[122] FELSON, M., y BOBA, R., *Crime and everyday..., op. cit.,* p. 21.

[123] Obviamente, tampoco lo era antes de forma absoluta, pero intuitivamente, y como posteriormente se explicará parece que la víctima es ahora más protagonista que en el espacio físico.

ciberespacio o no tiene relaciones personales allí, tales bienes no podrán ser afectados, al igual que no lo podrá ser su patrimonio si no utiliza la banca electrónica y no comunica sus claves en Internet. Podría decirse que esto es idéntico a que si la víctima no sale a la calle no puede ser víctima de robos en ella. Pero seguirían pudiendo robarla (matarla o violarla) yendo a su domicilio, lo cual no es posible en Internet si la víctima no introduce en él los bienes de que se trate. Al fin y al cabo en el ciberespacio no está la persona sino una expresión suya por ella misma elegida.

En segundo lugar la víctima define con su interacción en el ciberespacio el grado de visualización de sus objetivos y, por tanto, las posibilidades de contacto con un agresor motivado en un mismo tiempo y espacio o en otro distinto. Existen estudios que demuestran la especial importancia del comportamiento de la víctima en la victimización por la cibercriminalidad informática. Así, Alshalan [124] logra relacionar la victimización con la interacción de la víctima en el ciberespacio, y en el mismo sentido se sitúan los analizados estudios de Yucedal y Choi. Todos ellos vienen a confirmar algo que ya habíamos afirmado: que la víctima define el ámbito de riesgo al que puede acceder el agresor motivado. Podría argumentarse que esto no es más que lo que sucede en el espacio físico con el aumento de las posibilidades de sufrir delitos en el caso de visitar determinados lugares, hacerlo en determinados períodos del día, etc. Ciertamente es similar, pues se basa en que las actividades cotidianas de la víctima son parte de la explicación del evento criminal. La única diferencia es que en el ciberespacio no es necesario tiempo ni distancia física para la interacción, y que la misma en Internet depende por igual de todos los agentes, de modo que una vez hay una conducta criminal iniciada el que la misma afecte a uno, dos, cientos o miles de personas dependerá mucho de lo que hagan éstas. También cambia que mientras que ya hemos identificado en el espacio físico, y para determinado tipo de delitos, las conductas que pueden resultar peligrosas, aún no nos hemos preguntado todavía sobre cuáles son los comportamientos de riesgo en Internet, y es indudable que resultará esencial hacerlo de cara a la prevención de este tipo de criminalidad.

Por último, y en tercer lugar, la víctima va a ser prácticamente la única que puede incorporar guardianes capaces para su autoprotección. Al no existir en este ámbito criminológico distancias físicas ni guardianes formales institucionalizados, el uso cotidiano que haga de las TIC y en especial la incorporación (o no) de sistemas digitales de autoprotección serán determinantes a la hora de convertirse en víctima del cibercrimen. Si tenemos en cuenta, además, que en Internet, también al no existir distancias, el desplazamiento del cibercriminal hacia otros objetivos resulta, no sólo sencillo, sino incluso en muchos casos (virus y demás) instantáneo, y que la dirección del nuevo objeto del ataque la marcará la ausencia de sistemas de protección

[124] ALSHALAN, A., *Cyber-Crime Fear..., op. cit.,* p. 123.

o las vulnerabilidades del objetivo (entonces adecuado), parece evidente concluir el protagonismo de la víctima en su proceso de autoprotección y, en caso de carecer de ésta, de victimización. Claro que la víctima también influye en la capacidad de sus guardianes en el espacio físico, pero si bien no se venden casas sin puertas o pisos en una urbanización sin vecinos, sí que se venden sistemas informáticos con acceso a redes sin antivirus o sin actualización de los mismos, así como redes sociales y demás lugares de comunicación social sin información sobre los riesgos de su uso.

Evidentemente, no son los condicionantes derivados de la TAC los únicos que inciden en la cibervictimización. Los estudios analizados ponen de manifiesto que hay factores demográficos también relevantes a la hora de la mayor o menor victimización: en los realizados en Estados Unidos se confirma que las personas de raza blanca tienen un mayor riesgo de victimización, y lo mismo ocurre en general con los varones frente a las mujeres [125], lo cual, por otra parte, y de nuevo acercándonos a la TAC, se corresponde con la frecuencia de uso de Internet y la duración del tiempo pasado en el ciberespacio, que son mayores en los varones, como se muestra en la tabla basada en el estudio de Alshalan [126]. Es cierto, sin embargo, que la diferencia entre el tiempo de uso de Internet entre hombres y mujeres no es estadísticamente significativa, por lo que quizás debiera tenerse en cuenta el tipo de actividad cotidiana *online* que realizan los hombres (especialmente en cuanto a descarga de archivos o actividad de comercio electrónico), frente a la que realizan las mujeres, para entender el mayor riesgo de victimización del hombre [127]. También está generalmente admitido que el tiempo de uso en Internet es significativamente mayor en los usuarios jóvenes frente a los más mayores. Concretamente en el estudio de Pratt *et al.,* sobre victimización por ciberfraude, se señala que por cada unidad en la que se incrementa la edad, disminuye en tres unidades porcentuales el tiempo pasado en el ciberespacio durante la semana [128]. Puede decirse, por tanto, que hay un mayor riesgo de victimización en el ciberespacio para los jóvenes, si bien de nuevo ello puede estar derivado del estilo de vida de los mismos, concretamente de las horas que suelen pasar en Internet.

Y es que el análisis comparado de los estudios revisados nos lleva a la conclusión, como también a los autores que los han desarrollado, de

---

[125] *Ibid.,* p. 146.

[126] *Ibid.,* p. 83.

[127] También puede ser relevante el factor miedo al delito, que es mayor en mujeres que en hombres, conforme al propio estudio de Alshalan (Alshalan, A., *Cyber-CrimeFear..., op. cit.,* pp. 145 y ss.), aunque son menos susceptibles de ser victimizadas. Sería interesante analizar en qué medida el miedo al delito, condiciona las actividades concretas realizadas por las mujeres frente a los hombres en el ciberespacio.

[128] Pratt, T. C.; Holtfreter, K., y Reisig, M. D., «Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory», en *Journal of Research in Crime and Delinquency,* vol. 47, núm. 3, 2010.

que los factores demográficos son menos relevantes que las actividades cotidianas en Internet llevadas a cabo por las víctimas. Así lo demuestran los estudios empíricos conforme a los cuales, cuando se incluyen las variables derivadas de la teoría de las actividades cotidianas, se eliminarán los efectos de la edad, la educación y otros sobre la victimización por cibercrímenes [129].

Todo lo anterior se resumiría, por tanto, en la afirmación de que la falacia del crimen azaroso que constata Felson y conforme a la cual la gente cree, erróneamente, que el delito sucede independientemente de lo que se haga y de cómo se actúe, como una desgracia ajena a su comportamiento, se manifiesta de forma más expresiva en el ciberespacio [130]. Qué duda cabe de que lo afirmado tiene importantes consecuencias prácticas a efectos preventivos: si la conducta de la víctima va a ser un determinante especialmente significativo del delito, también será por ello un importante condicionante para su prevención. La educación de la víctima en seguridad informática, su concienciación para la adopción de *software* de protección y de rutinas seguras en su actuar cotidiano en el ciberespacio, así como la información real sobre los riesgos en el ciberespacio, serían los primeros pasos a adoptar para la prevención del cibercrimen.

4.2. De las actividades cotidianas a la prevención (situacional) del cibercrimen

Generalmente, se alude a la diferenciación entre los mecanismos de prevención del delito de tipo estructural, psicológico y circunstancial [131], según se atienda respectivamente a las consideraciones económicas, sociales y políticas que condicionan la delincuencia, a los elementos conductuales y cognitivos relacionados con el sujeto que puede llevar a cabo el crimen, o a las circunstancias sociales y físicas en las que tiene lugar el crimen. Habiendo adoptado hasta el momento para la explicación del ámbito de oportunidad criminal que es el ciberespacio la perspectiva de la teoría de las actividades cotidianas, es claro que serán estos dos últimos tipos de elementos los que centren nuestra atención, y de ellos es lógico comenzar, siguiendo el hilo anterior, por la extraordinaria relevancia que va a desempeñar la conducta de la víctima en el evento cibercrimen. Siendo estrictos diríamos que es idéntica a la de los demás factores: si no hay agresor motivado o hay guardián capacitado no habrá delito *online*, independientemente de lo que haga la víctima o el titular del «objetivo adecuado». Pero dado que hay pocos gestores del sitio

[129] Alshalan, A., *Cyber-Crime Fear..., op. cit.,* p. 146. En el mismo sentido, Pratt, T. C.; Holtfreter, K., y Reisig, M. D., «Routine Online...», *op. cit.,* p. 267.

[130] Felson, M., y Boba, R., *Crime and everyday..., op. cit.,* p. 21.

[131] Pease, K., «Crime Prevention»..., *op. cit.,* p. 964.

así como guardianes capaces en Internet y que la compresión de la distancia sitúa en un mismo plano a miles de potenciales agresores motivados, parece obvio que la conducta de la víctima determina significativamente el riesgo criminal al que estará sometida. Lo hará desde el momento de su entrada en el ciberespacio, con la selección de los bienes patrimoniales y relacionados con la privacidad, contenidos en su sistema informático y que entran en ese espacio de riesgo nuevo; también al elegir el tipo de actividades que realiza en Internet (sociales, personales, económicas) y al decidir los lugares que visita, los contactos personales que realiza, los archivos que descarga, y, muy especialmente, los medios tecnológicos (*software* antivirus, *firewalls* y demás sistemas de protección y de detección de accesos no autorizados, de la entrada de *software* malicioso y de demás ataques; pero también los sistemas de control parental, etc.) que incorpora a su sistema informático como auto-guardianes para la protección de sus datos y demás. En otras palabras, la víctima define, con su conducta, el ámbito de oportunidad delictiva, y si esto es así en general, en el ciberespacio, donde apenas existen guardianes capaces y donde el contacto con terceros exige de una definición, en esencia activa, de la propia representación que va a relacionarse con otras personas, de los medios de protección (autoguardianes capaces), aún lo será más.

Dice Pease que la teoría de la prevención de la delincuencia se ocupa de comprender los mecanismos que causan el evento criminal, siendo la cuestión central el cómo lograr perturbarlos [132]. A mi parecer, es esencial comprender que el cibercrimen como evento tiene mucho que ver con las decisiones que adopta la víctima en su día a día, con sus actividades cotidianas y con la (escasa) percepción del riesgo de las mismas. El objetivo debe ser, por tanto, mejorar su protección como forma de, en términos de prevención situacional, aumentar el esfuerzo necesario para la realización del delito.

Comenzando por lo primero, y como se verá con más profundidad posteriormente cuando se analicen los factores relacionados con la victimización por cibercrímenes, existe una íntima relación entre ésta y el estilo de vida en relación con Internet (número de horas en Internet, tipo de seguridad utilizada, etc.) de las víctimas de *grooming* o *phishing* [133]. La falta de educación en materia de seguridad informática, la inexistencia de unos usos sociales por todos aceptados relativos a la utilización segura de los sistemas y las redes informáticas, puede ser comprensible dada la novedad de las TIC y de los cambios sociales asociados a ellas, pero es factor determinante del incremento de la cibercriminalidad. Dejando a un margen la cibercriminalidad política, especialmente el *hacktivismo,* en el que el objetivo adecuado es prácticamente independiente del comportamiento de la víctima, tanto en la cibercriminalidad social como en la económica es usual la presencia de

[132] PEASE, K., «Crime Prevention...», *op. cit.,* pp. 963 y ss.
[133] Cap. V.

una conducta de quien recibe el ataque sin la cual el mismo difícilmente se hubiera producido. Tal conducta puede ser activa, como la respuesta a un correo de *phishing*, el envío de datos personales a un desconocido, la captación de imágenes propias a través de una *webcam* o del teléfono móvil o la utilización de un sistema de pago no seguro en Internet; o pasiva, como la no utilización de dispositivos de protección (antivirus, detección de *spyware* y cortafuegos), e incluso la aceptación de la propia desinformación en materia de seguridad sobre sistemas y redes telemáticas. Esto último quizás tenga que ver con la escasa percepción sobre los riesgos existentes en el ciberespacio, lo cual se correspondería con las conclusiones de un estudio llevado a cabo por Vozmediano, San Juan y Vergara [134], en el que se comprueba el escaso miedo de las personas al ciberdelito frente al miedo a otros crímenes cuya probabilidad de comisión sobre la víctima es claramente inferior [135].

Hay que tener en cuenta, además, que esta utilización insegura de las redes y los sistemas informáticos no sólo es un riesgo para los bienes e intereses de la víctima, sino que lo es para la propia seguridad del ciberespacio. La interconexión de sistemas en el ciberespacio conlleva que el ataque a uno de ellos implique también el riesgo para los demás. Esto se hace particularmente patente en los casos de infecciones de *malware*: la inseguridad de un sistema, del que siempre es en parte responsable la víctima, produce un inmediato riesgo para muchos otros, más en la actualidad con la infección de *bots* que conlleva la creación de *botnets* para el futuro envío de *spam* con intenciones de *phishing* o de nueva infección de *malware* o para la realización de ataques distribuidos de denegación de servicio que complican enormemente la defensa por parte del atacado. Es claro que en muchos casos es la pericia del *hacker* la que permite el éxito del ataque, pero como se verá después al analizar el perfil del cibercriminal, hoy tal logro se debe más bien al descubrimiento de vulnerabilidades y, por tanto, al aprovechamiento de las deficiencias de seguridad debidas a la víctima que a la especialización tecnológica de algunos sujetos que pueden realizar grandes daños con escasos conocimientos de informática.

Admitida, pues, como primera conclusión la extraordinaria relevancia de la conducta de la víctima en relación con la cibercriminalidad, su corolario es la necesidad de perturbar las facilidades que la víctima suele poner para el delito en el ciberespacio, en aras de reducir este tipo de delincuencia. La prevención de la cibercriminalidad, pues, requerirá la adopción de medidas

---

[134] Vozmediano, L.; San Juan, C., y Vergara, A. I., «Problemas de medición del miedo al delito: algunas respuestas teóricas y técnicas», en *Revista Electrónica de Ciencia Penal y Criminología,* 2008. En Internet, en *http://criminet.ugr.es/recpc/10/recpc10-07.pdf.*

[135] Explican y desarrollan algo más esta paradoja De la Cuesta Arzamendi, J. L., y San Juan Guillem, C., «La cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad», en De la Cuesta Arzamendi, J. L. (dir.), y De la Mata Barranco, N. J. (coord.), *Derecho penal informático, op. cit.,* pp. 73 y ss.

que permitan a la víctima convertirse en su propio guardián capaz y, a la vez, evitar la realización de las conductas que facilitan la ejecución del delito. Aumentar su formación para una mejor autoprotección y para la adopción de rutinas seguras, potenciar la utilización de sistemas de auto protección que eviten riesgos no deseados, e incluso enseñar a limitar los bienes personales y patrimoniales que pone en contacto con el ciberespacio, deberían ser objetivos político-preventivos básicos en relación con la cibercriminalidad.

Obviamente, la víctima no es el único elemento que debe tomarse en cuenta para la prevención del cibercrimen. Sin entrar en una perspectiva preventiva estructural, y antes de analizar la prevención psicológica ocupándonos del cibercriminal, podemos plantearnos en el seno de la perspectiva circunstancial la posibilidad de implantación de guardianes capaces en el ciberespacio. Lo primero que conviene aclarar al respecto, y en coherencia con lo que he señalado anteriormente, no me estoy refiriendo a aquellos sistemas tecnológicos de protección incorporados al sistema de la víctima. En contra de lo que señala Choi, para quien los tres tipos más comunes de *digital-capable guardianship* serían los programas antivirus, los programas *antispyware* y los programas cortafuegos [136], considero que tales elementos forman parte más bien del s*uitable target*, en este caso de la víctima de los ataques que los incorpora como sistemas de protección del bien que pretende defender. En todo caso, y dejando de lado estas consideraciones terminológicas sobre si es adecuado situar tales sistemas de seguridad en una u otra categoría, lo que me interesa plantear ahora es la posibilidad de incorporar sistemas de protección ajenos a la propia víctima que velen por la seguridad en el ciberespacio. Obviamente la desregulación y descentralización del ciberespacio, el propio hecho de que Internet no pertenezca a ninguna autoridad estatal ni supranacional, dificulta la existencia de organismos de vigilancia institucional, dejando de lado que su propia existencia, en el caso de que fuera posible, podría «chocar» en parte con la filosofía «sin barreras» de Internet. Podría haberlos impuestos por cada uno de los Estados, pero obviamente carecerían de legitimidad de intervención en la mayoría de las ocasiones, y también de eficacia en un espacio transnacional universalizado como ése.

Aun así, existen experiencias de vigilancia de la criminalidad en el ciberespacio, sobre todo en relación con la transmisión de contenidos ilícitos o nocivos, y tanto a nivel institucional-estatal como por parte de ONG, que tratan de identificar las webs desde las que se cometen los cibercrímenes para después denunciar tales conductas o incluso impedir su éxito de diferentes formas. En el caso de las ONG su actividad se ha relacionado muy especialmente con la persecución de las webs dedicadas a la difusión de pornografía infantil. Generalmente, por medio de la denuncia de tales pági-

[136] Choi, K., «Computer Crime Victimization...», *op. cit.*

nas web, pero también *hackeándolas* o infectándolas de virus para dañar sus recursos o tratar de identificar a sus usuarios y proveedores [137].

Más interesante resulta, en todo caso, la posibilidad de trasladar al ciberespacio los sistemas de prevención comunitaria informal, o en otras palabras, el vecindario vigilante o cualquier otra forma de control informal o «vigilancia natural» en Internet. En principio, esto parece extremadamente complejo en el ciberespacio, por donde los sujetos navegan de forma individualizada, sin contacto con terceros que puedan advertir de peligros a la potencial víctima. Sin embargo, ello podría estar cambiando gracias a la implantación de la web 2.0, de los blogs y foros en los que se informa sobre pautas de seguridad a los usuarios de Internet, pero muy

[137] A finales de los años noventa del siglo XX comenzaron a surgir, en España, fundaciones sin ánimo de lucro cuyo objetivo era combatir la pornografía infantil, ya que España es el segundo país del mundo con más visitas a estas webs. Las ONG facilitan a las autoridades el mayor número de informaciones verificables para la eliminación de páginas de pornografía infantil y la localización de sus autores. También desarrollan trabajos de prevención. Una de ellas es Alia2 (*www.alia2.org*), la cual trabaja conjuntamente con instituciones públicas (Ministerios de Educación, de Industria, de Turismo y Comercio; Oficina del Defensor del Menor de la Comunidad de Madrid, Grupo de Delitos Telemáticos de la Guardia Civil y la Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía) y privadas. Alia2 crea y potencia el uso de herramientas informáticas, como *Carolina*: filtro de control, defensa y denuncia de descargas digitales relacionadas con la pornografía infantil; *Danba*: herramienta que permite a los padres conocer los hábitos de navegación de sus hijos*; Germán*: aplicación informática de análisis, coordinación de esfuerzos e intercambio de información entre las Fuerzas y Cuerpos de Seguridad; *Florencia*: solución informática que rastrea las redes de intercambio de archivos o P2P; *Araña*: *software* entregado a la Guardia Civil para realizar análisis de discos de forma automatizada. También la Asociación Contra la Pornografía Infantil (*www.asociacion-acpi.org*), es miembro de la European Federation for Missing and Sexually Exploited Children, miembro del Inhope europeo y de la ECPAT [Red Internacional de Organizaciones Contra la Explotación Sexual Comercial Infantil (*www.ecpat.net*)]. La Asociación Catalana para la Infancia Maltratada, a través de ECPAT España, es la representación oficial en España de la Red ECPAT Internacional. Tiene el apoyo del Ministerio de Trabajo y Asuntos Sociales, el Ministerio de Asuntos Exteriores y de Cooperación y el Ayuntamiento de Barcelona. En 2001, unos piratas informáticos británicos crearon el virus Noped que ataca a los archivos susceptibles de ser imágenes pornográficas de niños. El virus se transmite a través de un correo: *«Help us to end ilegal child porn now»*. Una vez activado en el PC, el Noped busca en el disco duro los archivos de imágenes cuyos nombres puedan indicar que sus contenidos son imágenes pornográficas de menores. Tras detectarlos, el código malicioso envía un correo desde el ordenador del propietario a la policía. Por otro lado, hace unos años, una estudiante de ingeniería informática llamada Katiuska Santos, comenzó una campaña contra la pornografía infantil, difundiendo información sobre los servidores que publicaban pornografía infantil, y amenazaba a sus *webmasters* de infectarlos de por vida con un programa que destruiría la información de los discos duros y de los de sus visitantes. Google también desarrolló un *software* que puede detectar y eliminar pornografía infantil desde Internet. El programa lo está usando la organización británica NCMEC (National Centre for Missing and Exploited Children). En 2010 unos investigadores españoles crearon un prototipo (Baby Bot) basado en un robot que se expresa como un menor y crea señuelos para atrapar a los pedófilos en la Red. En la actualidad, el director de la Asociación Nacional para la Protección Infantil de Estados Unidos (National Association for Child Protection U.S.), ha acudido a unos científicos para utilizar un nuevo equipo muy veloz (Jaguar). Además han desarrollado una serie de algoritmos que comprueban el tráfico P2P, de forma que detectan en muy poco tiempo las búsquedas sobre pornografía infantil, y determinan cuantas direcciones IP responden a la consulta.

especialmente de las propias redes sociales que podrían convertirse en los vecindarios del futuro en los que el círculo más íntimo de amigos puede vigilar los contactos y comportamientos peligrosos de la potencial víctima. En efecto, el funcionamiento de redes como Twitter, Myspace, y muy especialmente en España Tuenti y Facebook, que permiten agregar amigos y compañeros creando redes de personas en un contexto en el que el sujeto acaba pasando gran parte del tiempo que dedica a Internet, puede ayudar a la prevención de cierto tipo de criminalidad social advirtiendo a la víctima de los riesgos que corre en relación con su actividad. También en esta línea podría citarse la propuesta planteada por Jones de utilizar las posibilidades que brinda la utilización del «*open source software*» para la modificación de los códigos fuente de los programas informáticos como modo de lograr sustituir el control policial reactivo frente al cibercrimen por una vigilancia de los propios usuarios de la Red al estilo del «*community policing model*» [138].

Junto a ello, y como forma de prevención paralela y separable [139] a las anteriormente analizadas, debe prestarse atención al último de los elementos que conforman la oportunidad delictiva y que estamos analizando siguiendo los presupuestos de las actividades cotidianas: el agresor motivado. En relación con él la perspectiva preventiva adoptada es obviamente la psicológica-motivacional: sabiendo de las características del ámbito de oportunidad criminal que es el ciberespacio se trata de analizar cómo puede influirse en su decisión para que finalmente no cometa el delito. Entramos aquí de lleno, pues, en el enfoque de la prevención situacional, partiendo como presupuesto de la teoría de la elección racional, esto es, de la idea de que la conducta delictiva deriva de un proceso racional de toma de decisiones en el que el sujeto actúa con una determinada finalidad eligiendo entre las opciones que tiene [140]. La existencia de una oportunidad criminal, por tanto, ayudará al criminal a tomar la decisión de cometer el delito, mientras que su reducción lo prevendrá. Una forma esencial, pues, de prevenir la conducta del

---

[138] JONES, B. R., «Comment: Virtual...», *op. cit.*, pp. 615 y ss. Destaca el autor las enormes ventajas que ofrece *Linux* y otros sistemas de *software* libre para la lucha frente a la cibercriminalidad, dado que se descentraliza la detección de riesgos y la aplicación de parches para la mejora de la seguridad de los sistemas. Aun así me parece algo forzada la comparación entre la utilización de este tipo de *software,* incluso en el caso de que se popularizara su uso en Internet, con los modelos de la vigilancia comunitaria, entre otras cuestiones porque en estos modelos la clave no es tanto las herramientas, sino la propia constitución de una comunidad de autoprotección que acerca más la cuestión a la comentada posibilidad de utilización de las redes sociales en este sentido. Cuestión distinta es que luego todos los usuarios que formaran esa comunidad utilizaran tal o cual sistema de *software*.

[139] CLARKE, R. V. (ed.), *Situational crime prevention. Successful Case Studies,* New York, Guilderland, Harrow and Heston Publishers, 1997 (2.ª ed.), pp. 25 y ss.

[140] Sobre la idea del crimen como comportamiento instrumental orientado a la consecución de necesidades básicas del delincuente, véase CORNISH, D. V., y CLARKE, R. V., *The reasoning Criminal...*, *op. cit.*

potencial cibercriminal, consiste, siguiendo la hipótesis básica de Clarke, en modificar el ámbito de oportunidad para modificar su percepción e incidir en su conducta, concretamente incrementando lo que percibe que le puede costar lograr su objetivo; aumentando el riesgo percibido de que al hacerlo sea capturado (en términos judiciales), y reduciendo los beneficios que valore que podrá obtener de su actividad, logrando así que no lleve a cabo la conducta.

Aplicado a lo que nos interesa, a la cibercriminalidad y su prevención, lo primero que podríamos afirmar es que todas las anteriormente analizadas medidas de prevención de la delincuencia en Internet, las centradas en la actividad de la víctima y en la incorporación de guardianes capaces en el ciberespacio, tendrán su influencia en la decisión del cibercriminal, especialmente en lo relativo a la valoración del esfuerzo que va a tener que realizar para cometer el delito. La utilización de medidas de protección tecnológica por parte de la víctima, o la existencia de sistemas de vigilancia y demás, serán tomados en consideración por parte del agresor potencial, desincentivando una primera decisión de cometer el ataque en el ciberespacio. Por el contrario, la inexistencia de estas medidas de tutela convierte a la víctima en objetivo adecuado contra el que es sencillo perpetrar el ataque y en objeto de preferencia por parte del cibercriminal. También es importante desde esta perspectiva la percepción de la ganancia que se obtendrá de la actividad criminal, lo cual parte de la idea anteriormente comentada relativa a que el delito tiene un carácter instrumental, en el sentido de que responde a la voluntad de consecución de objetivos básicos de los delincuentes tales como dinero, sexo, estatus y aventura [141]. Como se ha visto al explicar el ámbito de oportunidad criminal que es el ciberespacio, existe en él un aumento potencial significativo de las posibilidades de contacto entre agresor motivado y víctima debido a la destrucción de la distancia física como obstáculo para la comunicación directa entre personas y el acceso a los bienes. Precisamente por ello, y como analizaremos con algo más de profundidad después, medidas tendentes a la ocultación de objetivos y demás formas de minimización de las posibles ganancias o recompensas que el agresor percibirá que puede obtener.

Volvemos de nuevo, pues, casi inevitablemente, a concluir sobre la importancia de las medidas de autoprotección que incorpore el usuario para evitar ser víctima en el ciberespacio: las mismas no sólo reducirán, en términos objetivos, las posibilidades de éxito del cibercriminal, sino que influirán en la percepción por parte de éste de las dificultades de lograr su objetivo e incidirán, muy probablemente, en el desplazamiento de sus actos criminales hacia otro objetivo «menos protegido».

---

[141] Recuerda Medina Ariza ésta como una de las argumentaciones básicas del enfoque de la prevención situacional, MEDINA ARIZA, J. J., «El control social del delito...», *op. cit.,* p. 286.

También tienen que ver con la motivación del agresor para la comisión del cibercrimen, otros dos conjuntos de técnicas de prevención situacional, las medidas relativas al incremento del riesgo percibido y las tendentes a incrementar la vergüenza o culpabilidad del delincuente. Las he dejado a ambas para el final dada la especial complejidad que conllevará la implantación de medidas preventivas frente al cibercrimen de este tipo en el ámbito del ciberespacio. Al fin y al cabo, tanto una como otra percepción-valoración subjetiva, la de las posibilidades de «ser cazado» con las consecuencias que ello conlleva y la relacionadas con los sentimientos de culpabilidad y vergüenza derivados de la realización de una conducta desvalorada popularmente o a nivel de ética individual, van a ser generalmente bajas en el ciberespacio. La razón es distinta en cada una de ellas.

En el caso de la percepción del cibercriminal del riesgo de ser identificado y detenido, y como ya se ha adelantado anteriormente y explicado con profundidad, el ciberespacio es un ámbito que, además de que permite que se oculte la existencia de delito o de sus efectos durante mucho tiempo, favorece, por una parte, el anonimato de quien lleva a cabo la infracción criminal, siendo sencilla la realización de ataques desde sistemas informáticos remotos y, sobre todo, aun siendo posible la identificación de las direcciones IP, muy compleja la identificación personal de la persona (o una de ellas, dada la realización general de actividades colaborativas en el seno de organizaciones criminales) que estaba llevando a cabo la conducta delictiva; y por otra, permite la realización de los delitos desde otros Estados, con la consiguiente complejidad, añadida a la previa de la identificación, de la posterior persecución judicial de estas infracciones y para la final detención, enjuiciamiento y sanción del cibercriminal. Aun así resulta necesario plantear la posibilidad de aumentar la percepción de inseguridad del cibercriminal, lo cual debería pasar por incrementar el número de guardianes, por facilitar la identificación de los usuarios y demás medidas que serán concretadas en el punto posterior. Obviamente, junto a las medidas específicas que señalaremos destacan por el poderoso efecto que podrían tener otras más de tipo estructural, en cuanto que afectan a la propia construcción del sistema jurídico a nivel mundial o al funcionamiento de Internet, como serían la implantación de un sistema de jurisdicción universal de los delitos, la modificación de la Red para su configuración centralizada o para la total identificación de cada uno de sus usuarios, etc. No parecen estas medidas, sin embargo, y por distintos motivos complejos de explicar pero en el fondo obvios, realistas en el mundo actual en el que vivimos en el que los Estados-nación siguen siendo un pilar básico de la estructura mundial y en el que el ciberespacio libre y descentralizado representa tantos beneficios que resulta difícil (y poco recomendable) imaginar una modificación en cualquiera de los sentidos señalados. Es cierto, en todo caso, que estos dos tipos de medidas orientan sobre cuál sería el camino a seguir en aras a los objetivos pretendidos señalados: por una

parte la armonización de la justicia y la cooperación judicial para aumentar la vigencia de la ley, su eficacia y, por ende, la percepción de sus efectos por los que la infringen; y por otra el establecimiento de sistemas tecnológicos, sociales o jurídicos que, sin negar los principios básicos del ciberespacio tal y como está actualmente configurado, sí facilitaran la identificación de aquellos que lo utilicen para hacer daño a los demás y atentar contra los intereses de la mayoría.

En cuanto a la potenciación de los sentimientos de culpabilidad asociados a la realización del comportamiento criminal, tampoco es el ciberespacio un ámbito en el que vaya a ser esta tarea sencilla, sobre todo en relación con algunas conductas criminales que, pese a serlo, están prácticamente aceptadas como adecuadas por parte de los usuarios que acceden regularmente a la Red. Es lo que ocurre muy especialmente con los delitos contra la propiedad intelectual, infracciones que se realizan casi de forma generalizada por millones de personas en todo el mundo que acceden a Internet para intercambiar archivos no siempre de forma lícita y que, sin embargo, lo hacen sin la culpa que puede venir asociada a otro tipo de infracciones patrimoniales. También sucede esto en relación con otros ataques asociados al *hacktivismo* y, en general, a gran parte de las conductas enmarcadas dentro de la ética *hacker*. Así, algunos ataques de denegación de servicio, intromisiones no autorizadas a sistemas informáticos ajenos, o incluso infecciones de *malware*, concretamente aquellas llevadas a cabo con una finalidad política o ideológica, difícilmente podrán ser prevenidas apelando a la ilegalidad de las mismas cuando el que las lleva a cabo no percibe la legitimidad de tales normas [142].

De poco servirá, pues, la aprobación de leyes contra algunas de las conductas que afectan a la seguridad de los sistemas y las redes en el ciberespacio si no se hace una labor de concienciación de la gravedad de estas conductas para esos bienes jurídicos.

---

[142] Sobre la influencia de la valoración de legitimidad de la norma que lleve a cabo el sujeto con la realización de su conducta, es especialmente revelador el trabajo de TYLER, T., *Why People Obey the Law*, Princeton, Princeton University Press, 2009, pp. 1 y ss., en el que señala que el comportamiento desde una perspectiva instrumental está modelado por los incentivos y castigos tras el cumplimiento o incumplimiento de la norma, por ejemplo, en la medida en que se incremente la certeza y severidad del castigo la norma tendrá un mayor grado de cumplimiento. Para Tyler, el legislador cuando construye una ley adopta implícitamente una perspectiva instrumental. Sin embargo, existe otra perspectiva, la normativa, aquella en la que se percibe la norma como justa y moral, incluso aunque sea opuesta a los propios intereses, asumiendo su cumplimiento de manera voluntaria, independientemente del riesgo de castigo. Desde esta perspectiva, los ciudadanos perciben que las autoridades están legitimadas y por tanto, la probabilidad de incumplir la ley es menor. Por otra parte, desde el punto de vista de las autoridades, el cumplimiento voluntario de la norma presenta grandes ventajas. Si es necesario hacer cumplir las leyes resulta imprescindible recurrir a la Policía y a los jueces, será necesario emplear la fuerza e invertir grandes recursos. El cumplimiento voluntario tiene un costo mucho menor y en consecuencia, aumenta la valoración de los gobernantes y la legitimidad de la norma.

4.3. La prevención del cibercrimen y el enfoque situacional

4.3.1. *Medidas concretas para la prevención del cibercrimen desde el enfoque «situacional»*

Puede parecer extraño hacer referencia a la prevención situacional del crimen en el ciberespacio, sobre todo si se identifica este enfoque únicamente con la modificación del ambiente físico, del espacio geográfico en el que se produce el evento criminal. No lo es tanto si lo interpretamos como lo que es: un modelo de prevención del delito que, frente a las tradicionales teorías de la criminalidad que se interesan por las razones que llevan a las personas a convertirse en delincuentes, pone el énfasis en la importancia de los factores ambientales, es decir, en la existencia de lugares y momentos que propician la concentración de los delitos, lo que permite la intervención en el ámbito de oportunidad para reducirla y evitar que el criminal motivado pueda cometer el delito. Es obvio que el ciberespacio es también ambiente; concretamente es un nuevo ámbito de oportunidad criminal y por eso es adecuado acercarse al crimen que se desarrolla en dicho nuevo espacio desde el enfoque que parte de la premisa de que las características del lugar donde se produce el delito condicionan el mismo y, por ello, de que puede intervenirse en ellas para prevenir su realización.

Conviene matizar, sin embargo, que esto no significa que creamos que debe ser éste el enfoque único desde el que debe centralizarse las políticas de prevención del crimen en el ciberespacio. La utilización aquí de esta perspectiva criminológica para la recomendación de medidas preventivas frente a la cibercriminalidad ni supone dejar de lado cualesquiera otras perspectivas más centradas en lo estructural ni tampoco la consideración de que este enfoque es el adecuado y central que debe tomarse en materia de prevención del delito. Sí es cierto, sin embargo, que pese a lo que pudiera parecer en un primer momento debido a la inexistencia de distancias físicas en Internet, el ciberespacio como ámbito de oportunidad criminal aparece como uno especialmente apto para este enfoque, quizás simplemente porque la cibercriminalidad dista, generalmente, de ser una criminalidad impulsiva, en la que la razón o el cálculo de la decisión ceda ante otro tipo de elementos cognitivos. Si bien es cierto que va a ser un tipo de delincuencia llevada a cabo generalmente por gente joven, pues es la población que más utiliza Internet y las TIC, y que en ella hay siempre impulsividad, la criminalidad realizada en Internet generalmente es pensada y meditada por quien la lleva a cabo. No se trata de un tipo de crimen que se ejecute normalmente como respuesta a algún tipo de impulso o estrés, sino que los cibercrímenes económicos, también los políticos y la mayor parte de los cibercrímenes sociales, aunque muy especialmente los primeros que son el grueso de la delincuencia en Internet, se concretan en conductas llevadas a cabo de forma razonada, desde

la seguridad y tranquilidad que da el estar en el propio domicilio o en el lugar de trabajo, alejado a miles de kilómetros de distancia en muchos casos del espacio físico en el que se van a desplegar los efectos de la conducta. Es lógico, siendo esto así, que el autor haga cálculos racionales, que seleccione los objetivos contra los que se dirige, que valore el esfuerzo que va a tener que hacer, que analice los beneficios que puede obtener de su conducta y los riesgos que asume, tomando en consideración por tanto las condiciones ambientales en las que se va a producir el delito, las condiciones de protección de la víctima, la existencia de guardianes capaces, etc. Al fin y al cabo no hay que olvidar que el objetivo de las medidas de prevención situacional no es tanto el hacer imposible para el agresor motivado la realización del delito, sino influir en su decisión, en la valoración de costes-riesgos-beneficios que realiza en el momento antes de ejecutar o no el crimen [143].

A lo señalado hay que sumar otro elemento que hace que sea especialmente adecuado el enfoque situacional al ámbito de oportunidad que estamos analizando: el que el ciberespacio sea un ambiente «en construcción». Por mucho que Internet funcione ya como un sistema totalmente definido, es obvio que aún son muchos los elementos del mismo, no tanto como ente tecnológico (que también) sino especialmente como ámbito de intercomunicación social, que están cambiando permanentemente, en una suerte de evolución infinita derivada de los distintos intereses sociales que van surgiendo conforme el mismo va siendo descubierto funcionalmente por la sociedad. Precisamente por ello las posibilidades para modificar el ambiente con una finalidad de prevención de la criminalidad son altas. Sería muy recomendable, en definitiva, integrar el enfoque de la prevención situacional en las políticas de seguridad relacionadas con los sistemas de la sociedad de la información, incorporando las medidas necesarias para evitar los comportamientos delictivos que niegan su seguridad y ponen en riesgo su utilidad social y su eficacia.

Vamos a ocuparnos a continuación, por tanto, de las medidas de prevención situacional que pueden adoptarse para la prevención de la cibercriminalidad. Aunque ya se han propuesto aquí algunas de ellas, partiendo de la comprensión del nuevo ámbito de riesgo que es el ciberespacio desde las bases de la teoría de las actividades cotidianas y entrando incluso en el enfoque situacional, trataremos a continuación de concretarlas aún más y de sistematizarlas desde el enfoque de la prevención situacional. El objetivo es doble: por una parte identificar nuevas formas de prevención del cibercrimen a partir de las reglas de prevención situacional propuestas por los

---

[143] En este sentido recuerda Tilley el cambio que se produce en la exposición por Clarke de las técnicas de prevención del crimen, especialmente en lo referido a las tres grandes categorías que se denominaban «aumentar el esfuerzo», «aumentar el riesgo», y «disminuir las ganancias», cuando fueron enunciadas por Clarke en 1992, y pasaron a ser en 1997 sustituidas respectivamente por «aumentar el esfuerzo percibido», «aumentar el riesgo percibido» y «disminuir las ganancias percibidas». TILLEY, N., *Crime Prevention*, *op. cit.,* p. 111.

defensores de este enfoque criminológico, concretando la específica forma en que tales medidas pensadas para el espacio físico deben manifestarse para la prevención del crimen en el ciberespacio; por otra, aprovecharnos de la sistematización del enfoque situacional para una mejor definición de las políticas preventivas a adoptar frente al crimen en el ciberespacio.

Se trata, en última instancia, de pensar en las medidas de prevención de la delincuencia en Internet desde la idea del cibercriminal como sujeto racional que toma decisiones teniendo en cuenta el ambiente de oportunidad en el que actúa. Partiré, por tanto, de las categorías generales aceptadas por Cornish y Clarke, e incluso de la filosofía preventiva que hay detrás de cada una de estas medidas, pero buscando su referente o equivalente para el ámbito de oportunidad que es el ciberespacio.

En la última elaboración de Cornish y Clarke [144] se identifican cinco categorías y se proponen veinticinco medidas de prevención situacional [145].

Tabla 3.2. Veinticinco medidas de prevención situacional de Cornish y Clarke.

Aumentar el esfuerzo	*Aumentar el riesgo*	*Disminuir las ganancias*	*Reducir provocaciones*	*Eliminar excusas*
Entorpecer objetivos	Aumentar el número de guardianes	Ocultar objetivos	Reducir frustraciones/ estrés	Establecer reglas
Controlar accesos	Facilitar la vigilancia	Desplazar objetivos	Evitar disputas	Fijar instrucciones
Controlar salidas	Reducción del anonimato	Identificar la propiedad	Reducir la excitación emocional	Alertar la conciencia
Desviar trasgresores	Introducir «gestores» de sitios	Trastornar los mercados delictivos	Neutralizar la presión del grupo de referencia	Asistir la conformidad
Controlar facilitadores	Reforzar la vigilancia formal	Eliminar beneficios	Disuadir imitaciones	Controlar las drogas y el alcohol

[144] CORNISH, D. V., y CLARKE, R. V., «Opportunities, precipitator and criminal decisions: A reply to Wortley's critique of situational crime prevention», en SMITH, M., y CORNISH, D. B. (coords.), «Theory for Practice in Situational Crime Prevention», en *CPS,* vol. 16, New York, Monsey, Criminal Justice Press, 2003.

[145] Asumiendo la traducción de SUMERS, L., «Las técnicas de prevención situacional del delito aplicadas a la delincuencia juvenil», en *Revista de Derecho Penal y Criminología,* 2009, pp. 395-409.

Entrando en la caracterización general de la prevención situacional aplicada al ciberespacio, creo que se puede comenzar por dos modificaciones generales: la supresión de una categoría y la inclusión de una nueva. A mi parecer podemos, en primer lugar, prescindir de la categoría general referida a la reducción de provocaciones. La reducción de frustraciones y estrés, evitar disputas, reducir la excitación emocional, neutralizar la presión del grupo de referencia o disuadir imitaciones son medidas de carácter emocional que dada la despersonalización de Internet y su ámbito de incidencia, tienen difícil encaje en una delincuencia fundamentalmente tecnificada, cuyos objetivos han sido determinados y abordados en la mayoría de las ocasiones tras seguir una planificación elaborada y sin una conexión física ni emocional con la víctima. Es cierto que hay algunas formas de cibercriminalidad social para las que, probablemente, pudieran ser útiles estas medidas: ciberacoso, *grooming*, *sexting*, amenazas por medio de Internet, calumnias, etc. Pero, cuando sea así, serán válidas entonces las medidas tal y como son definidas en el enfoque situacional tradicional. Se trata, en definitiva, de una categoría que, al menos en cuanto a rasgos generales, no aporta nada a la prevención en el ciberespacio ni siquiera adaptando sus medidas al nuevo ámbito de oportunidad criminal.

En segundo lugar, y dada la especial significación que, como hemos visto de forma reiterada, va a conllevar la intervención de la víctima en la configuración del delito, proponemos la creación de una nueva categoría que incluya las medidas creadas para la reducción, por parte de la víctima, de la esfera de influencia potencial del ciberdelincuente y su conducta, tanto en el sentido de la disminución de los objetos sobre los que puede realizarse la acción criminal, como en el de reducir los efectos lesivos del mismo en el ciberespacio. Se trata de una categoría que guarda cierta relación con la referida a las ganancias percibidas como resultado del cibercrimen, pues en la medida en que se reduzca el número posible de objetivos, lo hará la percepción del sujeto de los beneficios del comportamiento criminal. Pero el plano es distinto: no se trata de llevar a cabo medidas que reduzcan la percepción de los beneficios que pueden ser obtenidos por el cibercriminal, sino más bien de, en un plano previo, llevar a cabo acciones que disminuyan los objetos disponibles para el cibercrimen y que impidan la propagación de sus efectos si éste se produce. Hay que tener en cuenta que en Internet va a ser generalmente la propia víctima la que, con su decisión y conducta se convierta en tal: en la actualidad para la infección de un virus suele ser necesario que la víctima descargue un archivo, el cual puede haber sido dejado en un determinado sitio por el cibercriminal esperando a que alguien llegue a él y se lo descargue. Siendo esto así es necesario que la prevención atienda a la perspectiva de la decisión de la víctima, pues será ella la que, en muchos casos, convierta o no en daño el riesgo creado por el ofensor motivado.

Por otra parte, también esta categoría tiene que ver con la dispersión del daño en el ciberespacio. Al fin y al cabo, veíamos anteriormente cómo

la contracción del espacio en Internet permitía la difusión de los daños derivados de cierto tipo de criminalidad viral en la que el receptor-víctima de la agresión se convertía, sin quererlo, en emisor de un nuevo ataque. Así las cosas, el objetivo de la prevención ya no deberá ser, únicamente, el evitar que el delito se cometa sino también que los efectos de éste se propaguen por el ciberespacio afectando no sólo al primer destinatario del ataque sino a muchos más.

Es obvio, en todo caso, que esta nueva categoría atendería en cuanto a la perspectiva preventiva más a lo circunstancial que a lo psicológico, y quizá, de ahí que la sitúe en una columna separada (tabla 3.3), no propia del enfoque situacional tradicional: no se trata tanto de influir en la decisión del cibercriminal como en reducir los efectos dañosos de su conducta previniendo minimizando aquello que puede ser afectado por sus ataques así como la contaminación a otros sistemas de los daños causados a uno determinado.

Sumando, pues, esta categoría a las más relacionadas con la (des)incentivación del agresor, sistematizándolas apoyándonos en la (modificada) categorización situacional, y reduciéndolas a cuatro medidas por categoría, nos quedaría un conjunto de veinte tipos de medidas de prevención situacional de la cibercriminalidad que quedaría como se ve en la tabla 3.3.

En la primera columna, la categoría que hemos denominado «reducción del ámbito de incidencia», incluiríamos medidas como la separación de los objetivos, centrada en la creación de ciberespacios cerrados y separados de la Red [146], la identificación de los riesgos (de contaminación), apoyada en campañas de información sobre los riesgos que implica la exposición a determinados ámbitos del ciberespacio (descargas ilegales de contenidos con derechos de autor, webs de pornografía, apoyo a grupos de ciberactivistas como el conocido Anonymous, etc.) que promoverían la autogestión del nivel de riesgo que cada uno está dispuesto a asumir, desde el conocimiento de las amenazas reales a las que se enfrenta. En todo caso quizá la categoría más significativa podría ser las medidas consistentes en la no introducción de objetivos. Desde la base, de nuevo, de la relevancia de la autoprotección en el ciberespacio, se trata de un conjunto de medidas que tratan de que el usuario, víctima potencial, no ponga a disposición de terceros bienes o información que mediante técnicas como la minería de datos pueden aportar a los

[146] Internet ya no es una red académica, los intereses comerciales y su utilización masiva por parte de empresas e instituciones han reducido considerablemente el ancho de banda destinado a la investigación, por ello universidades y centros de investigación han puesto en marcha diferentes proyectos, entre los que destaca Internet2, que pretende establecer un sistema alternativo a la Red, que apoyados en las nuevas tecnologías que permiten altas velocidades de transmisión de contenidos y funcionando independientemente del Internet comercial, permitan desarrollar una nueva generación de aplicaciones que se ejecuten del orden de 100 a 1.000 veces más rápido que las actuales y que faciliten la investigación y la educación. Véase Internet2 Consortium en *http://www.internet2.edu/*.

Tabla 3.3. Veinte tipos de medidas de prevención situacional de la cibercriminalidad. Elaboración propia.

Reducción del ámbito de incidencia [1]	*Aumentar el esfuerzo percibido*	*Aumentar el riesgo percibido*	*Disminuir las ganancias percibidas*	*Eliminar excusas*
No introducir objetivos Separación de discos duros con acceso y sin acceso al sistema; sistemas de control parental; filtros de contenido; controladores de seguridad ActiveX; no acceso a salas de chat *(grooming).*	**Controlar el acceso al sistema** *Firewall;* actualización de los sistemas operativos; claves de acceso al sistema; claves de acceso a las redes; renovación de claves; sistemas de perfiles en redes sociales.	**Aumentar el número de guardianes** Moderadores de foros; sistemas Echelon, Enfopol, Carnivore y Dark Web.	**Ocultar objetivos** Utilización de sistemas de encriptación; ocultar datos personales en redes sociales; no utilización de claves bancarias; perfeccionamiento sistemas e-comercio.	**Establecer reglas** Armonización internacional del Derecho; Netiquette.
Identificación de zonas de riesgo Campañas de información sobre riesgos; aviso en red de infección de *spam;* sistemas de listas blancas y negras de webs y *spam;* Identificación de *bots.*	**Detectar e impedir el ataque** Antivirus; *antispyware; antispam;* sistemas de control de banca electrónica.	**Reducción del anonimato** Identificar las IP; registro en foros web; sistemas de identificación del usuario [2]; identificación y autentificación biométrica.	**Desplazar objetivos** Discos duros extraíbles; sistemas de pago alternativos (PayPal); cambio de direcciones web, direcciones de dominio y demás.	**Fijar instrucciones** Avisos web de licencias: *copyright* y *copyleft;* avisos sobre privacidad en redes sociales.
Descontaminación/ limpieza de residuos Borrado y destrucción de virus latentes; desinfección de *bots.*	**Retirar transgresores**[3] Cierre de webs; solicitud de retirada de contenido ilícito; mecanismos de denuncia en redes sociales; cortar el acceso a una IP.	**Reforzar la vigilancia formal** Control de webs a través de *proxy;* equipos especializados de persecución del cibercrimen.	**Eliminar beneficios** Persecución a compradores de contenidos ilícitos; persecución del blanqueo capitales.	**Fortalecer la conciencia moral** Concienciación en materia de propiedad intelectual; reforzar moralmente los negocios lícitos.

Reducción del ámbito de incidencia[1]	*Aumentar el esfuerzo percibido*	*Aumentar el riesgo percibido*	*Disminuir las ganancias percibidas*	*Eliminar excusas*
Separación de objetivos Internet2, creación de sub-redes locales de seguridad.	**Controlar facilitadores** Obligaciones de vigilancia para IPPS; control de datos por RSS.	**Facilitar la vigilancia** Mejora de los sistemas de identificación de IP; reconstrucción de la arquitectura con fines defensivos.	**Trastornar los mercados delictivos** Ofrecer sistemas de intercambio de archivos económicos (Spotify y más); control de páginas de descarga directa de archivos.	**Facilitar la conformidad** Nuevos modelos de negocio (Apple); competiciones legales de *hackers*; fortalecimiento del *software* libre.

[1] La prevención situacional atiende a la decisión racional del sujeto. El individuo tiene en cuenta los objetivos que va a alcanzar como beneficios, pero es posible que se produzcan efectos distintos a los deseados al propio agresor.

[2] Véase en este sentido el proyecto para la creación de sistemas de identificación de usuarios «de confianza», propuesto por el gobierno de Estados Unidos. THE WHITE HOUSE: «National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy», draft, June 25, 2010, *http://www.dhs.gov/xlibrary/assets/ns_tic.pdf*, pp. 1 y ss.

[3] El término desviar, generalmente utilizado en la terminología de la prevención situacional, no parece aquí adecuado en cuanto parece implicar un desplazamiento de distancia física, y por eso he preferido referirme a la retirada de transgresores.

ciberdelincuentes información con la que organizar sus ciberataques, o bien impidiéndole a la propia víctima que descargue archivos que pueden estar infectados de virus (controladores de seguridad ActiveX) o que, mediante los distintos sistemas de filtrado de contenidos, acceda a webs en las que se difunde material peligroso, lo cual en el caso de los menores se concreta en las distintas formas de *software* de control parental. Finalmente, la descontaminación/limpieza de residuos impediría el crecimiento ilimitado de los peligros de Internet, que como una enfermedad supuestamente extinta que encontrase un nuevo portador, aumentase su virulencia extendiéndose en progresión geométrica.

La segunda columna incluye una categoría ya propia de la prevención situacional tal y como ha sido entendida tradicionalmente, como es la consistente en medidas que tratan de aumentar el esfuerzo percibido por el ofensor motivado. En el punto anterior, concretamente en el análisis de la prevención centrada en el «*motivated ofender*», ya hemos desarrollado la explicación de las posibilidades de las medidas preventivas enfocadas a incrementar el coste de esfuerzo que el cibercriminal va a percibir que tendrá que soportar al dirigir su conducta criminal contra un objetivo. Me limitaré simplemente a explicar, por tanto, las subcategorías adoptadas del modelo clásico y a concretar su aplicación en el ciberespacio.

Aunque generalmente se sitúa como primera de las medidas la de entorpecer objetivos, en la cibercriminalidad el primer obstáculo que puede percibir el potencial criminal es la dificultad para el acceso al sistema informático que va a atacar, siempre que éste sea imprescindible para llevar a cabo el ataque. En este sentido, y como ya hemos señalado reiteradamente, debe ser la víctima la que asuma la incorporación a su sistema de medios de autoprotección que impidan el acceso de otros como primer paso para dañar su equipo, adquirir información o demás conductas peligrosas. La configuración del sistema para la exigencia de una clave de acceso, sería en este sentido la primera exigencia básica para la autoprotección, sin olvidar tampoco la necesidad de que las propias redes telemáticas de acceso, concretamente las configuraciones *wifi* que se han generalizado en empresas y hogares, exijan también una clave para el acceso cuando la utilización de las mismas pretenda llevarse a cabo en un entorno de seguridad. Además es recomendable ir cambiando las claves de acceso y utilizar combinaciones complejas de cifras y dígitos que compliquen la averiguación de las mismas. También podríamos situar en esta categoría la utilización de cortafuegos, los dispositivos de *hardware* o *software* diseñados para impedir el acceso no autorizado a un sistema; e incluso la actualización de los sistemas operativos, que posibilita la corrección de vulnerabilidades en el sistema que permiten el acceso ilícito a los mismos. Todas estas medidas son especialmente eficaces frente a la cibercriminalidad económica centrada en la infección de virus, en el envío de *spam* y, en definitiva, en la tentativa de acceso al sistema para la recopilación de información en él para la posterior utilización ilícita de la misma. Junto a ellas también podemos situar como medidas de control de acceso los sistemas de definición de perfiles en las redes sociales, que permiten seleccionar las personas con las que se comparte determinada información.

Otro conjunto de medidas destinadas a aumentar la percepción del esfuerzo que va a tener que llevar a cabo el agresor son las que pretenden entorpecer el logro del objetivo pretendido por éste al permitir a la víctima detectar el ataque y, por tanto, impedir su perfeccionamiento. No se trata, como las otras medidas que hemos analizado en el primer bloque, de percibir la amenaza, sino de detectar que se está siendo víctima de un ciberataque y de impedir que el mismo acabe teniendo éxito. Para ello están todos los sistemas antivirus que intervienen una vez la infección se ha producido y que tratan de identificar la amenaza, bloquearla y finalmente eliminarla. En sentido similar actúan los programas *antispyware* frente al *software* que no infecta nuestro sistema pero trata de adquirir información valiosa (*keyloggers*, *sniffers* y demás) y que son bloqueados por este tipo de *software* defensivo. En cuanto al *antispam*, se trata de un tipo de *software* que filtra los correos electrónicos detectando la entrada de correos *spam* y ubicándolos en una carpeta aparte. Junto a estos tipos de *software* que se pueden instalar

en el propio sistema para la autoprotección, también hay otras formas de detección del ataque que tienen lugar cuando el mismo ya se ha producido contra el usuario pero aún no se ha perfeccionado por completo, pudiendo ser identificado por el vigilante-víctima para evitar que termine teniendo éxito. Es lo que ocurre con los sistemas de protección de la banca electrónica que vigilan no sólo el acceso a las cuentas sino, incluso, una vez se ha producido una transferencia, la legalidad de la misma antes de que el dinero sea definitivamente retirado.

No sólo con este tipo de medidas se puede aumentar el esfuerzo percibido, sino que tal objetivo también se puede lograr si el transgresor es retirado, aunque sea temporalmente, de modo que tenga que volver a empezar para perpetrar el ataque. Esto puede hacerse de distintas formas en el ciberespacio: cierre de páginas web por parte de las autoridades estatales competentes; solicitud de retirada de contenido ilícito como primer paso para el cierre de la web; mecanismos de denuncia en redes sociales que permiten que un contenido o una web sea retirado inmediatamente por el controlador de la red social, o cortando el acceso a una determinada IP identificada previamente como peligrosa.

Por último, el enfoque de la prevención situacional suele referirse a la utilidad, para la prevención del delito, que plantea el que los facilitadores del mismo, los elementos que hacen más sencilla la comisión del delito [147], sean controlados. En el ciberespacio los facilitadores generalmente son las propias víctimas que con su comportamiento poco diligente dan sus claves, cuentas, etc., permitiendo el posterior delito sobre ellas. Las medidas para evitar esto ya han sido incluidas en otra categoría, por lo que hay que referirse a otro tipo de facilitadores. Lo son, en el fondo, los prestadores de servicios de la sociedad de la información, cuyo control mediante la imposición de obligaciones de vigilancia puede constituir una eficaz medida preventiva; también lo son las redes sociales, que proveen de información personal a los cibercriminales siempre que no controlen bien el acceso a los datos personales de sus usuarios, lo cual nos obliga a exigirles una buena gestión de los datos en ellas contenidos, etcétera.

La tercera columna también ha sido desarrollada previamente. Se trata de las medidas que persiguen aumentar en el agresor la percepción de que su conducta entraña para él un riesgo, concretamente el de ser detenido. Como ya se dijo, éstas son las medidas más complejas de implantar en el ciberespacio, en el cual lo general es el anonimato del sujeto que interviene en él, pese a que sea posible, que no sencillo, identificar el sistema desde el que actúa. Las medidas concretas que podría proponerse en este sentido se ubicarían en cuatro bloques.

---

[147] Medina Ariza, J. J., «El control social del delito...», *op. cit.,* p. 292.

En el primero situaríamos todas aquellas medidas consistentes en aumentar el número de guardianes. No es el ciberespacio un ámbito en el que existan guardianes formales derivados de una autoridad centralizada, pero sí existen otro tipo de vigilantes en lugares concretos tales como las redes sociales o los foros de Internet, moderadores que actúan en ellos y que pueden vigilar la realización de expresiones injuriosas o de proposiciones sexuales y otras actividades de acoso. Junto a ello también existen otros sistemas de vigilancia cuya legitimidad, sin embargo, es más discutida. Se trata de aquellos sistemas de inteligencia tales como Echelon o su equivalente europeo Enfopol que, de forma no oficial, captan todas las transmisiones de información realizadas por medio de redes telemáticas con selección de términos y conceptos clave y que podrían estar violando la intimidad de las personas de forma flagrante [148].

El segundo bloque de medidas por medio de las cuales se podría tratar de aumentar la percepción de riesgo del cibercriminal son todas aquellas que tratan de reducir el anonimato con el que éste generalmente actúa. En la actualidad es bastante sencilla la identificación de direcciones IP, que puede desaconsejar la realización de comportamientos delictivos por parte de quienes ejecutan el hecho desde su propio domicilio o empresa, con su sistema informático, y en el mismo país en el que el delito va a desplegar sus efectos: la huella digital que dejan estas conductas facilitaría la identificación por parte de las brigadas tecnológicas de la policía o la guardia civil y llevarían a la detención del sujeto. La identificación de las direcciones IP, por el contrario, será de poca utilidad frente a la mayoría de los cibercrímenes económicos, los llevados a cabo por organizaciones criminales que o no tienen miedo a la identificación de la dirección IP real dado que con la misma tampoco sería posible posteriormente la identificación del usuario, o utilizan técnicas para esconder la dirección auténtica, o llevan a cabo el ataque tras una infección de *bot* y por medio de una *botnet* que hace prácticamente inútil la determinación de la dirección IP por parte de los investigadores. Precisamente por la escasa eficacia intimidatoria que conllevan los sistemas de identificación de las direcciones IP surgen otro tipo de propuestas para la reducción del anonimato como la que defiende la implantación de sistemas para la identificación de los usuarios que intervienen en el ciberespacio. Por medio del registro previo con la utilización de datos personales, lo que se pretende es garantizar la identidad real del sujeto que interacciona en el ciberespacio. No sería extraño que esto se implantase en un futuro cercano para actividades comerciales o incluso para otras actividades profesionales de tipo educativo y similares. De hecho, algo similar existe ya en algunas webs y redes internas que exigen a los usuarios una identificación con datos o claves personales en el ámbito institucional estatal, en el empresarial, educativo, social y demás. Obviamente la exigencia de identificación personal a través de medios como

[148] Sistemas Echelon, Enfopol, Carnivore y Dark Web.

la entrega de datos personales obligatorios y demás, supone un freno para el agresor motivado a la hora de cometer el delito y le llevará, generalmente, a «desplazarse» a lugares (para él) seguros en los que no le exijan identificarse para actuar. La contrapartida es, por tanto, que la exigencia de identificación supone para el que entra en estos sitios una garantía de que, a menos que se haya falseado la identidad, las personas con las que se relaciona también están identificadas, aumentando la sensación de seguridad y tranquilidad del usuario. Más sofisticada y lejana, pero no imposible dadas las experiencias existentes en otros medios, sería la implantación de sistemas de identificación y autentificación biométricos entre las que podrían estar el reconocimiento facial, el reconocimiento de huellas dactilares, el escáner de la geometría de la mano o el reconocimiento del iris, junto a otros sistemas de futuro como la comparación de ADN [149]. Hay que tener en cuenta, en todo caso, que tales sistemas requerirían de una aceptación para la primera identificación en el *enrolment process*, lo cual reduciría su ámbito de implantación, y que los cibercriminales también podrían tratar de engañar a esos sistemas precisamente en esa primera fase, creando una identidad falsa desde un primer momento y utilizándola posteriormente para el fraude [150].

Otras medidas dirigidas a incrementar el riesgo percibido por el criminal en el espacio físico son el reforzamiento de la vigilancia formal y la introducción de gestores de sitios. Aunque no exista una autoridad centralizada en el ciberespacio los distintos Estados están obligados a investigar y perseguir la criminalidad que allí se produce y que puede dañar los bienes jurídicos de sus nacionales, y por ello utilizan cada vez más los medios tecnológicos para la vigilancia del ciberespacio por medio de equipos especializados de persecución de este tipo de delincuencia. En la actualidad la intervención policial frente a la cibercriminalidad se centra en la persecución de la pornografía infantil en Internet, tanto de las páginas que se dedican a la distribución de este material como de quienes poseen este tipo de material prohibido.

Por último, y como medidas complementarias a las anteriores, también es posible la aplicación de medidas tendentes a facilitar los medios de vigilancia, a mejorarlos para una mayor eficacia. En este sentido la mejora de la identificación de las direcciones IP, especialmente frente a quienes utilizan sistemas de IP *spoofing*, y en general la mejora de los sistemas de detección de la huella digital serían esenciales para la identificación de los infractores. Como medidas de facilitación de los medios de vigilancia también se suelen citar la mejora del diseño del espacio para hacerlo más defendible. No es sencilla la aplicación de medidas de este tipo en el ciberespacio, pero no es imposible, dado lo joven del medio, la reconstrucción del ciberespacio me-

[149] Sobre todo ello, véase el interesante y completo análisis de SMITH, R. G., «Biometric solutions to identity-related cybercrime», en JEWKES, Y., *Crime Online*, Portland, Willan Publishing, 2007, pp. 47 y ss.

[150] *Ibid.,* pp. 53 y ss.

diante un sistema de redes conectadas de forma tal que permitan una mejor vigilancia para evitar el cibercrimen.

Y a estas cuatro clases de medidas se añade últimamente otra no institucionalizada pero que sin duda es tomada en consideración por algunos tipos de cibercriminales. Se trata del aumento de los riesgos derivados de la realización de ilícitos en Internet no consistentes en ser detenido o enjuiciado sino en ser víctima de daños o ataques a su sistema a causa de dichos ilícitos. Esto ocurre con algunas formas de *hacking* que llevan aparejados contraataques de los sistemas que se defienden infectando al sistema agresor, pero muy especialmente con algunas conductas ilícitas relacionadas con los derechos de autor, dado que algunos de los archivos compartidos que aparentemente contienen obras del ingenio más bien son virus en ocasiones cargados por los interesados en que tales sitios web no prosperen y que pueden causar graves daños al sujeto que se los descarga.

La cuarta columna incluye las medidas de prevención situacional que tratan de disminuir las ganancias que el agresor percibe que obtendrá de su conducta criminal. En primer lugar hay formas de ocultar los objetivos a los «ojos» del agresor motivado. Se puede hacer con la información, con valor personal o económico, mediante la utilización de sistemas de encriptación, y debe hacerlo la propia víctima en las redes sociales si no quiere compartir tal información con otros. También es conveniente la máxima diligencia en la utilización de las claves bancarias, números de cuenta y demás datos necesarios para la final defraudación en Internet, especialmente cuando se envíe por correo electrónico u otros sistemas telemáticos. Por último una eficaz forma de ocultación de los objetivos puede constituir en general el perfeccionamiento de los sistemas de pago por Internet que permitan la no utilización de claves o datos bancarios o, incluso, como señalan Felson y Boba, la exigencia de otro tipo de información que no suele ser necesaria para las transacciones comerciales tales como los números impresos en la tarjeta, y demás [151].

Al desplazar los objetivos se puede lograr disminuir las ganancias percibidas por el criminal. En Internet el desplazamiento debe entenderse en un sentido distinto al tradicional de movimiento del objeto cubriendo una determinada distancia, y más bien como cambio en la ubicación electrónica en la que algo está contenido hacia un ámbito nuevo dentro (incluso fuera, aunque entonces estaríamos más cerca de la retirada del objetivo) del ciberespacio. Así, será conveniente en ocasiones el realizar un cambio en las direcciones web, direcciones de dominio y demás con una finalidad defensiva, como también utilizar discos duros distintos en un mismo sistema para tener separada y más protegida la información, e incluso en discos duros extraíbles en el caso de que se trate de información confidencial que puede utilizarse y retirarse cuando se accede al ciberespacio. También se desplazan

[151] Felson, M., y Boba, R., *Crime and everiday life...*, *op. cit.,* p. 197.

los objetivos cuando se crean sistemas de pago alternativos a los tradicionales (sistemas bancarios de tarjeta de crédito, etc.). Con ello lo que se logra es que un objetivo sea, por sí mismo, menos apetecible.

El ataque cibercriminal puede combatirse eliminando los beneficios que el agente obtiene del mismo, influyendo así en la valoración sobre las posibilidades futuras de obtención de ganancias por tales conductas. En la cibercriminalidad económica, como en otras formas de criminalidad realizada con fines de obtención de un beneficio patrimonial, es importante la persecución de quienes permiten obtener los beneficios al delincuente. En el caso de la pornografía infantil esto se puede lograr con la punición de la tenencia de estos materiales, de forma tal que al sujeto que decide poseer ese material pagando al que lo distribuye, le cueste más la decisión al incrementar el perjuicio que puede derivarse de tal hecho. Del mismo modo, y dado que, como se verá en el siguiente capítulo, la mayoría de los cibercrímenes económicos son llevados a cabo por bandas organizadas, la persecución del blanqueo de capitales de estas organizaciones criminales puede ser de gran eficacia.

Por último se cita como esencial estrategia para la reducción de las ganancias de los criminales y la consiguiente minoración de los beneficios percibidos por la actividad criminal, la afectación a los mercados delictivos, haciéndolos menos atractivos y rentables de lo que son. En el caso de la pornografía infantil esto parece complejo, si no es controlando las páginas de descarga directa de archivos en los que se «cuelgan» en muchos casos archivos cifrados que contienen material de este tipo y cuya clave se entrega por el distribuidor directamente al usuario por medio de correo electrónico, en canales IRC y demás. En el caso de los intercambios de material protegido por los derechos de propiedad intelectual existen otras posibilidades para «trastocar» el mercado existente en Internet al respecto: dada la escasa calidad general de los archivos de propiedad intelectual contenidos, sería interesante la potenciación de formas de distribución lícita de tales contenidos como modo de hacer poco rentable para el consumidor acceder al mercado ilegal cuando por poco precio se obtiene un producto mejor en el mercado legal.

La última columna tiene que ver con eliminar las excusas o justificaciones morales, incrementando por tanto los sentimientos de vergüenza o culpabilidad en el delincuente. Clarke introdujo esta categoría en la segunda edición de su libro para poner de manifiesto, según el mismo, que «los delincuentes llevan a cabo juicios sobre la moralidad de su propio comportamiento y frecuentemente racionalizan su conducta para neutralizar sentimientos incapacitantes como la culpa o la vergüenza», de modo que evitar tales racionalizaciones puede incidir en la decisión final de muchos potenciales criminales [152]. Para ello es importante la fijación de reglas que pueden ser normas

[152] CLARKE, R. V., «Introduction», en CLARKE, R. V. (ed.), *Situational crime prevention. Successful Case Studies,* Guilderland, New York, Harrow and Heston Publishers, 1997 (2.ª ed.), p. 16.

jurídicas, puesto que hay sectores de la población que dan valor ético a lo normativo, o también reglas sociales que respondan a la moral colectiva. En este sentido es importante en el ciberespacio el fortalecimiento de lo que se ha venido en denominar *Netiquette*, o reglas del buen uso de Internet que servirán para que quien acceda a ese nuevo ámbito de comunicación social comprenda sus usos básicos, su funcionamiento aceptado por la sociedad que lo conforma. Igualmente, sería recomendable la armonización del Derecho que regula el ciberespacio a nivel internacional, pues en caso contrario siempre se puede utilizar la «excusa» de que en este otro país no se sanciona tal comportamiento.

En cuanto a la fijación de instrucciones y anuncios claros para evitar excusas por parte del agresor, es importante que en las páginas web se incluyan referencias claras a las licencias *copyright* o *copyleft* y demás, así como que en las redes sociales se avise sobre la privacidad de las imágenes y demás elementos personales de los usuarios de las mismas.

En lo relativo al reforzamiento de la conciencia moral ya se ha señalado anteriormente que esto es complejo en el ciberespacio, especialmente en relación con la ética *hacker* que entiende como un fin en sí mismo la existencia de un Internet libre y sin barreras y lo mismo para la información en él contenida. Las campañas de concienciación son complejas en este sentido, especialmente cuando, como se ha señalado, la eficacia de las mismas parece estar unida a su sectorialización [153] ciertamente compleja en el ciberespacio.

Otra forma de concienciación es el refuerzo de las actitudes positivas, en este caso de los negocios lícitos, en aras al debilitamiento moral de los que no lo son.

Finalmente se cita la facilitación de la conformidad o, en otros términos, del comportamiento lícito, que debería ser, a mi parecer, uno de los campos a explotar en relación con algunas de las actividades ilegales pero no consideradas inmorales por parte de quienes suscriben la ética *hacker.* Iniciativas como la creación de competiciones legales para *hackers* o el propio fortalecimiento y difusión del *software* libre como forma de fomento de la modificación y evolución de los sistemas informáticos, servirían para que muchas personas siguieran realizando sus actividades en el ciberespacio pero de forma lícita.

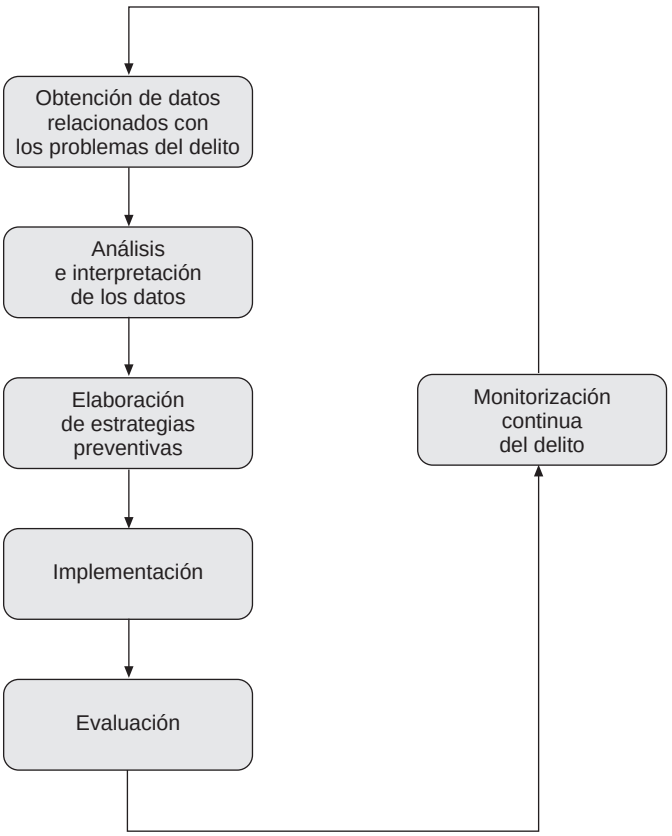
4.3.2. *Alcance y limitaciones del enfoque situacional: el desplazamiento (mejor adaptación) del cibercrimen*

Quizá convenga aclarar que el presente cuadro de medidas no pretende constituirse como una propuesta de prevención situacional de la delincuencia

[153] Medina Ariza, J. J., «El control social...», *op. cit.*, p. 295.

en el ciberespacio. Se trata, como ya se ha explicado, de una trasposición del catálogo de posibilidades que ofrece el enfoque situacional a ese nuevo ámbito de riesgo criminal. Hay que entender, por tanto, que no se pretende afirmar que todas esas medidas servirían para prevenir la cibercriminalidad, ni tampoco que sólo ésas lo harían. Como ocurre con el enfoque situacional en general no se trata de una clasificación dogmática para el cibercrimen, sino de una selección de *estrategias posibles* organizadas a partir de la división entre los principales vectores de la decisión criminal. En última instancia, y como ha señalado Tilley, la prevención situacional no promete ningún tipo de panacea [154], pero sí pueden servir para implantar políticas preventivas eficaces, para lo cual es esencial seguir el proceso de monitorización continua del delito:

Gráfico 3.19. Proceso preventivo de Ekblom [155].



[154] TILLEY, N., *Crime prevention...,* p. 106.

[155] EKBLOM, P., «Getting the best out of crime analysis», *Crime Prevention Unit Paper* 10, London, Home Office, 1988. Este cuadro se corresponde con las características que, según Clarke,

Para el cibercrimen debiéramos hacer lo mismo. Seleccionar un fenómeno criminal lo más concreto posible.

De momento este enfoque nos puede ayudar a comprender la relevancia de algunas decisiones que no están en el plano del agresor, tampoco en el control social del Estado (algo incapaz en los márgenes inmensos del ciberespacio), sino más bien en el de la víctima a la hora de la prevención del cibercrimen. La prevención situacional, la descripción de las medidas que hemos analizado, nos anuncian que además de políticas institucionales de tipo informativo, de concienciación y de incidencia en la arquitectura del ciberespacio para un diseño más defensivo, van a ser esenciales para la prevención de estos crímenes las precauciones cotidianas [156], la adopción de estrategias de autoprotección que, en el ciberespacio, convertirán a quienes las adopten en usuarios seguros y a quienes no en víctimas propiciatorias. Para el cibercrimen, por tanto, también sirve la enunciación de *«the random crime fallacy»,* conforme a la cual el crimen puede producirse en cualquier lugar y contra cualquiera, siendo una cuestión de suerte el convertirse o no en víctima [157]. Como señalan Felson y Boba, lo pernicioso de esta falacia es que elimina la responsabilidad personal al afirmar que el crimen no puede ser prevenido [158]. Sí puede serlo, y en muchas ocasiones por la víctima, y en el caso del cibercrimen, a mi parecer, todo parece indicar que esto es aún más evidente, y que la implementación de sistemas de autoprotección reducirá el riesgo de ser objetivo de un ciberdelito.

La prevención situacional del cibercrimen, especialmente las medidas en las que intervenga la propia víctima, pueden producir por tanto un desplazamiento del objetivo elegido por el cibercriminal: éste seleccionará aquel objetivo que le exija un menor esfuerzo criminal, que conlleve un menor riesgo de ser identificado y que pueda aumentar sus beneficios. A veces lo

---

debe tener cualquier proyecto de prevención situacional: *a)* recolección de datos sobre el problema criminal; *b)* análisis de las condiciones situacionales que permiten o facilitan la comisión del delito en cuestión; *c)* estudio sistemático de las posibles consecuencias derivadas del bloqueo de oportunidades en relación con el crimen incluyendo el análisis de costes; *d)* implementación de las medidas más prometedoras, flexibles y «baratas»; *e)* monitorización de los resultados y difusión de la experiencia. CLARKE, R. V. (ed.), *Situational Crime prevention..., op. cit.,* p. 15.

[156] El concepto de prevención rutinaria no podía más que surgir de la colaboración entre Felson, teórico y principal desarrollador de la teoría de las actividades cotidianas, y Clarke, el padre de la prevención situacional. La unión de estas dos teorías superando el Atlántico lleva a la idea de que la víctima, con su comportamiento, así como las comunidades en relación con ella, también pueden prevenir la delincuencia y, por tanto, deben responsabilizarse también de hacerlo, FELSON, M.; MARCUS, C., y RONALD, V., «Routine precautions, criminology and crime prevention», en HUGH D. BARLOW (ed.), *Crime and public policy: putting theory to work,* Westview Press, Boulder, 1995.

[157] Ésta es una de las famosas «falacias sobre el delito», que en la última edición de «Crime and Everyday...», *op. cit.,* Felson, y ahora Boba, han reducido a nueve. FELSON, M., y BOBA, R., *Crime and everyday..., op. cit.,* p. 21.

[158] *Ibid.,* p. 21.

hará el propio *malware* creado por el cibercriminal y diseñado para atentar contra los sistemas con vulnerabilidades no detectadas por la propia víctima. En todo caso el criminal seleccionará los objetivos más apetecibles y, entre ellos, los menos costosos y peligrosos.

En realidad, esto es parte del paradigma del desplazamiento, supuesta consecuencia de la utilización de políticas de prevención situacional y también principal problema atribuido a esta teoría por parte de sus críticos [159]. Señala Medina con razón que la más sencilla definición del desplazamiento es la que ofrecen Barr y Pease cuando lo describen como «la respuesta de los delincuentes al bloqueo de las oportunidades criminales» [160]: partiendo de la idea de que la prevención situacional no reduce la motivación interna a la comisión del delito sino sólo la concreta oportunidad de ejecutarlo en un determinado ámbito, el criminal ante esos obstáculos se desplazará hasta donde no haya barreras y pueda ejecutarlo. En palabras de Tilley: «Un delito frustrado [...] puede ser cometido en otro lugar, o contra otro objetivo, o utilizando una técnica diferente, o un tipo totalmente diferente de delito puede ser cometido por el mismo delincuente, o un delincuente diferente pueden cometer el delito» [161].

Lo cierto es que en los últimos años parece haberse pasado de la suposición de que el desplazamiento era una consecuencia inevitable de la prevención situacional, a la creencia de que tal desplazamiento, preferiblemente denominado desviación [162], raras veces es total y generalmente no tiene consecuencias negativas [163]. Sin entrar, en todo caso, a discutir si el

---

[159] Son muchas las críticas que se han realizado al enfoque situacional, generalmente provenientes de las teorías de la criminalidad tradicionales, y siguiendo la acertada distinción de Medina Ariza, se pueden diferenciar entre las que discuten la eficacia del enfoque dado su limitado alcance o sus nulos efectos (la crítica del desplazamiento), y las ya anteriormente analizadas que cuestionan la legitimidad moral y política de estas medidas. MEDINA ARIZA, J. J., «El control social...», *op. cit.,* pp. 303 y ss. Sobre las contestaciones a esas críticas, ahora en lo relativo al desplazamiento, resulta especialmente interesante el trabajo de CLARKE, «Situational prevention, criminology and social values», en VON HIRSH, GARLAND y WAKEFIELD., *Ethical and social..., op. cit.,* pp. 97 y ss., especialmente 101 y ss., pero también FELSON, M., y BOBA, R., «Crime and everyday...», *op. cit.,* y PEASE, K., «Crime Prevention», *op. cit.,* pp. 977 y ss.

[160] MEDINA ARIZA, J. J., «El control social...», *op. cit.,* p. 306.

[161] TILLEY, N., *Crime Prevention...*, *op. cit.*, p. 118, quien de ese modo integra los seis tipos de desplazamiento que se pueden producir y que, como advierte más adelante, se pueden dar mezclados entre sí. La clasificación de las formas en las que se puede dar el desplazamiento se debe en primer lugar a Reppetto, quien en 1976 vino a separar la desviación temporal, espacial, táctica, por objetivo o funcional (por el tipo de crimen que se comete), a lo cual se añadió posteriormente el desplazamiento de delincuentes por Barr y Pease. PEASE, K., «Crime prevention...», *op. cit.,* p. 977.

[162] PEASE, K., *ibid.,* p. 978, dado que la desviación puede ser positiva, lo cual no se suele decir del desplazamiento.

[163] WEISBURD, D.; WYCKOFF, L. A.; READY, J.; ECK, J. E.; HINKLE, J. C., y GAJEWSKI, F., «Does crime just move around the corner? A controlled study of spatial displacement and diffusion of crime control benefits», en *Criminology*, vol. 44, núm. 3, 2006, p. 551.

desplazamiento de la criminalidad supone una crítica definitiva al modelo de la prevención situacional [164], lo que es indudable es que la desviación del delito no siempre tiene que entenderse como un fracaso, especialmente si el delito que lo sustituye es menos lesivo que el que no se ha producido, pero también, a mi parecer, si al desviarse la acción se aumenta el esfuerzo que tiene que realizar el criminal para llegar a ejecutar un comportamiento delictivo, pues ello, simplemente por el tiempo que supone, ya es en sí mismo beneficioso.

Además el desplazamiento no es el único efecto secundario de la reducción del crimen, sino que también se aprecia la aparición de efectos positivos que podrían, por tanto, también venir asociados a una hipotética reducción del cibercrimen. En efecto, la contrapartida es que también es posible que se produzca, como efecto del éxito de una política de prevención situacional, un aumento en la difusión de beneficios, que viene a ser el reverso del desplazamiento y consiste en la reducción inesperada de los delitos que no son destinatarios directos de la acción preventiva situacional [165]. La difusión se puede producir según Clarke y Weisburd por disuasión, en el caso de que el alcance disuasorio de las medidas de prevención situacional sea exagerado por los delincuentes potenciales, que creen que están bajo una mayor amenaza de detención de la objetivamente existente [166]; o el desaliento, cuando pese a no haber aumentado los riesgos de detección sí lo ha hecho, desproporcionadamente, la sensación de esfuerzo que tienen que realizar para cometer un crimen [167].

---

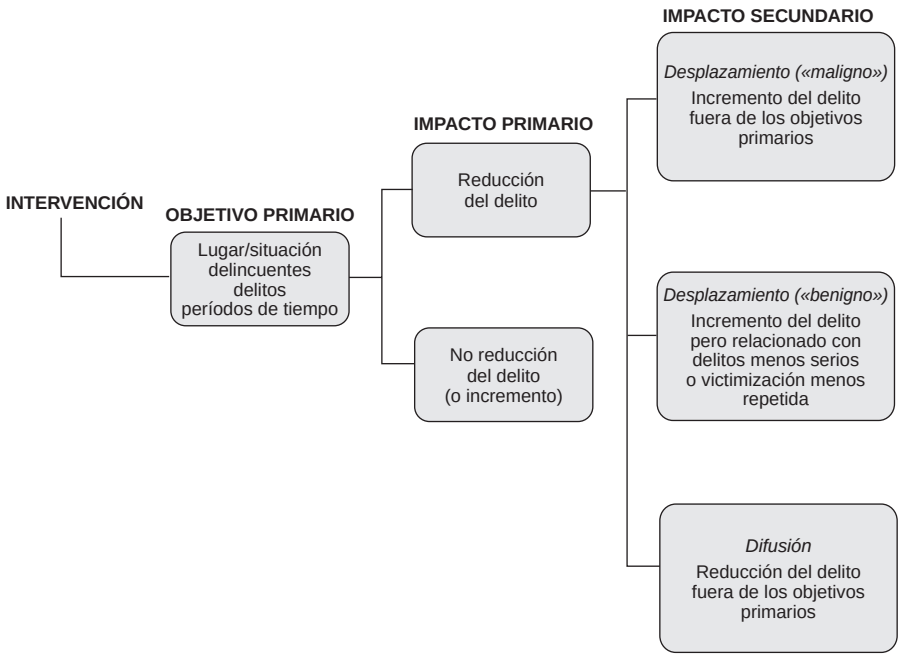
[164] Al fin y al cabo, el propio Clarke reconoce que el desplazamiento fue el talón de Aquiles de la prevención situacional, si bien el estudio de tal problema le lleva a entender que el desplazamiento no es algo «inevitable», en cuanto que si las otras alternativas «no son viables, el delincuente podría conformarse con pequeños premios o con una menor tasa de delincuencia». CLARKE, R. V. (ed.), *Situational crime prevention..., op. cit.,* p. 28. No es, obviamente, éste el lugar, ni son tampoco el método ni la persona adecuados para llevar a cabo una valoración general sobre el enfoque situacional y sobre si realmente el mismo sólo sirve para desplazar el crimen tal y como señalaron los críticos o también para reducirlo. Lo que es indudable, como ha señalado Pease, es que la posibilidad de que las políticas de prevención situacional desplacen el delito no justifican su inaplicación, y menos su sustitución por políticas consistentes en «no hacer nada» desde la perspectiva de la oportunidad, PEASE, K., «Crime prevention», *op. cit.,* p. 978. Cuando se previene un crimen puede volver a surgir como otro delito (desplazamiento) o puede no volver a producirse, difundiéndose los beneficios de la prevención. Como señala Pease, la existencia de estudios que demuestran que el crimen suele realizarse cerca del hogar del agresor o en relación con un propósito muy específico, fortalecerían la idea de que la prevención ambiental no sólo desplazará, sino que reducirá la criminalidad (PEASE, K., «Crime prevention», *op. cit.*, p. 979). Como veremos a continuación, sin embargo, en el ciberespacio es mucha la facilidad para el desplazamiento de los objetivos, lo cual influirá en los concretos efectos del desplazamiento o la desviación del cibercrimen.

[165] CLARKE, R. V., y WEISBURD, D., «Diffusion of crime control benefits: observations on the reverse of displacement», en *Crime Prevention Studies*, vol. 2, pp. 165 y ss., especialmente 167 y ss.

[166] *Ibid.,* pp. 172 y ss.

[167] *Ibid.,* p. 174.

Gráfico 3.20. Impactos primario y secundario de las estrategias preventivas (Clarke y Weisburd, 1994) [168].



Lo que nos interesa ahora, en todo caso, es analizar cómo funcionará el desplazamiento o desviación del delito y demás efectos de difusión, si es que los hubiera, por la aplicación de políticas de prevención situacional en el ciberespacio. En ausencia de los complejos, pero para ello imprescindibles, estudios empíricos [169], se trata de nuevo de plantearse hipotéticamente, a partir de la comparación entre la arquitectura digital y los desarrollos teóricos sobre los efectos de la prevención, cómo influirán las características del nuevo ámbito de oportunidad criminal en el desplazamiento del delito debido a la aplicación de medidas preventivas como las que hemos propuesto anteriormente.

---

[168] *Ibid.,* p. 170.

[169] Sobre el análisis empírico de la cuestión del desplazamiento, véase el completo trabajo de revisión de HESSELING, R. B. P., «Displacement: a review of the empirical literature», en *Crime Prevention Studies*, vol. 3, pp. 197 y ss., y también el más reciente estudio de WEISBURD, D.; WYCKOFF, L. A.; READY, J.; ECK, J. E.; HINKLE, J. C., y GAJEWSKI, F., «Does crime just move around the corner?», *op. cit.*, pp. 549 y ss., en el que revisan las investigaciones sobre desplazamiento y difusión de beneficios, discuten la metodología y realizan, además, un estudio de campo complejo y riguroso en el que, contrariamente a las perspectivas que predicen el desplazamiento espacial inmediato desde los puntos calientes en los que ha habido intervención policial hacia otros sitios, se comprueba una difusión de los beneficios de control de la delincuencia en las zonas que rodean los lugares en los que se ha intervenido.

Pues bien, la arquitectura del ciberespacio influirá en las formas de desplazamiento de la cibercriminalidad ante la implantación de medidas de prevención situacional. Concretamente habrá formas de desplazamiento que no se darán, bien por una mera cuestión de imposibilidad física en el nuevo ámbito, o bien por la propia dinámica de la comunicación (también la criminal) en el ciberespacio, y otras formas de desplazamiento que si acontecerán en este contexto. Esto se puede ver en la siguiente tabla 3.4.

Tabla 3.4. Los seis tipos de desplazamiento (en fondo gris las modalidades de desplazamiento en el ciberespacio, en fondo blanco, el tipo de desplazamiento que se producirá pero cambiando su naturaleza). Barnes (1995) de Reppeto (1976), Hakim y Rengert (1981) y Barr y Pease (1990) [170].

Tipo de desplazamiento	*Descripción*
Espacial	Delincuentes que abandonan las zonas donde el delito se ha vuelto más difícil de cometer y comienzan a llevar a cabo actos delictivos en otro lugar.
Objetivo	Delincuentes que abandonan objetivos que están bien protegidos y centran sus esfuerzos en otros más vulnerables.
Temporal	Delincuentes que trasladan a otras horas o días de la semana sus delitos, cuando cometer la infracción es menos arriesgado.
Táctico	Los delincuentes que cambian sus tácticas para evitar aquellos obstáculos destinados a frustrar la comisión del delito.
Autor	Como los delincuentes que suelen cometer ciertos delitos están arrestados o detenidos, otros delincuentes deciden ocupar su lugar.
Tipo de delito	Los delincuentes responden al bloqueo de un determinado tipo de acto delictivo, cometiendo delitos totalmente diferentes.

Antes de entrar en el desarrollo del cuadro, sin embargo, conviene hacer dos aclaraciones previas. En primer lugar no parece adecuado hablar de desplazamiento del cibercrimen, dada la asociación que tal verbo tiene con recorrer una distancia física. Es cierto que en el ciberespacio también se puede ir de un lugar (sitio web) a otro, pero quizás sería más adecuado hablar de desviación, que no parece hacer referencia necesariamente a un traslado físico, o incluso de la adaptación del cibercrimen. Si de lo que se trata, con el tópico generalmente denominado desplazamiento, es de analizar, como posible impacto secundario tras el impacto primario de la reducción

[170] La adaptación del cuadro la realiza BARNES, G. C.: «Defining and optimizing displacement», en *Criminal prevention,* 1995, p. 96

del crimen, la respuesta de los delincuentes al bloqueo de las oportunidades criminales, esto podría describirse, más que como un desplazamiento, como una adaptación del cibercrimen. La reducción de los cibercrímenes, debida a la prevención situacional de los mismos, conllevará, en muchos casos, una adaptación de la cibercriminalidad con cambio de los objetivos, de los medios o tácticas para su ejecución, de los tipos de infracción o, incluso, de la identidad virtual desde la que se realiza el ataque.

Otra importante precisión es que la adaptación o desviación del cibercrimen no será, obviamente, siempre igual, sino que dependerá especialmente del tipo de medida preventiva que se haya implantado y, por tanto, de la razón por la que se ha logrado el efecto reductor. Si la medida utilizada consiste en el aumento del esfuerzo que el agresor percibe que tendrá que llevar a cabo para el éxito de la infracción, pero el objetivo le sigue ofreciendo las mismas ganancias potenciales, lo lógico es que el cibercriminal trate primero de adaptar la táctica; y si ésta no es posible o es demasiado el esfuerzo, entonces se desvíe hacia otro objetivo sobre el que realizar el ataque. Si por el contrario las medidas consisten en la reducción de beneficios percibidos asociados a un tipo de delito, lo normal será que el desplazamiento sea de tipo de infracción cometida. Cuando las medidas consistan en el aumento del riesgo percibido la adaptación dependerá de si tal riesgo se relaciona con el objetivo o con el medio utilizado: en el primer caso el cibercriminal se adaptará sustituyendo el objeto del ataque, en el segundo cambiará la forma de realización siempre para evitar su identificación.

Lo que sí es cierto es que serán estas tres citadas formas de adaptación del crimen (de objetivos, tácticas o tipos de crímenes), y no las otras tres posibles para el resto de la criminalidad, las que se darán en el ciberespacio. No habrá un desplazamiento espacial en el sentido de la necesidad de recorrer una distancia física para ejecutar el crimen: el cibercriminal lo seguirá perpetrando desde el mismo lugar (físico), si bien es cierto que los efectos se desplegarán de otra forma o incluso en otro lugar. Tampoco será usual el cambio temporal: en el ciberespacio las dimensiones temporales tienen una configuración distinta a la que tienen en el espacio físico, pues nada aportará al cibercrimen que la amenaza, el contenido ilícito o el envío de *malware* se lleven a cabo por la noche o por la mañana. Por último sí puede ser que nos encontremos ante un cambio de personas en el caso de que los ciberdelincuentes sean detenidos o, más bien, sea identificada cuanto menos la zona geográfica desde la que acceden al ciberespacio para ejecutar la infracción criminal. No será lo usual, sin embargo, entre otras cosas porque la detención de los ciberdelincuentes es harto complicada en la mayoría de los casos dada la transnacionalidad del fenómeno criminal, la dificultad para la identificación del sujeto y demás caracteres del ciberespacio.

Tabla 3.5. Cuadro de la adaptación del crimen en el ciberespacio. Elaboración propia.

Adaptación del crimen en el ciberespacio	*Descripción*
De identidad virtual	Los cibercriminales cambian el lugar en el ciberespacio desde el que realizan el ataque o el nombre de la web desde el que actúan criminalmente.
De objetivo	Los cibercriminales desechan el ataque a objetivos bien protegidos y centran sus esfuerzos en otros más vulnerables.
Técnica	El cibercriminal mejora su ataque y utiliza nuevos instrumentos para superar las nuevas barreras.
Tipo de delito	Los delincuentes responden al bloqueo de un determinado tipo de acto delictivo, cometiendo delitos totalmente diferentes.

Lo que sí es posible, en cambio, es que se produzca en el ciberespacio un cambio del lugar, no físico, sino virtual, desde el que el agresor realiza el ciberataque. Estamos, por tanto, ante un híbrido entre el desplazamiento espacial y el desplazamiento de autor: el cibercriminal cambia la dirección desde la que ataca o, incluso más claramente, cambia el nombre y la ubicación de la página web desde la que ofrece, por ejemplo, un contenido ilegal: no hay un desplazamiento físico, ni un cambio de la persona, pero es un nuevo actor en el ciberespacio y desde un nuevo lugar en la Red, desde el que comete el hecho criminal. A este tipo de adaptación del cibercrimen podríamos denominarla «de identidad virtual», en la que la medida de prevención situacional ha conseguido, por ejemplo, la retirada en el ciberespacio de un transgresor que, sin embargo, y al no haber sido retirado en el espacio real, se adapta al nuevo contexto creando un nuevo sitio web desde el que seguir realizando la conducta criminal.

Como se ha adelantado este tipo de adaptación es particularmente útil para la tercera categoría de cibercrímenes dentro de la clasificación tipológica que analizábamos anteriormente [171], esto es, aquellos delitos en los que la ilicitud deviene de la transmisión (o puesta a disposición) de contenido ilícito, que puede ser pornografía infantil, materiales de incitación al odio racial, delitos contra la propiedad intelectual o diferentes formas de ciberterrorismo. La detección de, por ejemplo, las páginas webs de difusión de pornografía infantil y su cierre supondrá la desaparición del delito pero, probablemente, la adaptación del mismo a otra web o, incluso, a otro tipo de canal de comunicación más discreto como el envío directo por correo electrónico tras el contacto en foros, o la descarga desde webs del estilo de Rapidshare o Megaupload tras la identificación del material por medio del

[171] Véase *supra* cap. II.

correo electrónico o en foros tras el pago de la cantidad convenida. Algo similar ocurrirá con las webs yihadistas de difusión de mensajes violentos de incitación al terrorismo, o con las que realizan *hate speech*. Aunque es cierto que con este tipo de persecución y cierre de las webs ya se produce un beneficio pese a la adaptación (el aumento del esfuerzo percibido por el cibercriminal), es obvia la necesidad, debido a tal desviación, de conjugar esas medidas con otras referidas a la disminución de los beneficios percibidos, por ejemplo persiguiendo a los compradores de tales contenidos.

Junto a esta forma de adaptación, la prevención situacional de la cibercriminalidad también puede llevar al ciberdelincuente a adaptar su conducta buscando nuevas víctimas a las que agredir. Dado que la mayoría de las medidas de prevención situacional eficaces en el ciberespacio tienen que ser adoptadas por la propia víctima, y serán particularmente todas aquellas consistentes en aumentar la dificultad percibida por el agresor para lograr el éxito de la infracción, lo usual será que el agresor elija otro objetivo (si bien con idéntica naturaleza que el anterior) que esté más desprotegido sobre el que realizar el ataque, que utilice otras técnicas informáticas distintas a las usadas sobre el mismo objetivo para salvar las barreras impuestas, o que cambie de infracción delictiva realizada aunque siga actuando con similar propósito criminal. Lo primero será lo más usual en muchos tipos de cibercriminalidad, especialmente en la económica en la que el ataque consiste en la infección de *malware,* envío de *spam* o similar para la infección del sistema y la captación de información sensible. En ella, sin embargo, puede ser que ni siquiera haya una adaptación criminal dirigida por el agresor, sino una dispersión (y reducción) de los efectos hacia objetivos desprotegidos. En efecto, una dinámica usual en la cibercriminalidad es la de la creación de un *malware* y su envío, generalmente a través de una *botnet*, a un objetivo indeterminado, a un conjunto de usuarios sobre los que no se conocen las características esenciales de protección del sistema. El *malware*, en cambio, sí determina las características de la víctima: sólo será detectado por aquellas víctimas potenciales que tengan un sistema concreto de protección, de modo que cuando ellas lo reciban podrán evitar el ataque, cosa que no podrán hacer aquellas víctimas que no estén protegidas. En este caso más que un desplazamiento lo que hay es una reducción del ámbito de incidencia y una desviación de los efectos hacia los objetivos menos protegidos. En otros casos, cuando de lo que se trata es de la realización de un ciberataque contra un objetivo determinado (una empresa concreta para la obtención de información para una posterior extorsión o para la venta de la misma o similar), sí que habrá desplazamiento de objetivos hacia otros menos protegidos pero de similar naturaleza. Aquí sí que será el cibercriminal el que, al aumentar la percepción del esfuerzo que le va a suponer la realización del crimen contra una víctima en concreto, desvíe su ataque a otro menos protegido y, por tanto, con menor coste de dificultad.

Lo más usual en la cibercriminalidad, en todo caso, será la adaptación táctica, esto es, la adopción de nuevas estrategias, más bien técnicas informáticas, ante la constatación de una medida de prevención situacional en forma de barrera de protección en el sistema de la víctima. Con ello se consigue que aumente el esfuerzo del cibercriminal, quien, en algunos casos, preferirá cambiar de objetivo o incluso de tipo de delito ante la dificultad existente. Esto es lo que ha venido ocurriendo no tanto con el *hacking*, pero sí con los fraudes telemáticos que han ido evolucionando desde los más burdos tipos (*scam*) en forma de cartas nigerianas y demás, a las más elaboradas modalidades de *pharming* en las que la dirección del *e-mail* recibido y la web defraudatoria comparten total semejanza con los originales, pasando por el *phishing* general en el que a su vez han ido cambiando las excusas para solicitar las claves bancarias al usuario. La desviación, o mejor utilización, de nuevas técnicas por parte de los ciberagresores está totalmente comprobada también en relación con el *malware* que, de hecho, va cambiando a raíz de la evolución de las barreras de protección y viceversa. Y todo esto sucede tanto cuando se controla el acceso al sistema como cuando se detecta e impide el ataque, etcétera.

En los casos en los que no es posible la adaptación técnica ni la del objetivo, podemos encontrarnos con una adaptación de la cibercriminalidad consistente en un cambio de naturaleza de la conducta criminal realizada. Aquí ya no se trata de una selección distinta de la víctima informática usada para lograr el éxito del ataque, ni siquiera de una modificación de las técnicas, sino de un cambio del tipo de delito que se va a cometer siempre, eso sí, dentro del espectro de motivaciones que mueve al autor del crimen. En el caso de la cibercriminalidad económica, y dado que, como se verá continuación, es un tipo de delincuencia que generalmente cometen grupos organizados, no es inusual que ante la constatación de un aumento de la recompensa percibida o de los riesgos de ser detenido, el agresor cambie el tipo de objetivo del ataque. En muchos casos esto no será complejo, dado que muchas de las técnicas utilizadas para la cibercriminalidad (minería de datos, *hacking*, virus, ataques DDoS, etc.) pueden ser utilizadas para la ejecución de variados tipos delictivos.

El ciberespacio, pues, y como resumen conclusivo, favorece la adaptación de los cibercriminales, por lo que es de prever que muchas de las medidas de prevención situacional propuestas no reduzcan en exceso las cifras (blancas o negras) de la cibercriminalidad, si bien sí que retrasen y compliquen el éxito de los cibercriminales. Pero desde una perspectiva no global sino individual o sectorial, la enseñanza es importante: el cibercrimen se desplazará, mejor se adaptará, seleccionando los objetivos más débiles y vulnerables, por lo que, de nuevo, el centro de la prevención del delito está en la propia víctima, y en la adopción de las estrategias preventivas necesarias para evitar que sea ella la elegida como objetivo adecuado en el cálculo

motivacional del ciberagresor. O dicho con las precisas palabras de Newman «en realidad no es necesario el uso de complejos sistemas informáticos para la prevención del cibercrimen, dado que la mayoría de los cibercrímenes no se llevan a cabo gracias a las brillantes ideas de un mago de la informática, sino debido a debilidades humanas» [172].

[172] NEWMAN, G. R., «Cybercrime: prevention», en FISHER, B. S., y LAB, S. P., *Encyclopedia of Victimology and Crime Prevention,* vol. 1, California-London, Sage Publications, 2010, p. 253.

CAPÍTULO IV

EL CIBERCRIMINAL. PERFILES DE DELINCUENTES EN EL CIBERESPACIO

1. BESTIARIO DEL CIBERESPACIO

1.1. Introducción: del *hacker* cinematográfico al «cibercriminal común»

Resulta difícil extraer del imaginario social al *hacker* como protagonista único cuando se habla de cibercriminalidad. Esto se debe a que el *hacker* fue el gran protagonista de las primeras formas de «criminalidad informática», aquéllas centradas en el acceso a la información en sistemas informáticos, que reducían el perfil del sujeto activo de la cibercriminalidad al del modelo cinematográfico del genio informático, «joven intelectualmente superdotado y con unos problemas de adaptación social tales que le llevan a volcar todo su interés en el denominado universo cibernético, olvidándose casi por completo de lo que acontece en el mundo real» [1]; o también «hombre blanco varón de 14 a 19 años de clase media, con nivel alto de inteligencia (cociente intelectual por encima de 120), pero que suele estar excluido socialmente lo que le lleva a asociarse con otros sujetos fascinados por las nuevas tecnologías y el uso de los ordenadores» [2].

Pues bien, conviene comenzar este capítulo precisando que no puede identificarse completamente al *hacker* con el cibercriminal, puesto que en realidad no hay un perfil único de ciberdelincuente [3], sino múltiples, del mismo modo que no hay un perfil único de criminal del espacio físico. Al hablar de un cibercriminal nos referimos a cualquier sujeto que delinque

---

[1] Galán Muñoz, A., «Expansión e intensificación del Derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática», en *RDPP,* núm. 15, 2006, p. 19, en sentido crítico, que comparto, con que esta sea la única caracterización del delincuente informático.

[2] Adler, F.; Mueller, G. O. W., y Laufer, W. S., *Criminology and the Criminal..., op. cit.,* p. 355.

[3] Como dicen muy expresivamente Pinguelo, F. M., y Muller, B. W., «Virtual Crimes, Real Damages...», *op. cit.,* p. 121: «No existe un perfil estático de ciberdelincuente, ya que estos adquieren distintas formas en su intento de robar, engañar y destruir».

utilizando el ciberespacio como parte esencial o central del delito, por lo que no es posible una caracterización general del cibercriminal excepto en lo relativo a que debe usar la tecnología informática con acceso a las redes telemáticas. Teniendo en cuenta la popularización de Internet como medio de intercomunicación universal y el que ya no sean sólo los jóvenes de hasta 25 años los que interaccionen con él sino prácticamente todos los estratos de edad y todas las clases sociales, el espectro sigue siendo casi tan amplio como el de la criminalidad en el espacio físico. Así, puede ser cibercriminal tanto el joven experto y entusiasta de la informática que disfruta aprendiendo todo acerca de los sistemas y las redes digitales y superando las barreras tecnológicas por el mero hecho de hacerlo y de así aprender nuevos conocimientos informáticos [4] (el *hacker* en su sentido más cinematográfico), como el adulto de 40 años que utiliza el móvil para entrar a las redes sociales o para enviar correos electrónicos y también el trabajador de 50 años de edad que accede a Internet sólo desde su empresa desde donde pide a una menor que le enseñe su cuerpo a través de una webcam o le contará información privada de sus padres. Este último no tiene conocimientos de informática, sino que vendría a ser (como también el segundo) un cibercriminal común, cuya única caracterización distinta a la de otros sujetos que acosan sexualmente de otras personas es que la acción tiene lugar en el ciberespacio.

Esta idea de la multiplicidad de los perfiles del cibercriminal es totalmente coherente con la clasificación criminológica que realizábamos anteriormente y que nos permitía distinguir, sobre la base del propósito del cibercriminal, entre cibercrímenes económicos, políticos o sociales. El perfil de cada uno de estos tipos de cibercrímenes será distinto entre sí, sin que quepa pensar que el ciberacosador que intenta contactar con una menor de 14 años pueda tener idénticas características que el *cracker* que forma parte de una banda organizada que opera en Red. Del mismo modo tampoco sería acertado pensar que dentro de cada uno de estos grupos los sujetos compartan idénticas características: en la cibercriminalidad política nos podemos encontrar desde el *scriptkiddie hacktivista* que participa en los ataques de denegación de servicio sin ser del todo consciente de los daños que puede causar, hasta el ciberterrorista que puede ser, a su vez, un adulto sin apenas conocimientos informáticos que envía mensajes para el reclutamiento de terroristas o un *hacker* especializado pagado por la organización a la vez pagada por un Estado para atacar y dañar a otro; en la cibercriminalidad económica también podemos encontrarnos desde el *insider* que aprovecha el estar dentro de la empresa para causar el daño o robar la información de que se trate a cambio de una cantidad de dinero, pasando por el mulero del *phishing* que se encarga simplemente de enviar

[4] Barber, R., «Hackers Profiled. Who Are They and What Are Their Motivations?», en *CFS*, vol. 2001, núm. 2, febrero de 2001, p. 14.

por medios seguros las cantidades de dinero que recibe fruto del fraude, hasta llegar a los *hackers*, algunos de ellos muy especializados técnicamente que actualizan sus conocimientos para aprovechar las vulnerabilidades de los sistemas y atacarlos bien de forma individual, bien para un grupo organizado que les paga o bien de forma organizada con otros a través de la Red; por último, en la cibercriminalidad personal o social poco tienen que ver el chaval de 17 años que acosa a otro chico de menor edad de su colegio grabando vídeos del niño y colgándolos en una página de Internet, con el sujeto que realiza proposiciones sexuales a menores aprovechando la «oscuridad» del ciberespacio, o con el servidor en el que un usuario ha colgado insultos a una determinada persona y al que instan a que retire el foro o la web en el que están contenidos.

Junto a esta primera conclusión lógica relativa a que no es posible definir características generales a todos quienes realizan conductas criminales en el ciberespacio debido a la multiplicidad de delitos existentes, debemos añadir otra relativa a la dificultad para el *profiling* incluso de los autores de cibercrímenes concretos y de la misma naturaleza. La razón es sencilla: gran parte de los ciberdelitos no son enjuiciados por los motivos que ya hemos ido señalando, de forma que no es fácil ni la realización de estudios cuantitativos que traten de identificar los caracteres generales concurrentes en las personas enjuiciadas por cibercrímenes, ni los estudios cualitativos que, en todo caso, servirán como referencia con escaso valor científico para un determinado ámbito de la delincuencia en el ciberespacio pero no para establecer conclusiones generales.

Por ello, el propósito de este capítulo no es el de establecer una definición precisa de cada uno de los perfiles posibles de cibercriminales y de los delitos que cometen, sino analizar, a modo de bestiario, los diferentes tipos de personas que participan en la criminalidad en el ciberespacio, comenzando por el necesario análisis de las figuras más generalmente asociadas a la cibercriminalidad, las de *hackers* y *crackers*, y tratando después de individualizarlo a las que hemos definido como categorías criminológicas de cibercrímenes teniendo en cuenta los estudios empíricos existentes.

1.2. Los *hackers* (y dentro de la categoría, también *crackers*, *scriptkiddies*, etc.)

Si antes afirmaba que el cibercriminal no puede identificarse con el *hacker*, afirmo ahora que tampoco hay un único tipo de *hacker* ni las características más comunes del mismo coinciden con aquellas del *hacker* cinematográfico que he comentado previamente. El *hacker* ha ido evolucionando a lo largo del tiempo: desde los denominados *true hackers*, pioneros aficionados a la informática en los primeros días de la aparición de esta tecnología en los años sesenta, pasando por los *hardware hackers* de los setenta, que desa-

rrollaron algunos de los equipos y tecnologías más importantes, y también por los *game hackers* en los años ochenta que desarrollaron aplicaciones de *software* para juegos, y siendo la penúltima meta la conformada por la dualidad *hacker/cracker* de los años noventa que incluye a quienes utilizan las tecnologías informáticas en el nuevo marco de la Red de Redes para acceder ilícitamente a sistemas o redes [5] y los diferencia según su actuar sea inocuo o malicioso, hasta llegar a los *hackers* clandestinos de la web 2.0 y de la era de la tipificación delictiva del acceso informático ilícito que pueden dedicarse tanto a la intromisión informática, a la realización de ataques DoS, a la creación de webs para el fraude, al diseño de virus, a la infección de *bots* o al envío de *spam*, y todo ello con finalidad económica (generalmente) o bien política en el caso de los *ciberhacktivistas,* y actuando de forma individualizada o formando parte de un grupo, que bien puede ser una banda organizada tradicional que opera ahora en el ciberespacio o una ciberbanda de *hackers* que unen sus esfuerzos para un fin criminal común.

Esta primera acepción posible de *hacker* es, pues, amplia y englobadora y tiene un inequívoco significado de ilicitud: conforme a la misma lo es cualquier persona con conocimientos informáticos que realiza alguna actividad ilícita, o simplemente no autorizada, en el ciberespacio. La misma abarcaría, por consiguiente, todas y cada una de las tipologías incluidas en las múltiples categorizaciones de los años noventa que distinguían entre *hackers, crackers, phreakers* y *pirates* [6], o entre *pranksters, hackers, malicious hackers, personal problema solvers, career criminals, extreme advocates* y otros [7], también en aquellas otras taxonomías más recientes que diferencian entre *scriptkiddies, cyberpunks, hacktivists, virus writers, professionals* y *cyber-terrorists* [8]; y a las cuales podrían sumarse muchas otras (*spammers, snoopers, spoofers, sniffers*), correspondientes a cada una de las nuevas for-

---

[5] Taylor, P. A., «From hackers to hacktivists...», *op. cit.,* pp. 630 y ss. Incluye además, otras categorías posteriores de *hackers* como los denominados *microserfs*, que vienen a constituir los *hackers* que acaban integrándose en la propia industria informática, los dedicados al desarrollo de *software* libre que tuvo su auge a finales de los noventa y sigue en la actualidad, y los que denomina «*hacktivistas»,* que son aquellos que unen la actividad *hacker* con las finalidades políticas que acaban constituyendo la auténtica razón de ser del *hacker.*

[6] La diferenciación clásica de Lee, M. J., «Computer Viruses, Computer Hackers: Security Threats of the 1990's», en *National Criminal Justice Reference Service*, 1991, pp. 1 y ss.

[7] Parker, D. B., *Fighting Computer Crime: A new Framework for Protecting Information,* New York, Wiley, 1998, citado por Mcquade III, S. C., «Cybercrime», *op. cit.*, p. 483.

[8] Ésta es la clasificación de Rogers, M. K., «The Psyche of Cybercriminals: A Psycho-Social Perspective», en Ghosh, S., y Turrini, E. (eds.), *Cybercrimes: A Multidisciplinary Analysis*, Heidelberg, Springer-Verlag Berlin, 2010, pp. 218 y ss. La de Rogers no es propiamente una clasificación tipológica, dado que va más allá de las conductas realizadas y analiza las motivaciones (económica, venganza, notoriedad, curiosidad) de quienes conforman cada una de las categorías a las que añade, además, otras dos categorías: los *insiders,* que actúan esencialmente por venganza y dinero, y los *old guards* que podríamos traducir como «la vieja guardia», que tienen profundas habilidades técnicas y aunque no poseen intenciones criminales, sino que se mueven esencialmente por curiosidad, generalmente muestran poco respeto hacia los bienes personales.

mas de conducta criminal existentes en el ciberespacio [9]. A mi parecer, es preferible utilizar el concepto general de *hackers* (o de *crackers*, como se verá, en el caso de que se pretenda diferenciar entre uno y otro tipo) dado que como ha señalado Mcquade III [10] las categorizaciones analizadas o no son funcionales, o no están validadas empíricamente [11] o, añadiría yo, no sirven para describir a personas sino más bien a conductas concretas, lo cual no resulta útil a los efectos pretendidos de definición de los distintos sujetos intervinientes en la Red dado que no será extraño encontrarnos un *hacker* que utilice varias herramientas distintas y que ejecute comportamientos delictivos diferentes entre sí.

Junto al concepto amplio o genérico de *hacker* también podemos utilizar otro más estricto, preferido por la gran mayoría de *hackers* y otros expertos en Internet, que haría referencia a la figura del que también se conoce como samurai informático: experto en informática (y apasionado de Internet y las nuevas tecnologías) que busca superar barreras por el mero hecho de su existencia si bien sin entrar en el campo de lo delictivo, en ocasiones incluso usando sus conocimientos para la mejora de la seguridad de las redes y los sistemas. Para el *hacker* en sentido estricto, el acceso a un sistema informático es esencialmente un reto tecnológico que mejora el propio sistema [12], un fin en sí mismo y no un medio para lograr algo [13]. Esto deriva de las propias bases psicosociológicas del fenómeno [14]: entre el *voyeurismo*, el puro

---

[9] Véase *supra* cap. II.

[10] Mcquade III, S. C., «Cybercrime», *op. cit.,* p. 481, quien, sin embargo, acaba realizando a su vez una categorización de *cyber offenders*, distinguiendo entre «estafadores y ladrones, *hackers,* intrusos en sistemas y *crackers* de contraseñas, escritores de códigos maliciosos y distribuidores de los mismos, piratas, acosadores y extorsionistas, acosadores, pedófilos y otros delincuentes sexuales, espías de empresas, gobiernos o *freelance,* ciberterroristas, aprendices interesados [*wannabe lammers*], recién iniciados, *hackers* maliciosos, *hackers* éticos, *hackers* tranquilos, expertos, paranoicos, ciberguerreros, espías industriales, agentes del gobierno o *hackers* militares». No hace falta un análisis detallado de las categorías para presumir que tal clasificación, si es que pretende serlo, adolece de los mismos defectos que las otras.

[11] El último gran esfuerzo sistematizador es el de Chiesa Ducci y Chiapi, mediante el *The Hacker's Profiling Project (HPP*®*)*, que les llevó a establecer nueve categorías de *hackers: wannabe lammer, scriptkiddie, cracker, ethical hacker, quiet paranoid skilled hacker, cyber warrior, industrial spy, government agent,* y *military hacker*. Aunque hay un trabajo empírico detrás, la sistematización y categorización es evidentemente aleatoria y la utilidad de la misma más que discutible, aunque, por el contrario, este trabajo aporte datos muy interesantes sobre las características de muchos delincuentes en el ciberespacio así como la diferenciación entre sus motivaciones personales. Véase al respecto de todo ello, Chiesa, R.; Ducci, S., y Ciappi, S., «Profiling Hackers», en *The Science of Criminal Profiling as Applied to the World of Hacking,* Taylor & Francis Group, 2009, pp. 57 y ss.

[12] Sukhai, N. B., *Hacking and Cybercrime* (2004), Base de datos ACM. En Internet en *http://portal.acm.org/citation.cfm?id=1059553* (última visita el 9 de septiembre de 2010).

[13] Raymond, E. S., *How To Become A Hacker* (2001), en Internet, en *http://www.catb.org/~esr/faqs/hacker-howto.html* (última visita el 9 de septiembre de 2010).

[14] Señala Yar, M., *Cybercrime and society, op. cit.*, p. 33, que gran parte de las emociones y percepciones atribuidas psicológicamente a los *hackers* son contradictorias entre sí, lo cual viene a

entretenimiento [15], la voluntad de notoriedad en el ámbito de las tecnologías informáticas [16]. Tradicionalmente se ha venido asumiendo que los *hackers* son personas con habilidades sociales bajas o no desarrolladas. Como ha señalado Rogers, esto es sin embargo discutible, dado que esta afirmación se suele basar a partir de la definición tradicional de las habilidades sociales, esto es, las interacciones y comunicaciones cara a cara, olvidando, sin embargo, que las comunicaciones *online* también son vida social [17]. En este sentido señala el autor que los cibercriminales tienen una gran actividad social en el ciberespacio, con normas de comportamiento propias (*netiquette*), amistades e incluso comportamientos prosociales como el tutorizar a los nuevos a entender la tecnología y el *software*, etcétera [18].

A todos estos rasgos psicológicos se suele añadir cierta suma de ideas que, según algunos [19], conjugan una «ética del *hacker*» [20], entre las que destaca la comprensión de la Red como un lugar sin barreras en el que todo el mundo debe poder acceder a todo para «poner en común la información» [21]; el *hacker* se ve a sí mismo como un mago de la programación y de la cultura

---

reflejar, en realidad, las muy distintas personalidades, motivaciones e intereses que se encuentran en ese término común que es «el *hacker*».

[15] Véase en este sentido, el interesante estudio cualitativo de TURGEMAN-GOLDSCHMIT, O., «Hacker's Accounts: Hacking as a social entertainment», en *SSCR,* núm. 23, 2005, pp. 8 y ss., en el que entrevista a más de cincuenta *hackers* israelíes para situar en el centro de sus intereses el puro entretenimiento, con base de superación tecnológica, obtenido mediante el *hacking.*

[16] Aunque la notoriedad no se expresa públicamente como un fin del *hacker*, es uno de los grandes propósitos del acceso ilícito. Al fin y al cabo, en la comunidad *hacker* se considera que uno no debe describirse a sí mismo como un *hacker*, sino que deben ser los demás los que le nombren como tal. SINROD, E. J., y REILLY, W. P., «Cyber-crimes: a Practical Approach to...», *op. cit.,* p. 4.

[17] ROGERS, M. K., «The Psyche of Cybercriminals...», *op. cit.*, p. 224.

[18] *Ibid.,* pp. 223 y ss.

[19] Digo según algunos, no dando por sentada la existencia de una única «ética *hacker*» porque algunos estudios recientes parecen dar la razón al conocido *hacker* Acid Phreak cuando en 1990 dijo que: «No hay una ética *hacker*. Cada uno tiene la suya. Afirmar que todos pensamos lo mismo es absurdo». Véase en todo caso, con múltiples referencias a favor y en contra, y sobre la posible relación entre la actividad *hacker* y el liberalismo, el interesante estudio de COLEMAN, G., y GOLUB, A., «Hacker practice: Moral genres and the cultural articulation of liberalism», en *AT,* núm. 8, septiembre de 2008, pp. 255 y ss.

[20] Véase en este sentido, desde una perspectiva sociológica, HIMANEN, P., *La ética del hacker y el espíritu de la era de la información,* Barcelona, Destino, 2004, pp. 25 y ss. Desde una perspectiva más cercana a la jerga y a la realidad práctica del ciberespacio, que ya no se refiere a la ética, sino a la «actitud *hacke*r» es especialmente interesante, RAYMOND, E. S., *How to Become a Hacker, op. cit.*

[21] La ética del *hacker* se podría resumir en la frase: «El acceso a las computadoras, así como a cualquier cosa que pueda enseñarte algo acerca de la forma en que funciona el mundo, debe ser ilimitado y total». LEVY, S., *Hackers. Heroes..., op. cit.,* p. 28. En todo caso, el credo general de los *hackers* suele resumirse en los siguientes principios: 1. el acceso a los sistemas informáticos debe ser ilimitado y total. 2. toda la información debe ser libre. 3. desconfía de la autoridad y promueve la descentralización. 4. los *hackers* deben ser juzgados por sus actos de *hacking*, no por criterios falsos relativos al grado, la edad, la carrera, la raza o la posición. 5. puede crearse arte y belleza con un ordenador. 6. los ordenadores pueden cambiar tu vida para mejor. Véase PRICE, D., y SCHMADEKE, S., «Hackers Expose Web Weakness: There's No Defense Against Internet Assaults, Experts Confess, and Attackers are Elusive», en *DN*, 14 de febrero de 2000, p. 1.

virtual, como los auténticos constructores de Internet, los que hacen que funcione [22].

Esta visión algo idílica del *hacker* está en peligro debido a que cada vez más se está restringiendo su ámbito de actuación en el marco de lo lícito. Como se verá posteriormente para el análisis del *hacking*, su consideración como delito puede llevar a la desaparición del *hacker* puro, cuanto menos en lo que respecta a la intromisión en sistemas informáticos, puesto que desde el momento en que la misma, independientemente del fin con el que se lleve a cabo, resulte delictiva, la diferenciación entre *hacker* y *cracker* a efectos del acceso carecerá de sentido. Ésta es una de las causas de que en las últimas décadas se haya pasado de una idílica visión del *hacker*, de su visión de héroes que les atribuye Stephen Levy, a una criminalización de los mismos, a su categorización como cibervillanos por parte de la sociedad, que los asocia inmediatamente al cibercrimen [23]. De la edad de oro *hacker,* se ha pasado a una época en la que se les ha demonizado [24], lo que ha incluido significativamente en la caracterización del *hacker* que, en los últimos años, o bien se convierte definitivamente en *cracker,* o bien centra sus actividades en el desarrollo de *software* abierto y otros proyectos como *creative commons* que se corresponden con sus principios éticos [25], e incluso se resitúa en el nuevo marco legal gracias a la explosión de las empresas tecnológicas, que están atentas a cualquier actividad innovadora en Internet para hacer propuestas a los mejores *hackers* e integrarles en el mundo empresarial. Hoy el *hacker,* pues, no sólo es el informático altruista que explora las barreras de redes y sistemas, sino que también es el informático que utiliza Internet como campo de pruebas con la finalidad de obtener beneficio económico de su actividad. A éste lo único que le diferencia de otros expertos informáticos que exploran los sistemas y las redes, acceden a ellas y cambian sus protocolos gracias a su conocimiento informático, es que los *crackers* obtienen sus beneficios de la actividad ilícita que desarrollan en Internet.

El término *cracker* comenzó a ser utilizado por los propios *hackers* para referirse a quienes utilizaban el acceso informático para robar información relevante o causar algún otro tipo de daño, y diferenciarlos así de quienes superaban las barreras de acceso por el mero hecho de hacerlo [26]. Estos

---

[22] Véase, aún con más vehemencia y claridad, RAYMOND, E. S., *How To Become A Hacker*, *op. cit.*

[23] NISSENBAUM, H., «Hackers and the contested...», *op. cit.,* pp. 195 y ss.

[24] Véase sobre ese proceso, el interesante estudio de THOMAS, J., «The moral ambiguity of social control in cyberspace: a retro-assessment of the "golden age" of hacking», en *NMS,* núm. 7, 2005, p. 607, en el que hace una revisión de decenas de artículos de prensa norteamericana en la que, a finales de los noventa, se comienza a identificar al *hacker* con todas las formas de criminalidad en Internet que comienzan a aparecer.

[25] WARK, M. K., «Hackers», en *TCS,* núm. 23, 2006, p. 321.

[26] SINROD, E. J., y REILLY, W. P., «Cyber-crimes...», *op. cit.,* p. 4.

son los *crackers*, cuya principal diferencia con los *hackers,* no es tanto su capacitación informática que se supone inferior a la de los *hackers* pero puede llegar a no serlo, como la finalidad delictiva o, en otros términos, la diferencia entre construir cosas y destruirlas [27]. Aunque la frontera entre *hackers* y *crackers* es tan estrecha que algunos de ellos la traspasan de forma constante, pasando de actividades lícitas a ilícitas y utilizando para ello *nicks* distintos. Muchos *crackers* son *hackers* que no encuentran una salida profesional o económica a su actividad y que la logran en el terreno de la ilegalidad. Son muchos los *crackers* que actúan en solitario que son captados (o instruidos) por las mafias organizadas para sus actividades en el ciberespacio, pero empieza a ser también habitual que los propios *crackers* conformen grupos, generalmente pequeños, aunque también hay otros transnacionales, dedicados específicamente a la cibercriminalidad [28]. Éstos son los cibergrupos o ciberbandas organizadas sobre las que se tratará después.

En la actualidad, gran parte de los *hackers-crackers* ya no son expertos informáticos sino que también comienzan a realizar tales actividades usuarios, generalmente jóvenes, con conocimientos básicos de informática que aprovechan programas y aplicaciones sencillas para realizar sus incursiones [29]. Éstos son los denominados *scriptkiddies* [30], pues aunque algunos actúan para lograr notoriedad, normalmente sus actividades no buscan crear y explorar, sino aprovechar vulnerabilidades y dañar. Los *scriptkiddies* son un fenómeno nuevo derivado de la popularización de Internet y de los propios conocimientos informáticos, que hace que sean muchos los que se animen a ser *hackers* pese a no disponer siempre de los conocimientos necesarios para ello. En todo caso, la de por sí naturaleza insegura de Internet hace que con unos mínimos conocimientos informáticos puedan ponerse en riesgo el patrimonio o la intimidad de innumerables personas [31], de forma que han aparecido todo un conjunto de sujetos que pueden realizar graves infracciones con importantes daños, sin tener unos conocimientos informáticos superiores al nivel de usuario, ni presentar especiales problemas de adaptación social [32]. Los *scriptkiddies* son, pues, jóvenes que no siendo expertos *hackers* capaces de acceder a sistemas mediante programaciones propias, realizan sus ataques informáticos, generalmente eligiendo las vícti-

---

[27] Raymond, E. S., *How to become a hacker*, *op. cit.,* pp. 1 y ss.

[28] Mcquade III, S. C., «Cybercrime...», *op. cit.,* p. 482.

[29] Véase, extensamente, Yar, M., *Cybercrime and society, op. cit.,* p. 32.

[30] En realidad, se trata de una forma despectiva de referirse a estos sujetos que, por tanto, no se llaman a sí mismos en esos términos. También se les denomina, bajo la misma idea de burlarse de ellos, *ankle-biters* o *packet monkeys*.

[31] Parliament of the Commonwealth of Australia: *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime. The Report of the Inquiry into Cyber Crime,* Canberra, junio de 2010, p. 4.

[32] Galán Muñoz, A., «Expansión e intensificación...», *op. cit.,* p. 19.

mas al azar [33], aprovechando programas y *scripts* básicos [34] y causando daños en muchos casos más fruto de su impericia o de la dañosidad del *malware* utilizado, que de sus habilidades. Los *scriptkiddies* no suelen, pues, realizar *hacking* al uso [35], sino que más bien se les relaciona con ataques de DoS y similares, pero también son reclutados por las bandas organizadas para la ejecución de sus ataques en Internet [36].

2. ESPECIALIDADES DEL PERFIL DEL CIBERCRIMINAL DERIVADAS DE LA MODALIDAD DE CIBERCRIMEN REALIZADO

2.1. El cibercriminal económico

Aunque, como hemos visto anteriormente, no son los ataques realizados con ánimo de obtener un lucro patrimonial los únicos crímenes que se realizan en el ciberespacio, sigue siendo con esta cibercriminalidad económica con la que se identifica el fenómeno del cibercrimen y al *hacker* en general. En el fondo esta percepción no está nada lejos de la realidad. La mayoría de los crímenes en el ciberespacio se realizan con intención económica, y ésa es con la que actúan la mayoría de los *hackers* (en este caso *crackers*) que ejecutan ataques de muchos tipos.

Los *hackers* económicos buscan vulnerabilidades, superan barreras en sistemas o en redes bien sean para el acceso a un sistema, para la configuración de una red telemática, o de cualquier otro tipo, interrumpen y saturan servidores y sistemas, o diseñan herramientas específicas con la intención final de obtener por su actividad un beneficio económico directo o indirecto en el caso de que sean *hackers* contratados por grupos organizados. Así son *hackers* económicos aquellos que desarrollan virus y demás modalidades de *malware*, generalmente como forma de potenciar vulnerabilidades en los sistemas informáticos o de crear *backdoors* para poder acceder a redes o

---

[33] Así, se señala que los *scriptkiddies* no tienen, como generalmente los *hackers,* un objetivo determinado, sino que utilizan modos de búsqueda en Internet de sistemas vulnerables y, una vez encontrados, tratan de explotarlos con sencillos programas.

[34] SPITZNER, L., *Know Your Enemy: The Tools and Methodologies of the Script Kiddie.* En Internet, en *http://www.firstvpn.com/papers/misc/KnowYourEnemy1.pdf* (última visita el 6 de diciembre de 2010, p. 1).

[35] Excepto en el caso del uso de programas de entorno gráfico de acceso ilegal, que pueden obtenerse gratuitamente en la Red como algunos *backdoors* de fácil uso, como son *Net Buso Back Orifice.* Así MORALES GARCÍA, Ó., «Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas», en QUINTERO OLIVARES, G., *La reforma penal de 2010. Análisis y comentarios,* Cizur Menor, Aranzadi, 2010, p. 184.

[36] En general, sobre el reclutamiento de *hackers* en Internet, GRABOSKY, P., «The Internet, Technology, and Organised Crime», en *AJC*, vol. 2, núm. 2, 2007, pp. 146 y ss.

sistemas [37]; también lo son los denominados *information warriors* que obtienen información y la transmiten al grupo organizado del que forman parte o a otros a cambio de dinero; y también los meros ladrones, que utilizan burdos engaños o técnicas más sofisticadas para hacerse con la información bancaria que después les permite acceder al dinero por medio de la banca *online* [38].

Como veremos a continuación, sin embargo, no sólo los *hackers* individuales y con conocimientos informáticos protagonizan los cibercrímenes económicos. En la actualidad los principales actores de tales delitos son las bandas organizadas para las que trabajan los propios *hackers*, y con ellos operan también como colaboradores *insiders* y mulas sin las que no sería posible el éxito de la cibercriminalidad.

2.1.1. *No sólo* hackers: *también* insiders *y especialmente grupos organizados*

Otro de los cibercriminales clásicos es el *insider* que pertenece o trabaja para la institución o empresa víctima de la infracción. Este último es precisamente uno de los principales protagonistas de los *data breaches*, aunque la evolución de las TIC ha cambiado en algo la caracterización del ciberviolador de datos. En efecto, y tal y como pusieron de manifiesto, entre otros, en los años setenta y ochenta, Ullrich Sieber en Alemania [39] y Romeo Casabona en España [40], la gran mayoría de las violaciones informáticas de datos en la empresa eran llevadas a cabo por empleados de las empresas víctima del ataque. La popularización y mundialización de la Red ha cambiado, sin embargo, esta proporción de sujetos protagonistas de los ataques, en el sentido de que, conforme indica el *informe Verizon,* hoy en el 70 por

---

[37] Se utiliza en castellano y dentro de la «jerga» de los propios *hackers*, el término *virucker*, para referirse a aquéllos que programan *malware* malicioso y realizan con él ataques a sistemas informáticos. Aunque algunos autores han tratado de encontrar caracteres sustanciales entre los *viruckers* distintos a los de los *crackers* (De la Cuesta Arzamendi, J. L., y Pérez Machío, A. I., «Ciberdelincuentes y cibervíctimas», *op. cit.,* p. 107), lo cierto es que en la actualidad en Internet, mientras que sí puede decirse que existen diferencias «de perfil», y no sólo relativas a la actividad que llevan a cabo, entre *hackers* y *crackers* (esencialmente el fin con el que actúan), y entre estos últimos y los *scriptkiddies* (la edad y, más allá, los conocimientos informáticos utilizados y la ausencia de ánimo de explorar las posibilidades del mundo informático en los últimos), no puede afirmarse lo mismo de estos *viruckers* (término que, por otra parte, no se utiliza en el mundo anglosajón). Son *hackers* y *crackers* los que actúan, realizando unos y otros, actividades de programación y de creación de virus. De hecho, la mayor parte de los virus difundidos a través de Internet, o los han creado *hackers* con propósitos comerciales para incluir *cookies* y otras formas de seguimiento y de incorporación de publicidad al sistema informático de un usuario, o son creados por *crackers* con propósito destructivo o para encontrar vulnerabilidades o abrir *backdoors* y acceder al sistema o tratar de controlarlo con ánimo malicioso.

[38] Rogers, M. K., «The Psyche of Cybercriminals...», *op. cit.,* p. 219.

[39] Sieber, U., *Computerkriminalität und Strafrecht, op. cit.,* p. 130.

[40] Romeo Casabona, C. M., *Poder informático...*, *op. cit.,* p. 36.

100 de las violaciones de datos intervienen sujetos que no tienen ninguna relación con la empresa frente al 48 por 100 de casos en los que interviene un *insider*[41]. Aun así, casi la mitad de los ataques de este tipo son realizados con deslealtad, por lo que no se trata de que haya disminuido el número de sujetos que aprovecha su condición en la empresa para violar los datos de su entidad, sino que ha aumentado exponencialmente el número de sujetos externos que puede violar tal tipo de información. Además, y como han señalado Pinguelo y Muller, si bien los ataques de los *insiders* no son tan frecuentes como los externos, la tasa de éxito de los primeros puede ser mucho mayor, dado que es más posible que pasen desapercibidos y suponen un riesgo, por el mayor acceso a la información, mucho mayor que los ataques externos[42].

En todo caso hoy no puede afirmarse, como se hace por algún autor, que la caracterización general del sujeto activo de los delitos informáticos (que en gran parte coincide con la cibercriminalidad como se explicó anteriormente) sea el *insider*[43]. Eso ya no es así ni siquiera para los *data breaches*. Más bien los estudios empíricos actuales confirman que los ataques externos son la gran mayoría y que los mismos vienen protagonizados por grupos organizados de cibercriminales.

En efecto, hoy puede decirse que el cibercrimen ha pasado de ser una infracción realizada por el inadaptado *hacker* a convertirse en un crimen cometido por el crimen organizado a nivel transnacional y con una potencial lesividad de enormes dimensiones[44]. Y es que cada vez destaca más la interrelación entre cibercriminalidad y delincuencia organizada. Bien sea por la tendencia general, destacada entre otros por Terradillos Basoco, a la aparición y proliferación de manifestaciones criminales de alcance transnacional[45], las cuales ya no se ocupan sólo de los delitos de tráfico de drogas, blanqueo de dinero fruto de actividades ilícitas, el tráfico de armas, etc., sino de cualesquiera otras actividades criminales que puedan ser lucrativas porque el propio uso de las TIC ha sido según todos los indicios una de las causas del éxito y expansión del crimen global[46], o por la unión de estos

---

[41] Baker, W. *et al.,* «2010 Data Breach Investigations Report. A study conducted by the Verizon RISK Team...», pp. 4 y ss.

[42] Pinguelo, F. M., y Muller, B. W., «Virtual Crimes, Real Damages...», *op. cit.*, p. 126.

[43] Así lo considera Galán Muñoz, A., «Expansión e intensificación...», *op. cit.,* p. 19, quien probablemente y aunque no lo especifique, se estará refiriendo a las violaciones de datos.

[44] Véase en este sentido, por citar algunos ejemplos de estudios empíricos en los que se analiza la relación entre el cibercrimen y la delincuencia organizada, el estudio del Parliament of the Commonwealth of Australia, *Hackers, Fraudsters and Botnets...*, *op. cit.,* pp. 9 y ss.

[45] Terradillos Basoco, J., «El Derecho penal de la globalización: luces y sombras», en *Transformaciones del Derecho en la mundialización,* Madrid, Consejo General del Poder Judicial, 1999, p. 187.

[46] Castells, M., *La era de la información. Vol. 3. Fin de milenio*, Madrid, Alianza Editorial, 2006, p. 141.

factores a las especiales características del ciberespacio anteriormente señaladas, muy particularmente su carácter transnacional, mundial, desregularizado y con tendencia al anonimato, que lo convierten en un ámbito de oportunidad de lucro económico como no lo ha tenido nunca la criminalidad organizada y con escaso riesgo para la detención policial [47], lo cierto es que hoy las TIC son una de las principales herramientas del crimen organizado, que es, por tanto, un importante sujeto activo de los delitos cometidos en el ciberespacio [48].

En realidad, como ha señalado Williams, al igual que han hecho muchas empresas que han tenido que «trasladarse» al ciberespacio para realizar sus actividades económicas, las «empresas criminales», con similar filosofía, están aprovechando las oportunidades del medio para continuar con sus actividades criminales [49]. En otras palabras: el ciberespacio es para los grupos y bandas organizadas el área de desarrollo emergente más importante del siglo XXI [50]. Esto deriva tanto de las múltiples actividades ilícitas muy lucrativas que pueden llevar a cabo las bandas organizadas en el espacio virtual, de la facilidad para el anonimato que seducen significativamente a los grupos criminales, como de las propias mejoras que el uso de las TIC conlleva para la realización de actividades criminales tradicionales, como muy especialmente de las características del ciberespacio de transnacionalidad.

En cuanto a esto último, y como ha señalado Choo, son múltiples las pruebas que demuestran que las bandas organizadas se han aprovechado de las TIC para facilitar o mejorar la comisión de delitos, para identificar nuevas oportunidades o para luchar contra las medidas policiales de los Estados destinadas a evitar sus actividades. Estos grupos se han adaptado a los cambios tecnológicos y han aprovechado las TIC para facilitar sus lucrativas actividades criminales en el espacio físico tales como el narcotráfico, la trata de personas, etcétera [51]. Pero, además, el ciberespacio se ha convertido en un nuevo ámbito de actividad de las organizaciones criminales. El ciberespacio ofrece a las organizaciones criminales clásicas unas posibilidades de expansión de sus actividades a otros Estados y a otras víctimas que serían prácticamente imposibles en «el mundo real», por lo que a las citadas actividades delictivas tradicionales se unen ahora otras como el tráfico de secretos empresariales obtenidos por Internet, la extorsión y los ciberfraudes, el

---

[47] Factor que, según McCusker, R., «Transnational organised cyber crime: distinguishing threat from reality», en *CLSC,* 46 (4-5), 2006. p. 273, es determinante en la entrada de las bandas organizadas tradicionales en la cibercriminalidad.

[48] Choo, K. K. R., «Organised crime groups in cyberspace: a typology», en *TOC,* 2008, núm. 11, p. 272.

[49] Williams, P., «Organized Crime and Cybercrime...», *op. cit.,* p. 2.

[50] Chatterjee, J., *The Changing Structure of Organized Crime Groups* (2005), *Royal Canadian Mounted Police*. En Internet, en *http://dsp-psd.pwgsc.gc.ca/Collection/PS64-9-2005E.pdf* (última visita el 6 de diciembre de 2010).

[51] Choo, K. K. R., «Organised crime groups...», p. 273.

blanqueo de dinero a través de sistemas de pago *online*, la distribución ilegal de materiales a través de Internet y el uso de Internet como un mercado de venta ilegal de productos falsificados y drogas farmacéuticas.

Resulta lógica la expansión de las actividades de las bandas criminales organizadas al ciberespacio. Hay que tener en cuenta que la transparencia y el secretismo son valores importantes para el desarrollo estratégico de las organizaciones criminales, por lo que el mayor anonimato que Internet garantiza a las acciones delictivas llevadas a cabo en él desde cibercafés, locutorios telemáticos o por otros medios más sofisticados como la infección de *bots*, ofrece a las bandas criminales una seguridad mayor que la que puede tener en «el mundo real» [52]. Si a ello sumamos, por último, las dificultades para la persecución de estas infracciones, entenderemos lo cómodas que están las organizaciones criminales en el nuevo espacio virtual universal.

Dentro de este fenómeno de unión entre cibercriminalidad y delincuencia organizada, hay que diferenciar, sin embargo, entre las organizaciones tradicionales (mafia siciliana, mafias rusas, tríadas chinas o yakuzas, etc.) que suman a sus múltiples actividades la realización de delitos por medio de Internet, y aquellas otras ciberbandas organizadas o conjunto de *crackers* que se organizan como grupo criminal y cuyo único ámbito de actuación es el ciberespacio [53].

Las primeras, los grupos organizados clásicos operando en Internet, comenzaron su relación con el ciberespacio en ámbitos muy específicos de transmisión de contenido como la pornografía infantil o la piratería intelectual a través de la distribución callejera de archivos y mediante la explotación de inmigrantes para la ejecución de los hechos [54], pero pasaron pronto a ampliar sus actividades criminales al ámbito de la defraudación bancaria interviniendo en fraudes de tarjetas de crédito [55]. En la actualidad, la intervención de la criminalidad organizada en el ciberespacio abarca, como se ha dicho, prácticamente todas las formas de comportamiento delictivo en Internet (si quitamos conductas como el *ciberbullying,* el *child grooming* o similares), si bien centrándose especialmente en las distintas formas de fraude, por

---

[52] Williams, P., «Organized Crime and Cybercrime...», *op. cit.,* p. 3. No hay que olvidar, sin embargo, que Internet también «deja huella», y que un uso descuidado de la misma por parte de las organizaciones criminales puede ayudar a localizarlas o a impedir algunas de sus actividades, dado que no es fácil borrar el rastro en el ciberespacio una vez se deja.

[53] Así lo hacen, también, De la Corte Ibáñez, L., y Giménez-Salinas Framis, A., *Crimen. org. Evolución y claves de la delincuencia organizada,* Barcelona, Ariel, 2010, pp. 391 y ss.

[54] Walterbach, M., «International illicit convergence: the growing problem of transnational organized crime groups' involvement in intellectual property rights violations», en *FSULR*, vol. 34, núm. 2, 2007, p. 592.

[55] Así, relata Williams, P., «Organized Crime and Cybercrime...», *op. cit.,* p. 6, que ya en septiembre de 1999 fue condenado un grupo denominado Phonemasters, por fraudes a compañías telefónicas y bancarias, que se dedicaba a descargar miles de números de tarjetas de crédito y que terminaron finalmente en manos de la mafia italiana.

ser las más beneficiosas económicamente [56]. Generalmente las formas más burdas de *phishing* y de ataques *scam*, provienen de mafias y bandas organizadas clásicas que comienzan a actuar en el ciberespacio [57], a las cuales hay que sumar el *skimming*, conducta que no es propiamente un ciberataque [58]. Su evolución, sin embargo, es imparable hacia el aumento de la sofisticación de los ataques: por medio del reclutamiento de *hackers* e incluso de la financiación de sus estudios para la mejora de sus conocimientos [59]; todo lo cual hace que hoy se haya identificado la presencia de bandas organizadas en la ejecución de casi cualquier tipo de ciberataque desde el *spam*, infección de *bot*, *spoofing* e *identity theft* y envío de *malware*, entre otros [60].

Como se ha señalado anteriormente, además de la interconexión entre bandas organizadas tradicionales y el cibercrimen, existen en la actualidad grupos de *hackers* que actúan como cibercriminales de forma organizada. Pese a que se señaló por parte de algunos autores la dificultad de que el crimen organizado con su estructura jerarquizada tuviera éxito en el ciberespacio [61], y aunque se hayan presentado generalmente los *hackers* como personas aisladas socialmente que se recluyen del mundo real, la realidad actual es que existen bandas organizadas de hackers (en este caso se podría hablar de *crackers*) y que los mejores *de ellos* están activamente involucrados en grupos de este tipo [62]. Ya sea intercambiando opinión e información, suministrándose unos a otros apoyo, o más allá de ello, preparando ataques conjuntos en los que se dividen los roles y las funciones para lograr un objetivo común, cada vez es más frecuente la colaboración entre cibercriminales, algunos de los cuales acaban formando grupos dedicados a la realización de actividades ilícitas. La literatura especializada señala que la forma de organización de

---

[56] Aunque no sólo, dado que estos grupos organizados también realizan otros cibercrímenes, por su finalidad económicos pero atentatorios de bienes jurídicos muy distintos, como la distribución de pornografía infantil.

[57] De la Corte Ibáñez, L., y Giménez-Salinas Framis, A., *Crimen.org. Evolución y claves de...», op. cit.,* pp. 390 y s.

[58] El *skimming* es la obtención de información relativa a tarjetas de crédito bien mediante engaño o gracias a la utilización de técnicas de clonado o de fotografía o de grabación de la actividad de una tarjeta de crédito con la intención de usar tales datos para el posterior fraude. Ya sea por medio de microcámaras, de dispositivos incorporados a la ranura de los cajeros automáticos que clonan la banda magnética, o de engaños más burdos realizados en conjunción con camareros o vendedores cómplices que pasan la tarjeta al sujeto que las clona cuando el cliente no lo ve, el *skimming* es una técnica habitual que produce muchas pérdidas.

[59] De la Cuesta Arzamendi, J. L. (dir.), y De la Mata Barranco, N. J. (coord.), *Derecho penal informático, op. cit.*

[60] Véase el completo estudio de Choo, K. K. R., «Organised crime groups...», *op. cit.,* pp. 274 y ss., en el que se recogen ejemplos de estos y otros ciberataques cometidos presuntamente por bandas organizadas tradicionales que se incorporan al ciberespacio.

[61] En este sentido Brenner, S. W., «Organized Cybercrime? How Cyberspace May Affect the Structure of criminal Relationships», en *NCJOLT*, vol. 4, núm. 1, 2002, pp. 41 y ss., y también McCusker, R., «Transnational organised cyber crime...», *op. cit.,* pp. 257-273, si bien poniendo en boca de Nisbet lo que afirma en realidad Brenner.

[62] Brenner, S. W., «Organized Cybercrime?...», *op. cit.,* pp. 41 y ss.

los grupos criminales cuando operan en el ciberespacio no es la misma que la de las organizaciones tradicionales con las que, por otra parte, muchas veces se relacionan. Más bien se trata en el caso de las primeras de estructuras descentralizadas y flexibles formadas por miembros de gran variedad de países, que no tienen por qué funcionar con estructura jerarquizada sino que los miembros pueden actuar conjuntamente pero con cierta independencia e incluso manteniendo el anonimato [63]. Al fin y al cabo, y como señala Brenner, la propia naturaleza del ciberespacio viene a ser incompatible con la jerarquía: el ciberespacio es una red de redes laterales que es difusa, fluida y en evolución, mientras que las jerarquías son verticales, concentradas y tienden a ser rígidas y fijas; de forma que las estructuras organizativas jerárquicas no son ni necesarias ni apropiadas para las actividades realizadas en el ciberespacio [64].

Esta idea de la estructura horizontal, casi difusa, de las ciberbandas criminales concuerda con una de las características más particulares que se atribuyen a estas organizaciones delictivas: el que habitualmente los miembros de las mismas no tienen entre sí ningún tipo de contacto físico directo sino que sólo se conocen a través de Internet, en ocasiones desconociendo incluso la identidad real del sujeto y teniendo como única referencia algún tipo de pseudónimo, *nick* o nombre clave. Al fin y al cabo, esto es perfectamente coherente con la naturaleza y posibilidades que ofrece el ciberespacio: la conjunción de personas situadas en lugares distantes entre sí pero unidas por ideas afines y/o por idénticos propósitos, para lo cual colaboran por medio de una estructura de organización de trabajo conjunto [65]. Aunque no es fácil la constatación de tal forma de estructuración del grupo debido a la dificultad que plantea el enjuiciamiento del cibercrimen, Choo aporta varios ejemplos de esta modalidad de ciberbandas como la del grupo clandestino Shadowcrew que llegó a la defraudación *online* de más de 1,7 millones de tarjetas de crédito [66].

Junto con los *insiders* y los grupos organizados, y especialmente relacionados con éstos, otros intervinientes relevantes en la cibercriminalidad son las mulas. Tanto los grupos tradicionales que actúan en el ciberespacio como los cibergrupos organizados se sirven para la realización de sus actividades de las denominadas cibermulas [67]. En realidad, las cibermulas no son, desde una perspectiva criminológica, cibercriminales, puesto que no son autores del delito en el ciberespacio sino colaboradores o recolectores de los be-

---

[63] Parliament of the Commonwealth of Australia, *Hackers, Fraudsters..., op. cit.,* p. 61. Véase también Brenner, S. W., «Organized Cybercrime?...», *op. cit.,* p. 39.

[64] *Ibid.* Añade la autora que el ciberespacio es una red, o, más correctamente, una red de redes.

[65] Choo, K. K. R., «Organised crime groups...», *op. cit.,* p. 277.

[66] *Ibid.,* p. 278.

[67] *Ibid.,* p. 271.

neficios en Internet que luego envían por medios seguros de transmisión el dinero a los autores del delito (las ciberbandas) o a los responsables de los grupos organizados tradicionales que operan en Internet. Las cibermulas son reclutadas por Internet bajo la promesa de la recepción de importantes cantidades de dinero que tienen que transmitir quedándose un tanto por cien como ganancia [68]. Generalmente estas cibermulas son las únicas detenidas por estos delitos y pueden ser hechas responsables de los mismos como cooperadores necesarios o cómplices.

En los últimos tiempos está apareciendo un nuevo tipo de mula en el que el engaño es algo más elaborado. Se trata del *reschipper* o reenviador, que se diferencia de la mula en que ya no envía cantidades de dinero a través de Western Union o MoneyGram, sino que envía paquetes de bienes comprados por Internet por medio de cuentas corrientes ajenas a las que se ha accedido por medio de *phishing*. Debido a que las mulas cada vez son más conscientes del riesgo y, por tanto, se reduce su número, las mafias organizadas que operan en el ciberespacio y ciberbandas optan por comprar bienes y enviarlos fuera de Estados Unidos, para lo cual necesitan un ciudadano americano que realice el envío. Este nuevo tipo de mula o reenviador es reclutado del mismo modo que las mulas, por medio de ofertas de empleo en las que se promete un sueldo a cambio de reenviar paquetes bajo argumentos variados. En ocasiones, incluso, según ha recogido el IC3, se llegan a entrabar aparentes relaciones sentimentales con la víctima y, con la excusa de que el enamorado no puede recibir sus paquetes al estar fuera de Estados Unidos, le empiezan a llegar paquetes al *reschipper* que, cuando pregunta y se da cuenta del engaño, deja de recibirlos [69].

Por último, y siguiendo la acertada clasificación de Choo, a los grupos organizados tradicionales que utilizan el ciberespacio para la comisión de nuevos delitos, y las nuevas ciberbandas que operan específicamente en el ciberespacio, habría que sumar un tercer tipo, el de los grupos organizados motivados política o ideológicamente que utilizan las TIC para facilitar sus objetivos criminales [70]. Evidentemente se refiere Choo a los grupos terroristas o a otros grupos relacionados con el *hacktivismo* que utilizan el ciberespacio como forma de difusión de sus mensajes e incluso de ejecución de sus ataques. Este tipo de grupos serán analizados posteriormente cuando nos refiramos a la cibercriminalidad política.

---

[68] Véase *supra* cap. II.

[69] En Internet, en *http://www.ic3.gov/crimeschemes.aspx#item-5.*

[70] Choo, K. K. R., «Organised crime groups...», *op. cit.,* p. 271.

2.1.2. *Perfil del cibercriminal económico: ¿delincuente común, de cuello blanco, socioeconómico o universitario? La cuestión de la tecnificación del cibercriminal económico*

Aunque se haya llegado a la conclusión de que gran parte de los cibercrímenes económicos son llevados a cabo por *hackers* en el seno de organizaciones criminales, conviene que nos preguntemos quiénes son esos *hackers* que conforman o son reclutados por grupos o que actúan en solitario pero con finalidad de fraude económico. Lo cierto es que pese al gran número de artículos existentes sobre los *hackers*, apenas existen estudios criminológicos contrastados que den luz sobre el perfil del ciberdelincuente económico. Quizá no nos debiera extrañar: el fenómeno todavía es muy nuevo y, además, aun son pocos los detenidos por estas infracciones en comparación con la significación del fenómeno, debido entre otros factores a la complejidad para su identificación y su procesamiento. Aun así, y desde los datos existentes, se suele admitir generalmente como punto de partida que el perfil del cibercriminal (económico) no coincide en cuanto a nivel de estudios, estrato social, etc., con el perfil del delincuente común [71]. Pero ¿a qué perfil de delincuente común se refieren? Tratándose de criminales que actúan bajo una motivación económica, podríamos plantearnos si estos cibercriminales concuerdan con el perfil, bien de los delincuentes comunes, autores de hurtos, robos, pequeñas estafas y otras defraudaciones patrimoniales, o bien de los delincuentes de cuello blanco, categoría de extrema ambigüedad [72], y en todo caso reconocida como excesivamente amplia por la criminología moderna [73], dentro de la cual se admite la existencia de la delincuencia lle-

---

[71] KSHETRI, N., «The simply economics on cybercrime...», *op. cit.,* p. 34.

[72] Véase al respecto, el interesante análisis de NELKEN, D., «White-Collar crime», en MAGUIRE, M.; MORGAN, R., y REINER, R., *The Oxford handbook of criminology,* 2.ª ed., New York, Oxford University Press, 1997, pp. 891 y ss., especialmente en el capítulo que titula «los siete tipos de ambigüedad de la delincuencia de cuello blanco», *op. cit.,* pp. 895 y ss.

[73] Desde que Sutherland acuñara el término de delincuencia de «cuello blanco» para referirse a los delitos cometidos por personas de respetabilidad y estatus social alto, y aprovechando para ello el curso de sus ocupaciones, el concepto ha sufrido un proceso de difusión y generalización que ha hecho que debamos replantearnos la necesidad de un ajuste a características distintas, que viene demandado —especialmente— por una nueva perspectiva originada por la combinación de la utilización de las nuevas tecnologías y los cambios socioculturales y económicos desarrollados desde la primigenia afirmación del mencionado autor. Efectivamente, hace tiempo que se ha mostrado necesario distinguir entre ese concepto original, y nuevos fenómenos delictivos relacionados con el ámbito socioeconómico, pero que no ponen tanto el acento en ese alto estatus social y económico de sus autores. HERRERO, C., «Capítulo 33: Los delitos socioeconómicos», en HERRERO, C., *Criminología (Parte General y Especial),* Madrid, Dykinson, 1997, p. 588. De ahí que actualmente se distinga entre diferentes tipologías delictivas relacionadas con este ámbito, como los delitos corporativos, los incidentales, o los denominados de empleados que no tienen por qué ser cometidos por individuos con esas especiales características remarcadas por Sutherland. Así lo hacen, por ejemplo, Garrido Genovés y Sanchís Mir —citando a Clinard y Quinney— al definir los delitos corporativos como aquéllos cometidos por la propia corporación o sus directivos, para obtener beneficios para

vada a cabo por las élites sociales como delincuencia de cuello blanco en sentido estricto, pero también la denominada delincuencia de cuello gris, la perpetrada por la creciente masa gris de los ejecutivos o empleados con un cierto poder de decisión económica para conseguir más fácilmente sus propios e ilegales fines, muchas veces amparados y estimulados por la posesión de unos conocimientos técnicos e informáticos especializados [74].

Aparte de las dudas que, para la criminología actual, ofrece la diferenciación del delincuente económico basado en el distinto estrato social que ocupa el criminal, no hay que olvidar como han señalado Chiesa *et al.,* que Internet parece igualar ese tipo de diferencias [75]. Quizá por ello sea mejor acercarse al perfil del delincuente socioeconómico, concepto que emplea Edelhertz y en el que integra a personas que cometen delitos contra el patrimonio a través de medios no físicos, y mediante ocultación y/o engaño [76], y que ha venido popularizándose en la criminología para ubicarse a modo de categoría intermedia entre los verdaderos delincuentes de «cuello blanco» clásicos y los tradicionales delincuentes contra la propiedad. A esta conclusión llegarían también Benson y Simpson quienes en la denominada «investigación Yale» [77], integran a los autores de fraudes informáticos dentro de los delincuentes socioeconómicos para extraer de su estudio las diferencias entre éstos, los delincuentes comunes y la población general [78], con los siguientes resultados:

---

la empresa, o los delitos ocupacionales, que son los cometidos por los individuos en beneficio de sí mismos y normalmente en el curso de sus ocupaciones. Dentro de esta última categoría se pueden distinguir, a su vez, dos clases de situaciones que muestran características diferenciadas: los delitos incidentales, que son los cometidos por determinados individuos aprovechando una ocasión favorable, o los delitos «de empleados», que son los abusos cometidos por éstos aprovechando la confianza depositada en ellos por la empresa o sus directivos (GARRIDO, V., y SANCHÍS, J., *Delincuencia de «cuello blanco»,* Editorial Instituto de Estudios de Policía. Colección «Politeia», núm. 1, 1987, p. 30).

[74] Y es que el desarrollo tecnológico, informático y burocrático ha provocado que las características de la actual delincuencia económica lleven consigo una mayor posibilidad de proliferación de esta nueva figura delincuencial, intermedia entre la delincuencia puramente económica y la de «cuello blanco». Y nuevas modalidades delictivas (o, más concretamente, nuevas formas de delitos de siempre), además de un círculo más amplio de víctimas potenciales (GARRIDO, V.; STANGELAND, P., y REDONDO, S., *Principios de Criminología*, *op. cit.*).

[75] CHIESA, R.; DUCCI, S., y CIAPPI, S., *Profiling Hackers...., op. cit.,* pp. 1 y ss.

[76] GARRIDO, V., y SANCHÍS, J., *Delincuencia de «cuello blanco»..., op. cit.,* p. 23.

[77] Realizada mediante una revisión de sentencias de ocho tipos de delitos socioeconómicos (vulneraciones de seguridad empresarial, delitos contra la propia empresa, sobornos, desfalcos bancarios, fraudes en el ámbito de las telecomunicaciones, defraudaciones de impuestos, falseamiento de contabilidad y/o salarios y defraudaciones relacionadas con créditos o instituciones crediticias) de tribunales de Los Ángeles, Atlanta, Chicago, Baltimore, Nueva York (Manhattan y Bronx), Dallas y Seattle (BENSON, M., y SIMPSON, S., *White collar crime: an opportunity prespective,* Routledge, 2009, p. 21).

[78] Si bien en el cuadro se refieren gramaticalmente a los delincuentes de «cuello blanco», señalan anteriormente —en la misma obra— que lo hacen más bien en el concepto que emplea Edelhertz, el cual indica que se trata de personas que cometen delitos contra el patrimonio a través de medios no físicos, y mediante ocultación y/o engaño. Lo cual, básicamente, coincide con el

Tabla 4.1. Resultados de la denominada «investigación Yale».

	Delincuentes comunes	*Delincuentes socioeconómicos*	*Población general*
Sexo masculino	68,6%	85,5%	48,6%
Raza blanca	34,3%	81,7%	76,8%
Media de edad	30	40	30
Educación			
Secundaria	45,5%	79,3%	69,0%
Universitaria	3,9%	27,1%	19,0%
Empleo			
Desempleado	56,7%	5,7%	5,9%
Contrato fijo	12,7%	58,4%	No disponible

En resumen, las características que diferencian a los delincuentes socioeconómicos, según los resultados del estudio mencionado son que se trataría en su gran mayoría de hombres [79] que provienen de un entorno social y demográfico diferente al de los delincuentes comunes, y que —en comparación con estos últimos—, tienen una edad media mayor, hay una mayor probabilidad de que sean casados y con hogar propio, son económicamente estables, su nivel de educación es superior a la población general (y especialmente más elevado que el de los delincuentes comunes) y tienen trabajo; y no coincidían mucho con el perfil de respetabilidad y alto estatus social de los delincuentes de la definición de Sutherland [80]. Conforme a otros estudios [81], otra característica de este tipo de delincuentes es que se tienen a sí mismos en alta consideración, no se autoconceptúan como delincuentes, ni creen del todo que sus actividades sean delictivas.

---

concepto manejado aquí como delincuencia socioeconómica, más que con el de «cuello blanco» de Sutherland.

[79] Algunas investigaciones parecen sugerir diferencias en función de la clase de delitos, aun cuando éstos se cometan como delincuencia «de empleados». Por ejemplo, Robin (ROBIN, G., «Employees as Offenders», *op. cit.,* p. 20), encontró que el 93 por 100 de los encargados de las cajas que habían llevado a cabo conductas reprobables eran mujeres. Pero es que, en este caso, parece tratarse de delincuencia «de empleados» de tipo puramente patrimonial, y sin las características propias de los delitos socioeconómicos.

[80] Lo que viene a confirmar la hipótesis de la diferencia entre los conceptos de delincuente de «cuello blanco» y delincuente socioeconómico.

[81] Muchos autores, como por ejemplo Geis y Meier Sutherland, Clinard y Quinney, aseguran que tal vez sea una de las características más diferenciadoras y uno de los resultados más consistentes de las investigaciones en este ámbito, siendo habitual en ellos el uso de racionalizaciones y técnicas de neutralización (GARRIDO, V., y SANCHÍS, J., *Delincuencia de «cuello blanco»..., op. cit.,* p. 104).

Algunas de estas características pueden cuadrar con el prototipo de *hacker* dedicado a la criminalidad económica: especialmente el nivel de educación [82, 83] y el ser económicamente estables, así como el verse como personas brillantes y, por el contrario, el no considerarse a sí mismos como delincuentes ni estimar sus conductas como ilícitas [84] y el género masculino en un mundo criminal en el que, sin embargo, empiezan a aparecer las mujeres [85]. Por el contrario, la edad media de los cibercriminales parece alejarse de la de este perfil general de los delincuentes socioeconómicos. Gran parte de ellos son, como ya hemos visto, jóvenes que son reclutados por las organizaciones por sus conocimientos de informática y su voluntad de ganar dinero fácil, por lo que los estudios de *profiling* cifran lejos de los cuarenta, e incluso de los treinta, y más cerca de los veinte o veinticinco años, la edad media de unos cibercriminales que, sin embargo, en los últimos años ha aumentado un poco [86]. Tampoco parece que tengan que pertenecer a un estrato social alto: los cibercriminales reclutados por las bandas pueden serlo de cualquier clase social, hasta el punto de que muchos de ellos utilizan herramientas informáticas muy básicas [87]. En realidad esto deriva del efecto democratizador del

---

[82] Así lo indican por ejemplo los estudios realizados por KSHETRI, N., «The simple economics...», *op. cit.,* p. 34, y muy particularmente el de JEN, W.; CHANG, W., y CHOU, S., *Cybercrime in Taiwan: an analysis of suspect records. Paper to Workshop on Intelligence and Security,* 2006, pp. 38 y ss., en el que se analizaba, entre otras variables, el nivel educativo de personas sospechosas de cibercrímenes. Los resultados de la investigación eran bastante significativos: la mayoría de los sospechosos detenidos tenían por lo menos el alto diploma de secundaria que vendría a corresponderse al bachillerato (45,5 por 100), siendo el segundo grupo más grande el de graduados universitarios (27,8 por 100), el tercero el de los diplomados en escuela secundaria o nivel inferior al del bachillerato (17,9 por 100) y abarcando otros el 8,9 por 100 restante. En otras palabras, y conforme al estudio, de 1999 a 2004, el 80 por 100 de los casos de delitos cibernéticos fueron cometidos por personas con formación en la escuela secundaria, bachillerato y universidad, mientras que en ese mismo período el total de delitos denunciados a la policía fueron ejecutados por personas con formación en la escuela primaria, secundaria y bachillerato. O de otro modo: las personas que cometieron cibercrímenes en Taiwán con nivel de educación primaria fueron sólo el 5,3 por 100, frente al 13,0 por 100 en la criminalidad global; los presuntos autores de cibercrímenes con formación universitaria ascendían al 27,8 por 100 frente al 8,0 por 100 de los sospechosos de cualquier otro delito. Si bien señala Choo que tales afirmaciones pueden ser discutibles, dado lo poco extrapolables que resultan los estudios debido especialmente al escaso tamaño de las muestras.

[83] Por otra parte recuerda Chiesa que el que sean personas con estudios no significa que tengan brillantes resultados en ellos, dado que en muchas ocasiones su interés por la informática les hace bajar el rendimiento. CHIESA, R.; DUCCI, S., y CIAPPI, S., *Profiling hackers..., op. cit.,* p. 98.

[84] CHIESA, R.; DUCCI, S., y CIAPPI, S., *Profiling hackers..., op. cit.,* p. 91.

[85] Señalan Chiesa, Ducci y Ciappi (*ibid.,* p. 90), que el mundo *hacker* comenzó siendo absolutamente masculino en los años setenta y ochenta, si bien desde los años noventa las mujeres han comenzado progresivamente a incrementar su presencia y a ser más relevantes en la actividad *hacker*, y parece que este crecimiento está comenzando a ser exponencial en los últimos años.

[86] En efecto, los autores del Proyecto hpps señalan que si bien no hay limitaciones la gran mayoría de los *hackers* pertenecen a la franja de edad adolescente, si bien en los últimos años ha comenzado a aumentar la edad de quienes comenzaron sus actividades hace 10 o 15 años y ahora están cerca de los 30 o 35 años. Según *ibid.,* p. 91.

[87] *Ibid.,* p. 95.

ciberespacio: no es necesario nada más que ligeros conocimientos informáticos, ni siquiera una terminal propia, para convertirse en un cibercriminal y tratar de defraudar a otras personas en el ciberespacio. Eso sí, y quizás por la clara unión entre nuevas tecnologías y desarrollo urbano, aunque los cibercriminales lo pueden ser de cualquier parte del mundo lo serán, generalmente, de ciudades o zonas cercanas a ellas [88].

En definitiva, aunque el cibercriminal económico está más alejado del perfil del delincuente común que de aquél del delincuente socioeconómico, tampoco se puede decir que ambos coincidan ni se acerquen. Lo están en el nivel educativo y, por supuesto, en la finalidad criminal, pero es evidente que el ciberespacio, con su capacidad democratizadora que iguala estratos y potencia a los jóvenes por su mayor conocimiento de las nuevas tecnologías, ha potenciado un nuevo tipo de delincuente económico que lleva zapatillas o chaqueta de cuero y va a la facultad o que no tiene trabajo pero sí un ordenador, pero que tiene capacidad para causar enormes daños económicos a nivel transnacional, especialmente si forma un grupo organizado o si es reclutado por uno de ellos para obtener dinero más fácilmente y causar un daño aún mayor.

Esto enlaza, pues, con la cuestión de la tecnificación de los cibercriminales económicos, esto es, la de hasta qué punto es necesaria una alta cualificación en conocimientos informáticos para ser un criminal que opere en una banda organizada. Aunque como se dijo es perfectamente posible la realización de un cibercrimen económico sin gozar apenas de conocimientos informáticos más allá de lo básico, la cibercriminalidad económica lleva aparejada generalmente un alto nivel de tecnificación, especialmente en los últimos años en los que las inversiones en seguridad informática están comenzando a ser muy altas, y sobre todo cuando hay un objetivo preciso para el ciberataque y no se trata de un mero aprovechamiento de una oportunidad [89].

Precisamente por ello el *hacker* (en este caso *cracker*) que realiza cibercrímenes económicos o que, como se verá, forma parte de una organización criminal que opera en el ciberespacio, suele tener un alto nivel de conocimientos informáticos. Así, señala Choo, que el cibercriminal que actúa a alto nivel bien de forma particular o, más generalmente, como parte de una estructura organizada, está obligado a poseer un nivel mínimo de conocimientos técnicos y habilidades de la computadora como el conocimiento del *software* y las vulnerabilidades de *hardware* y de cómo estas vulnerabilidades pueden ser explotadas, comprensión de los sistemas de archivos y sistemas operativos, así como conocimientos de programación [90].

---

[88] *Ibid.,* p. 91.

[89] Así, KSHETRI, N., «Pattern of global cyber war and crime: A conceptual framework», en *Journal of international Management,* 11, 4, 2005, p. 247.

[90] CHOO, K. K. R., «Organised crime groups...», *op. cit.,* p. 277.

2.2. *Ciberhacktivistas,* ciberterroristas y demás cibercriminales políticos

Ya se anunció anteriormente que no es posible una caracterización general de los cibercriminales intervinientes en la que hemos venido en denominar cibercriminalidad política, puesto que la misma engloba todos los delitos en Internet realizados con un objetivo político o ideológico y, por tanto, figuras tan distintas entre sí y en las que los protagonistas divergen tanto como el *ciberhacktivismo* concretado en ataques de DDoS, el *cyberhate* o *hate speech* plasmado en páginas web de difusión de odio racial, la ciberguerra llevada a cabo por servicios de inteligencia de Estados contra recursos de otros Estados, o el ciberterrorismo, en el que los grupos organizados aprovechan Internet para la difusión de sus contenidos, de sus propósitos, para la captación de nuevos miembros o para la preparación de nuevos ataques.

De nuevo, por tanto, el objetivo de este punto del libro es la categorización de los distintos tipos de cibercriminales existentes en el ciberespacio. Esto deja fuera del análisis, por tanto, a gran parte de los *hackers* que actúan en el ciberespacio con un propósito ideológico generalmente relacionado con la difusión del mensaje de la libertad en el ciberespacio y que no cometen ningún tipo de conducta delictiva. Es indudable, sin embargo, que este grupo va a ir viéndose reducido significativamente en los próximos años, y no tanto por una presunta radicalización de los *hacktivistas* sino por la tendencia de los Estados a criminalizar gran parte de las conductas que ellos realizan. Como se ha señalado anteriormente, la tipificación del *hacking* como conducta delictiva supone la conversión en delincuentes de los *hackers* o personas que acceden ilícitamente en sistemas informáticos ajenos, y ello sea cual sea su propósito. Lo mismo ocurre con los ataques de denegación de servicio. Es ésta una de las principales armas reivindicatorias utilizadas por los *hacktivistas* y su comisión a partir de la reforma de 2010, sea cual sea el propósito y sea cual sea el objetivo, siempre que se considere como grave, resultará delictiva. Y esto hace que, en definitiva, pueda afirmarse que hoy se ha criminalizado gran parte del *hacktivismo* y que tal forma de protesta política en el ciberespacio sea delictiva pese a que en ningún caso tales sujetos se vean a sí mismos, probablemente con razón, como ciberterroristas [91].

Comenzando ya, pues, con el análisis de las principales características y tipologías de autores de cibercrímenes políticos en el ciberespacio, lo primero que debe afirmarse es que tanto el *ciberhacktivismo* como el ciberterrorismo suelen realizarse en grupos más o menos organizados [92], si bien de nuevo, y al igual que ocurría con la cibercriminalidad económica, las características

[91] Fitri, N., «Democracy Discourses through the Internet...», *op. cit.,* p. 9.
[92] Choo, K. K. R., «Organised crime groups...», *op. cit.,* pp. 278 y ss.

del ciberespacio conllevan que el funcionamiento de los mismos sea distinto al de los grupos organizados criminales que operan en el espacio físico. De nuevo existe poca información concreta sobre las características organizativas de estos grupos, pero los estudios existentes y las intervenciones policiales sobre algunos de estos grupos muestran que se trata de agrupaciones en forma de células horizontales unidas en lo vertical únicamente por un mensaje o idea común que se transmite a todas y que cada una de ellas ejecuta a su propio modo. Esta estructuración propia del terrorismo de Al Qaeda, puede estar presente de forma más tenue en los grupos terroristas más tradicionales que operan en el ciberespacio y que siguen bajo estricto orden jerárquico, pero sobre todo lo está en el terrorismo yihadista que utiliza el ciberespacio como forma de transmisión global de mensajes de odio y de incitación a la violencia.

Más curioso es, en cambio, que este mismo tipo de funcionamiento organizativo en el que el único orden jerárquico es ideológico o «de mensaje» existiendo a partir de ahí unas relaciones horizontales y no verticales entre todos los miembros del grupo, parece imperar también en el *hacktivismo,* tal y como muestra, según los datos existentes hasta el momento, el desarrollo del grupo Anonymous.

Quizá el grupo *hacktivista* más importante, o por lo menos el que más relevancia mediática ha adquirido en los últimos años ha sido Anonymous, formado por *hackers* que venían realizando actividades *hacker* en general y ataques DDoS en particular contra distintos Estados y organizaciones empresariales, pero que saltó a la palestra a finales de 2010 en relación con el fenómeno Wikileaks [93], si bien sus principales ataques se relacionaban con iniciativas legislativas en todo el mundo en materia de derechos de autor o de regulación de Internet entre otros temas que les convirtieron en el grupo *hacktivista* representativo de la nueva ética *hacker* [94].

Anonymous comenzó a hacerse notar en febrero de 2010, a raíz de un ataque DDoS contra la web del Parlamento australiano, primero, y del Parlamento europeo después, en la denominada *operación Titstorm* justificada por el grupo por la propuesta del Gobierno de Australia de una Ley para el filtrado de Internet como forma de lucha contra la pornografía infantil. Según señalan Zuckerman, Roberts y York, el ataque no fue realizado utili-

---

[93] Véase ZUCKERMAN, E.; ROBERTS, H., y YORK, J. C., «Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites», en *The Berkman Center for Internet & Society at Harvard University,* núm. 16, 2010, p. 31.

[94] Al respecto, es ciertamente significativo el estudio de PRAS, A.; SPEROTTO, A.; MOURA, G. C.; DRAGO, I.; BARBOSA, R.; SADRE, R.; SCHMIDT, R., y HOFSTEDE, R., «Attacks by "Anonymous"», *op. cit.*, en el que analizan el tipo de DDoS llevado a cabo por el citado grupo Anonymous, mostrando que debido a la sencillez del programa usado y a la no utilización de IP *spoofing,* su identificación era realmente sencilla. Lo interesante de la investigación no es tanto la falta de anonimato del grupo como la facilidad con la que prácticamente cualquiera con unos conocimientos básicos de informática puede ejecutar ataques de DDoS.

zando una *botnet,* sino por medio de voluntarios que ejecutaron a la vez el ataque sobre los sitios, organizados a través de mensajes en foros de Internet del mundo *hacker*. Similar técnica fue utilizada el 18 de septiembre de 2010, en el ataque dirigido contra la página web de la Motion Picture Association of America. Desde los sitios web 4chan y Culture Site Reddit se promovió la descarga e instalación del *Low Orbit Ion Cannon*, un programa informático fácil de usar para la ejecución de un ataque DDoS que impidió el uso de la citada web durante más de 20 horas. Y también se utilizó tal técnica en los ataques reivindicados por Anonymous ejecutados contra compañías como Amazon, Paypal, Visa, Mastercard o Postbank, como represalia contra ellas por haber dejado de prestar servicio a Wikileaks [95, 96].

Anonymous plasma con perfección, a mi parecer, los caracteres esenciales, aunque no por ello unívocos, del ciberactivismo: se trata de un grupo abierto e indefinido de personas con conocimientos informáticos pero entre los que puede haber desde *hackers* a meros iniciados, generalmente jóvenes, a los que unen convicciones ideológicas antisistema, en general, y en particular contrarias a la restricción de Internet. El poder de este tipo de grupos estriba, por una parte, en la fácil sustituibilidad de sus miembros unida a la inmutabilidad de la idea o mensaje; por otra, en lo atractivo que resulta para un sector de la población como el juvenil que prácticamente ha entrado en la etapa adulta al mismo tiempo que ha explotado el ciberespacio como lugar de interconexión mundial, las ideas consistentes en fomentar que Internet se mantenga libre de intromisiones y censuras.

Además, es especialmente significativo el que no sean necesarios grandes conocimientos informáticos para participar en un ciberataque de este tipo [97]. Cualquier usuario sensibilizado con el mensaje político de libertad y neutralidad de Internet que acceda a foros de este tipo y siga sencillas instrucciones puede convertirse en coautor de un ataque DDoS. Quizás lo complejo en este caso, y lo que hace más apetecible para el criminal y más potencialmente peligroso la utilización de *bots*, es generar en todo el mundo una red de colaboradores voluntarios que, bajo una misma ideología, se conviertan en los que hagan posible el ciberataque. Estamos viendo, sin embargo, que el mensaje de la neutralidad de la Red está ganando cada vez más adeptos si

---

[95] ZUCKERMAN, E.; ROBERTS, H., y YORK, J. C., «Distributed Denial...», *op. cit.,* p. 31.

[96] La declaración del grupo Anonymous al *Guardián* en 2010 en relación con el tema Wikileaks plasma a la perfección su filosofía: «Estamos en contra de que las corporaciones y los gobiernos interfieran en Internet. Creemos que debe ser abierto y libre para todos. Los gobiernos no deberían tratar de censurar la información por el mero hecho de no estar de acuerdo con ella. Anonymous está apoyando a Wikileaks no porque esté de acuerdo o en desacuerdo con lo que está enviando, sino porque estamos en contra de cualquier censura en Internet. Si dejamos que Wikileaks caiga sin luchar entonces los gobiernos creerán que pueden cerrar los sitios con los que están en desacuerdo», traducción de la nota del *Guardián* citada por FITRI, N., «Democracy Discourses through the Internet...», *op. cit.,* p. 12.

[97] ZUCKERMAN, E.; ROBERTS, H., y YORK, J. C., «Distributed Denial...», *op. cit.,* p. 32.

bien es indudable que la penalización de estas conductas llevará una reducción de los colaboradores de estos grupos organizados.

Hemos visto cómo gran parte de la cibercriminalidad política o ideológica es llevada a cabo por grupos organizados, si bien es cierto que sustituyendo el funcionamiento jerárquico tradicionalmente asociado a estas estructuras por otro más horizontal y difuso en el que la organización define los objetivos genéricos y el resto depende del individuo. No es, sin embargo, la organizada la única forma de autoría de los cibercrímenes políticos, pues también es posible que sea un sujeto individual, único, y sin ningún tipo de relación organizativa con otros sujetos, el que lleve a cabo el cibercrimen. Esto ocurre tanto con el *cyberhate* o difusión de odio racial por Internet como con el *hacktivismo.* En el primer caso es perfectamente posible que una persona cree una página web en la que difunda mensajes de odio sin depender de ninguna estructura organizativa. Lo mismo ocurre en el *hacktivismo,* como demostró el *hacker* identificado como «Jester», que llevó a cabo diversos ataques durante 2009 y 2010 contra lo que él había definido como «webs yihadistas», utilizando un programa que denominó Xerxes y afectando a más de 29 webs de entre las que destacaba la página de Wikileaks.org [98]. Su ideología, coincidente o no con la de otros, le mueve a la realización individual de un comportamiento criminal.

2.3. El cibercriminal social

Si decíamos que no era fácil derivar unas características generales de los criminales que ejecutaban alguno de los delitos incluidos en la categoría de los cibercrímenes económicos o políticos, aún más complejo resultaría hacerlo para los autores de los cibercrímenes sociales. La razón es que es esta categoría la que incluye una más variada tipología de motivaciones criminales, que pueden ir desde quien actúa con un propósito sexual que bien puede ser un mayor de edad con ánimo de abusar de una menor u otro menor que envía fotos de un desnudo propio a otra persona, pasando por quien muestra su agresividad en el ciberespacio insultando y amenazando a otras personas en foros o en redes sociales, hasta quien acosa a otra persona enviándole numerosos mensajes de *e-mail* o utilizando las redes sociales y ello pese a la insistencia de la víctima en que la deje en paz. Y también los menores podrán ser, por tanto, autores de cibercrímenes sociales, especialmente de aquellos cometidos en el seno de redes sociales y otros lugares de intercomunicación social en el ciberespacio. Así, los menores serán protagonistas como sujetos activos de delitos tales como el *sexting*, las injurias y calumnias vertidas en foros o similares, así como del *cyberbullying* o acoso a menores en el que las redes sociales pueden convertirse en un instrumento más de acoso a la víctima.

[98] *Ibid.*

En realidad, pues, hay tantos potenciales perfiles de autores de cibercrímenes sociales como modalidades delictivas existentes, y las únicas características atribuibles a cada una de esas categorías de sujetos serán, en principio, similares a las que se puedan atribuir a los que cometen los mismos delitos en el espacio físico. Lo realmente interesante es, sin embargo, analizar cómo el ciberespacio, al modificar el ámbito de riesgo en el que se comete el delito, también cambia en muchos casos el perfil de quien lo comete. Sin la profundidad que requeriría y a modo de revisión parcial, voy a tratar de mostrar esta tendencia con los perfiles de los agresores de los tres ciberdelitos sociales más llamativos, el *cybergrooming*, el *cyberstalking* y el *cyberbullying*.

2.3.1. *El* cybergroomer

Comenzando por el denominado *groomer*, parece en este caso obvio que Internet no sólo ha cambiado la forma de hacer *grooming*, sino que, y esto es más importante, ha modificado el perfil del sujeto que lo hace, ha aumentado las posibilidades de que potenciales abusadores sexuales lleguen a serlo, y, con ello, ha incrementado significativamente el número de posibles víctimas.

En efecto, estudios psicológicos y criminológicos certifican que el ciberespacio aumenta las posibilidades de que potenciales abusadores sexuales lleguen a serlo. Así se concluye, por ejemplo, de un estudio de Young que señala, entre otros factores, la relación existente entre el aislamiento social y la existencia de una sexualidad compulsiva o adictiva [99]. Internet, en este sentido, es un vehículo utilizado por muchos sujetos para vencer el aislamiento social y comunicarse con otros. En segundo lugar Internet aumenta el número potencial de víctimas a las que puede acceder un agresor. Además, Internet permite que el agresor realice una investigación del perfil de víctima antes de decidir quién puede ser más vulnerable al ataque [100]. Por último, Internet difumina la percepción del potencial abusador del riesgo a ser descubierto. Como señala Young respecto a los ataques sexuales, mientras que los mismos «pueden parecer un viaje a un "territorio desconocido", las conductas sexuales *online* las ejecuta el agresor en el ambiente familiar y cómodo de casa o la oficina, lo que reduce la sensación de riesgo y permite incluso los comportamientos más aventureros» [101]. Se trata, eso sí, de un anonimato que sirve al sujeto para potenciar su sensación de seguridad y decidirse a atacar, pero no para utilizarlo falseando su identidad y haciéndose pasar por menor, como ahora se verá [102].

---

[99] YOUNG, K. S., «Profiling online sex offenders...», *op. cit.,* p. 9.

[100] Como señalan las investigaciones criminológicas, WOLAK, J.; FINKELHOR, D.; MITCHELL, K. J., e YBARRA, M. L., «Online "predators"...», *op. cit.*, p. 112.

[101] YOUNG, K. S., «Profiling online sex offenders...», *op. cit.,* p. 12.

[102] A esa conclusión se llega después de analizar la revisión de WOLAK, J.; FINKELHOR, D.; MITCHELL, K. J., e YBARRA, M. L., «Online "predators"...», *op. cit.*, p. 112, conforme a la cual tan

Esto, obviamente, incide en el cambio del perfil del *cybergroomer* frente al *groomer* que operaba en el espacio físico tradicional. Los estudios de *profiling* criminológico de los ciberdepredadores sexuales aseguran que el perfil del agresor en el ciberespacio es significativamente distinto, e incluso desde una perspectiva preventiva-especial, menos peligroso, que el del abusador sexual clásico o tradicional. Mientras que el depredador tradicional suele llevar a cabo sus ataques contra niños como forma de autogratificación, debido a una necesidad de ejercer poder, dominio, control o rabia, sin ser consciente en ningún momento del daño infligido, el ciberabusador que realiza *grooming* en los chats deriva sus fantasías sexuales de los desórdenes psicológicos motivados por la necesidad de escapar de la soledad, de la dificultad de las relaciones personales, de su baja autoestima, por lo que sí es consciente del significado de su conducta y del daño que puede infligir [103]. Siguiendo el modelo comparativo de los perfiles del ciberpredador frente al clásico de Young, se puede afirmar que mientras que este último es un depurado manipulador que oculta sus intenciones e incluso su identidad hasta que está en disposición de llevar a cabo el ataque, el sujeto que realiza *grooming* a través de Internet muchas veces no tiene una intención real de llevar a cabo sus fantasías, sino que las hace públicas generalmente de forma descarada, sin importarle que otros miembros del chat puedan sentirse ofendidos, reconociendo en la gran mayoría de los casos que se trata de varones de edad avanzada con deseos de realizar fantasías sexuales con menores, etc. [104]. Y este perfil de los sujetos que utilizan Internet para molestar a menores, también es confirmado por Wolak, Finkelhor, Mitchell e Ybarra, quienes afirman que los sujetos que se dedican a molestar a menores en Internet ocupan un margen estrecho dentro del espectro de los delincuentes sexuales, excluyendo claramente a los pedófilos y a los agresores violentos o sádicos [105]. Esto quedaría confirmado por la comparación psicológica entre los agresores sexuales clásicos y los agresores *online*, que tienen mayor empatía con las víctimas, menor índice de desviación sexual y menos distorsiones cognitivas que los primeros [106].

---

sólo el 5 por 100 de los que realizan *grooming* por Internet se hacen pasar por menores para atraer a sus potenciales víctimas.

[103] YOUNG, K. S., «Profiling online sex offenders...», *op. cit.*, p. 15.

[104] Véase el completo análisis que lleva a cabo YOUNG, K. S., «Profiling online sex offenders...», *op. cit.,* pp. 9 y ss., de la forma de actuar en las salas de chat de los ciberdepredadores, frente al comportamiento de los pedófilos que realizan el *grooming* fuera del ámbito virtual.

[105] WOLAK, J.; FINKELHOR, D.; MITCHELL, K. J., e YBARRA, M. L., «Online "predators"...», *op. cit.*, p. 117.

[106] BABCHISHIN, K. M.; HANSON, R. K, y HERMANN, C. A., «The characteristics of online sex offenders: a meta-analysis», en *SA*. En Internet, en *sax.sagepub.com/content/23/1/92.abstract* (última visita el 23 de diciembre de 2010, pp. 1 y ss., especialmente p. 10). Señala la autora, posteriormente, que esto implica que para un ciberagresor sea más difícil acabar cometiendo el ataque sexual, que para el agresor tradicional, dado que el primero tiene más mecanismos inhibitorios que este último. BABCHISHIN, K. M.; HANSON, R. K., y HERMANN, C. A., «The characteristics...», *op. cit.,*

Podría afirmarse, conforme a estos estudios, que el sujeto que utiliza Internet para molestar y hacer proposiciones a menores no es generalmente un pedófilo, dado que sus objetivos no son niños (menores preadolescentes), sino adolescentes, en general, y chicas que ya hayan tenido experiencias sexuales y que estén dispuestas a tenerlas, en particular [107]. El objetivo, pues, de los ciberabusadores sexuales, y ésta es una conclusión importante sobre la que se volverá después y que se relaciona con la cuestión de la edad desde la que se debe sancionar el delito, no es tanto el abusar de menores de trece años, como el mantener relaciones sexuales consentidas con menores de edad de trece a dieciocho años.

Y lo anteriormente comentado entronca con la cuestión del mayor riesgo que, como veíamos anteriormente [108], se atribuye al *cybergrooming* frente al *grooming* tradicional por parte de la sociedad y que podría haber tenido reflejo en España con la tipificación del *online grooming*. Lo cierto es que no parece posible afirmar que cualitativamente el riesgo de este tipo de *cibergrooming* sea mayor al tradicional, en el sentido de que es discutible, conforme a los estudios que hemos visto, que pueda decirse que hay más riesgo de un abuso sexual en el caso de un adulto que realiza proposiciones sexuales en un chat a una chica de quince años que se muestra aparentemente desinhibida en temáticas sexuales, que en el caso de un adulto que se acerca a un niño de once años para convertirse en su confidente con la intención de intentar estar sólo con él en algún momento y llegando a concretar una cita en su casa. Los estudios criminológicos indican que el agresor *online* tiene un mayor autocontrol y una menor impulsividad que el agresor que no utiliza Internet [109].

2.3.2. *El* cyberstalker

Frente a lo que acabamos de ver que sucede con el *grooming*, todo parece apuntar, pese a la casi inexistencia de estudios sobre el perfil de los *cyberstalkers*, que poco varían las características de este respecto a las del *stalker offline*. Del estudio de Bocij y McFarlen se desprende que los *cyber-*

---

p. 17. A idénticas conclusiones llegan ELLIOTT, I. A.; BEECH, A. R.; MANDEVILLE-NORDEN, R., y HAYES, E., «Psychological profiles of Internet sexual offenders: comparisons with contact sexual offenders», en *SA,* vol. 21, núm. 1, 2009. En Internet, en *http://sax.sagepub.com/content/21/1/76* (última visita el 23 de diciembre de 2010, pp. 76 y ss., especialmente en pp. 87 y ss.), a partir de un estudio comparativo entre predadores sexuales que consumaron el contacto con menores y agresores *online*, especialmente en lo relativo a las mayores distorsiones cognitivas y distorsiones de empatía con la víctima de los primeros.

LANNING, K. V., «Law enforcement...», *op. cit.,* pp. 4-9.

[107] *Ibid.*

[108] Cap. II.2.2.5.3.

[109] BABCHISHIN, K. M.; HANSON, R. K., y HERMANN, C. A., «The characteristics...», *op. cit.,* pp. 1 y ss., especialmente p. 16.

stalkers suelen ser hombres (84,6 por 100 de los hombres frente a 15,4 por 100 de mujeres) con una edad media de 41 años aunque el rango de edad puede variar de 18 a 67 años [110]. Respecto al estado civil de los agresores, la mayoría suelen ser solteros (52,3 por 100) aunque también se pueden dar en menor medida casos de agresores casados (21,7 por 100) o que estén separados o divorciados (17,3 por 100). Suelen tener conocimientos informáticos, habiendo obtenido los autores del estudio que el 41 por 100 poseía conocimientos medios y un 50 por 100 conocimientos altos o muy altos. Finalmente, respecto a la ocupación laboral, obtuvieron que un 50 por 100 de los *cyberstalkers* tenían trabajo frente a un 18,2 por 100 que se encontraban en paro y un 8,3 por 100 que era estudiante [111].

En el mismo estudio, Bocij y McFarle, elaboraron una clasificación de *cyberstalkers* distinguiendo cuatro tipos: el vengativo (*vindicative*), el integrado (*composed*), el íntimo (*intimate*) y el colectivo (*collective*). De acuerdo con la clasificación, el *cyberstalker* de tipo vengativo se correspondería con el tipo más violento que generalmente presenta antecedentes delictivos. Además, suele tener un nivel alto de manejo de las tecnologías y usa una amplia gama de métodos para acosar a sus víctimas como el envío de correos masivos, el envío de troyanos, el robo de identidad, etc. Los autores comentan que existe la posibilidad de que los *cyberstalkers* vengativos presenten algún tipo de enfermedad mental a raíz del análisis de los mensajes que enviaron a sus víctimas.

Siguiendo la tipología propuesta por Bocij y McFarlen, el *cyberstalker* de tipo integrado tiene como objetivo molestar e irritar a sus víctimas sin intención de mantener algún tipo de relación sentimental con ellas. Presentan un nivel alto de manejo de Internet y, a diferencia con el *cyberstalker* de tipo vengativo, no suelen tener antecedentes delictivos ni presentar historial psiquiátrico previo. La tercera categoría propuesta, los denominados *cyberstalkers* íntimos, tienen como objetivo establecer una relación íntima con sus víctimas y el medio que suelen emplear para contactar con ellas es el correo electrónico y las webs de citas. El nivel de manejo de Internet de este tipo de *cyberstalkers* varía desde el que apenas tiene conocimientos hasta el que tiene conocimientos altos. Y, finalmente, se refieren con *cyberstalkers* colectivos a cuando dos o más personas se unen para acosar a una misma víctima a través de medios tecnológicos. Este tipo de agresores se caracterizan por tener conocimientos amplios de informática y de emplear técnicas muy variadas para acosar a sus víctimas.

---

[110] Los porcentajes de *cyberstalkers* por rangos de edad son: el 23,1 por 100 tenía entre 18 y 30 años; el 34,6 por 100 tenía entre 31-40 años y un 42,3 por 100 era mayor de 41 años.

[111] McFarlane, L., y Bocij, P., «An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers», en *First Monday,* vol. 8, núm. 9, 2003. En Internet, en *http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1076/996*.

2.3.3. *El* cyberbully

Más datos fiables encontramos respecto al perfil del *cyberbully* o los *cyberbullies*, incluyendo las dos modalidades que, según Mason, existen: los proactivos, que cometen su acción para conseguir un fin, y los reactivos, que agreden como respuesta a una provocación, agresión o amenaza [112]. Respecto al número, de nuevo el porcentaje de agresores varía entre estudios, desde el 0,4 por 100 de los encuestados hasta el 52 por 100 [113], aunque la mayoría sitúan la prevalencia entre el 4 y el 18 por 100 de los alumnos estudiados. Así, por ejemplo, Kowalski y Limber realizaron un estudio con 3.767 sujetos de los cuales un 4 por 100 se declaraba agresor y un 7 por 100 agresor victimizado [114]. Por su parte, Hinduja y Patchin obtuvieron porcentajes más elevados. El 18 por 100 de los chicos declaró realizar alguna de las conductas, mientras que en el caso de las chicas declararon ser agresoras un 16 por 100 [115]. Vandebosch y Van Cleemput realizaron un estudio con 2.052 estudiantes belgas de entre 10 y 18 años, en el que obtuvieron que un 18 por 100 eran agresores [116]. En Suecia, Slonje y Smith encontraron que un 10,3 por 100 de los encuestados eran agresores [117]. En Inglaterra Smith, Mahdavi, Carvalho, Fisher, Russel y Tippet, situaron el porcentaje de agresores en un 11 por 100 [118]. Finalmente, en España, el Defensor del Pueblo situó la cifra de ciberagresores en un 5,4 por 100 [119]. Las discrepancias encontradas se pueden deber a las diferencias culturales de los encuestados o, en mayor medida, a la metodología empleada, sobre todo teniendo en cuenta que cada uno mide un rango de edad y no coinciden las conductas medidas ni la temporalidad.

Respecto al sexo de los ciberagresores la mayoría de los estudios indican que son los chicos quienes más involucrados están en este tipo de conduc-

---

[112] Mason, K. L., «Cyberbullying: A Preliminary Assessment for School Personnel», en *Psychology in the Schools*, 45 (4), 2008, pp. 323 y ss.

[113] Mora-Merchán, J. A., y Jäger, T. (eds.), *Cyberbullying. A Cross-national comparison*, Landau, Verlag Empirische Pädagogik, 2010.

[114] Kowalski, R. M., y Limber, S. P., «Bullying Among Middle School Students», en *Journal of Adolescent Health,* 41 (6), 2007, pp. 22-30, especialmente p. 25.

[115] Hinduja, S., y Patchin, J., «Personal Information of Adolescents on the Internet: A Quantitative Content Analysis of MySpace», en *JA,* 31(1), 2008, p. 141.

[116] Vandebosch y Van Cleemput: «Cyberbullying among youngsters: profiles of bullies and victim», en *New Media and Society,* 11 (8), 2009, pp. 1349-1371.

[117] Slonje, R., y Smith, P. K., «Cyberbullying: another main type of bullying?», en *Scandinavian Journal of Psychology,* 49 (2), 2008, pp. 147-154.

[118] Smith, P. K.; Mahdavi, J.; Carvalho, M.; Fisher, S.; Russell, S., y Tippett, N., «Cyberbullying: Its nature and impact in secondary school pupils», en *Journal of Child Psychology and Psychiatry and Allied Disciplines*, 49 (4), 2008, pp. 376-385.

[119] Defensor del Pueblo-UNICEF, *Violencia escolar: el maltrato entre iguales en la educación secundaria obligatoria. 1999-2006,* Madrid, Publicaciones de la Oficina del Defensor del Pueblo, 2007.

tas [120]. Aunque otros como Patchin e Hinduja no han encontrado diferencias significativas entre chicos (18 por 100) y chicas (16 por 100) [121]. O incluso resultados opuestos como Ybarra y Mitchell, quienes obtuvieron que eran más agresoras las chicas [122]. Esto último es especialmente significativo si se compara con el género del agresor en el *bullying* tradicional, en el que son los chicos quienes más agreden [123]. Sin embargo, es cierto, como explica Olweus que las chicas destacan por ser las que realizan, en el espacio físico, las formas de acoso más sutiles e indirectas como insultar, extender rumores falsos y hablar mal, mientras que los chicos emplean más la fuerza física y las amenazas [124]. Teniendo en cuenta que el *cyberbullying* se caracteriza por ser un tipo de agresión indirecto, más emocional y psicológico, donde no es necesario tener especiales cualidades físicas, como plantean Hinduja y Patchin, lo lógico es que las chicas fueran las que más hicieran uso de estas técnicas para dañar a sus compañeros o incluso como un medio de venganza tras haber sido víctima de algún tipo de victimización [125].

En cuanto a la edad, tampoco existe un consenso en si puede ser un factor determinante en la victimización [126]. No obstante, los cursos en los que más casos de *cyberbullying* se registran son en segundo y tercero [127] de secundaria como ocurre con el *bullying* tradicional [128].

---

[120] Ortega, R.; Calmaestra, J., y Mora-Merchán, J., «Cyberbullying», en *International Journal of Psychology and Psychological Therapy,* vol. 8, núm. 2, 2008. En Internet, en *http://redalyc.uaemex.mx/redalyc/pdf/560/56080204.pdf*, p. 190; Calvete, E.; Orue, I.; Estévez, A.; Villardón, L., y Padilla, P., «Cyberbullying in adolescents: Modalities and aggressors' profile», en *Computers in Human Behavior,* 26 (5), 2010, pp. 1128-1135; Avilés Martínez, J. M., «Éxito escolar y ciberbullying», *Boletín de Psicología,* núm. 98, 2010, pp. 73-85. Calmaestra, J., Cyberbullying: *prevalencia y características de un nuevo tipo de* bullying *indirecto. Tesis doctoral*, p. 170.

[121] Hinduja, S., y Patchin J., «Personal Information of Adolescents», *op. cit.,* p. 141. Otros autores también han obtenido resultados similares, como Ortega, R.; Calmaestra, J., y Mora-Merchán, J., *Las TIC y la convivencia: un estudio sobre formas de acoso en el ciberespacio. Investigación en la Escuela,* 64, 2008, pp. 93-104; Kowalski, R. M., y Limber, S. P., «Bullying Among Middle School Students», *op. cit.,* pp. 22-30, p. 25; Vandebosch, J., y Van Cleemput, K., «Cyberbullying amon youngsters:...», *op. cit.,* pp. 1349-1371.

[122] Ybarra, M. L., y Mitchell, K., «Youth engaging in online harassment: associations with caregiver-child relationships, Internet use, and personal characteristics», en *Journal of Adolescence*, 27 (3), 2004, pp. 319-336.

[123] Defensor del Pueblo-UNICEF, *Violencia escolar..., op. cit.,* p. 178.

[124] Olweus, D., «*Bullying* en la escuela: datos e intervención», en Sanmartín, J. (ed.), *Violencia y Escuela,* Valencia, Centro Reina Sofía para el Estudio de la Violencia, 2005, pp. 13-30.

[125] Hinduja, S., y Patchin, J., *Cyberbullying: An Exploratory Analysis of Factors Related to Offending and Victimization,* Deviant Behavior, 2008, pp. 129-156.

[126] Calmaestra, J., Cyberbullying: *prevalencia y características..., op. cit.,* p. 131.

[127] Calvete, E.; Orue, I.; Estévez, A.; Villardón, L., y Padilla, P., «Cyberbullying in adolescents:...», *op. cit.*, pp. 1128-1135; Ybarra, M. L., y Mitchell, K., «Youth engaging in online harassment...», *op. cit.,* pp. 319-336.

[128] Defensor del Pueblo-UNICEF (2007), *Violencia escolar: el maltrato entre iguales en la educación secundaria obligatoria. 1999-2006,* Madrid, Publicaciones de la Oficina del Defensor del Pueblo, p. 178.

Otras características que también se han replicado en el *cyberbullying* es el referido a la autoestima de los agresores. Así, Calmaestre apunta que tienen una autoestima más elevada que las víctimas [129] como ya apuntaba Olweus en el caso del *bullying* tradicional donde además de no presentar problemas de autoestima, siente una fuerte necesidad de dominar y someter a otros estudiantes, son impulsivos e iracundos, carecen de empatía, suelen ser desafiantes y agresivos con los adultos incluidos los padres y los profesores y suelen presentar otro tipo de conductas antisociales, como el vandalismo [130]. Finalmente merece la pena destacar que, como han comentado Walware y Wannes, existen determinados factores que pueden potenciar cometer *cyberbullying*. Entre ellos se encuentran tener una percepción favorable sobre este tipo de conductas, ser usuarios frecuentes de Internet, tener acceso a un ordenador privado y hacer uso de él en dependencias poco vigiladas y tener conocimientos específicos sobre las TIC [131].

[129] Calmaestra, J., Cyberbullying*: prevalencia y características..., op. cit.,* p. 191.

[130] Olweus, D., «*Bullying* en la escuela...», *op. cit.,* p. 18.

[131] Walrave, M., y Wannes, H., «Cyberbullying: Predicting Victimisation and Perpetration», en *Children & Society*, 25 (1), 2009, pp. 59-72.

CAPÍTULO V

LA CIBERVÍCTIMA: PERFILES DE VICTIMIZACIÓN Y RIESGO REAL DE LA AMENAZA DEL CIBERCRIMEN

1. INTRODUCCIÓN: MULTIPLICIDAD DE CIBERCRÍMENES = MULTIPLICIDAD DE CIBERVÍCTIMAS

Se debe recordar, de nuevo, que al hablar de cibercriminalidad, lo hago en sentido amplio como concepto englobador de cualquier delito cometido mediante el uso (esencial) de las TIC. Esto nos debe servir para comprender la variedad de delitos de naturaleza distinta que conforman tal categoría y, por tanto, y a los efectos que ahora nos interesan, la variedad de objetivos sobre los que pueden actuar las, por su parte, diferentes tipologías de cibercriminales y, por ende, la multiplicidad de víctimas de la cibercriminalidad que existen. Cualquier usuario de Internet, cualquier persona que tenga un sistema informático conectado a una red o que a través de los sistemas existentes en colegios, bibliotecas, universidades, instituciones públicas, cibercafés, hoteles y demás, puede ser víctima de cibercrímenes de muy distinto tipo, dependiendo de la motivación del sujeto que realiza el ataque pero, también, del tipo de actividad que el propio usuario realice. De nuevo, por tanto, escapa a lo posible la configuración de un perfil único de víctima potencial del cibercrimen, puesto que por lo menos habrá tantos perfiles como ámbitos de oportunidad criminal en el ciberespacio, pero entendiendo el ámbito de oportunidad como también definido por el actuar de la víctima. Esto significa, como ya se vio, que no es únicamente la motivación criminal la que define el ámbito de oportunidad criminal en el ciberespacio, sino que la propia víctima con su conducta también construye los ámbitos de riesgo. Así, y por anticipar ejemplos sobre los que se profundizará más adelante, la utilización de la banca electrónica permite configurar (junto con la motivación de la ciberbanda organizada o del *hacker* individual de que se trate) un ámbito de oportunidad que no existiría si el sujeto no utiliza la banca electrónica, y lo mismo puede ocurrir con los datos personales o con su intimidad.

Puede decirse, por tanto, que hay ámbitos de victimización específicos definidos por el actuar de la víctima en el ciberespacio, que conformarán un ámbito de oportunidad criminal al interaccionar con el ciberagresor motivado. Antes de analizar dos de los más importantes de ellos y de tratar de definir los condicionantes derivados del actuar de la víctima que pueden incidir en el mismo, creo conveniente reflexionar sobre la amplia variedad de sujetos que se pueden ver afectadas por la cibercriminalidad.

Lo primero que puede afirmarse al respecto es que prácticamente todos los agentes sociales son susceptibles de ser víctimas de un ciberataque, dado que todos, en la actualidad, interactúan en lo económico, social y personal en el ciberespacio. Desde empresas privadas, realicen o no sus principales actividades económicas en la Red, hasta usuarios individuales de todo tipo de condición, pasando por instituciones y organismos públicos, son potenciales víctimas del cibercrimen. Las empresas, del tamaño que sea y se dediquen o no al negocio tecnológico, pueden sufrir en la actualidad ataques desde el ciberespacio de muy diverso tipo, aunque siempre predominando las distintas modalidades de fraude informático. También el espionaje informático tiene como principal objetivo las empresas y, de ellas, las tecnológicas dedicadas a los servicios por Internet, pueden sufrir ataques de denegación de servicios que pueden producirles grandes perjuicios patrimoniales. Éstos también pueden derivarse de los ataques con *malware* procedentes del exterior, o de los daños informáticos cometidos por un empleado o ex empleado de la empresa con algún tipo de resentimiento hacia ella.

Junto a las empresas, destacan como potenciales víctimas de ciberataques de todo tipo las instituciones públicas. Las mismas, al disponer de un gran número de funcionarios que usan el correo electrónico y al funcionar generalmente por medio de redes internas, tienen especial riesgo de sufrir importantes daños mediante ataques de envío de *malware* o de denegación de servicio. Las instituciones públicas pueden ser víctimas y, de ese modo, verse afectada directamente toda la sociedad debido, por ejemplo, a la inutilización de servicios públicos *online* o similares que, en el mundo en que vivimos, cada vez van a generalizarse más.

En todo caso, las víctimas potenciales más vulnerables frente al cibercrimen son los usuarios privados, y tanto desde una perspectiva cuantitativa dada la generalización del uso de ordenadores privados por parte de miles de millones de usuarios en todo el mundo, como desde una perspectiva cualitativa pues mientras que instituciones públicas y empresas privadas disponen de medios de protección que pueden complicar el éxito del ciberataque, gran parte de usuarios particulares siguen utilizando Internet sin seguir las reglas básicas de seguridad informática. El escaso nivel de seguridad de los ordenadores personales les convierte, además, en potenciales víctimas de ataques de *botnets* que les vuelve, a su vez, ignorantes partícipes de ataques de todo tipo a otros usuarios, empresas o instituciones públicas. Los prin-

cipales ataques a usuarios se producen por ser ellos, directamente, un objetivo deseable para los cibercriminales: su intimidad, su libertad sexual, su dignidad pero, sobre todo, su patrimonio, puede ser objeto de ataque en el ciberespacio. Y pueden ser víctimas del cibercrimen tanto usuarios mayores de edad como menores, adolescentes y jóvenes totalmente integrados en la web 2.0 que si bien a edades tempranas apenas realizan actividades económicas en Internet sí desarrollan allí múltiples relaciones sociales que también les puede convertir en las víctimas de la cibercriminalidad.

Además, las víctimas de la cibercriminalidad lo pueden ser también de cualquier condición social si bien, como se ha avanzado y como se desarrollará a continuación con profundidad, será su propia actividad en el ciberespacio la que defina en términos generales el ámbito de riesgo al que estarán sometidas, de forma que un menor uso de Internet o su no utilización, por ejemplo, para actividades económicas derivada de su capacidad económica, de su edad o de su educación social y cultural, reducirá mucho sus posibilidades de ser víctima de un cibercrimen. En otras palabras, y como han señalado Pratt, Holfreter y Reisig, lo relevante no son tanto los datos demográficos como el actuar cotidiano de la víctima para la configuración del ámbito de riesgo [1]. A profundizar en estas cuestiones nos vamos a dedicar a continuación.

2. LA VICTIMIZACIÓN EN EL CIBERESPACIO: CONSIDERACIONES GENERALES DE NUEVO DESDE EL PRISMA DE LAS ACTIVIDADES COTIDIANAS

La víctima y su comportamiento son siempre elementos determinantes del evento criminal acontecido. Sin embargo, y como se vio en un capítulo anterior, en el ciberespacio la víctima juega incluso un papel condicionante aún mayor, en el sentido de definitorio del ámbito de oportunidad criminal, dado que ella misma determina desde un primer momento, al incorporar determinados bienes y esferas de su personalidad al ciberespacio, los márgenes genéricos del ámbito de riesgo al que va a estar sometida y dado que, además, al no existir en éste ámbito criminológico distancias físicas ni guardianes formales institucionalizados, el uso cotidiano que haga de las TIC y en especial la incorporación (o no) de sistemas digitales de autoprotección, serán determinantes a la hora de convertirse en víctima del cibercrimen. Si tenemos en cuenta, además, que en Internet, también al no existir distancias, el desplazamiento del cibercriminal hacia otros objetivos resulta no sólo sencillo sino incluso en muchos casos (virus y demás) instantáneo, y que la dirección del nuevo objeto del ataque la marcará la ausencia de siste-

[1] Pratt, T. C.; Holfreter, K., y Reisig, M. D., *Routine Online Activity and Internet Fraud Targeting..., op. cit.*, p. 283.

mas de protección o las vulnerabilidades del objetivo (entonces adecuado), parece evidente concluir el protagonismo de la víctima en su proceso de victimización.

Son varios los autores que han planteado la especial importancia del comportamiento de la víctima en la victimización por la cibercriminalidad informática. Lo hizo indirectamente Yar, quien partiendo de la teoría de las actividades cotidianas, y de la valoración en el ciberespacio de las cuatro propiedades conformantes que debe tener un objetivo para ser adecuado (VIVA: *Value, Inertia, Visibility and Accessibility*) [2], ya otorgaba especial importancia en relación con el riesgo delictivo al comportamiento de la víctima en cuanto a restringir la accesibilidad a su sistema por medio de programas informáticos que compliquen el acceso del agresor al objetivo.

Esa línea de buscar la relación entre la teoría de las actividades cotidianas y el riesgo delictivo, pero ya totalmente centrado en la victimización, es la que sigue Alshalan [3]. Su estudio analiza la victimización por virus informáticos, por una parte, y por otra por cibercrímenes tales como el ciberfraude en sus múltiples formas, *identitytheft* y *phishing*, fraudes de seguridad, *cyberstalking* y *cyberharassment*, extorsión y *hacking* [4].

La hipótesis de partida, desde las bases de la teoría de las actividades cotidianas, es que el comportamiento de la víctima en el ciberespacio es un importante predictor de su victimización, y la misma es demostrada en este estudio empírico de regresiones logísticas, en el modelo de victimización concretamente, que a mayor frecuencia de acceso a Internet mayor riesgo de victimización; también a mayor tiempo en el ciberespacio; así como la realización de actividades en Internet que conllevan la divulgación de datos personales de tipo financiero [5] y, exclusivamente para la infección por virus, el tener hijos que acceden al ciberespacio.

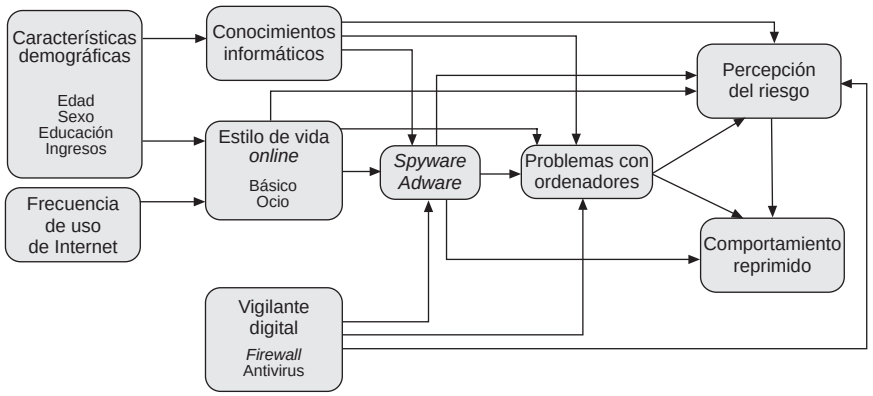
Otros dos interesantes estudios relacionan la victimización en el ciberespacio con los tópicos de la teoría de las actividades cotidianas y, también, la de los estilos de vida. El último de estos estudios lo acomete Yucedal, quien examina los factores que inciden en la victimización por conductas de *spyware* y *adware* a partir de los presupuestos de las citadas teorías.

El autor concluye, en aplicación de la primera, que el comportamiento cotidiano en relación con el uso de Internet es un elemento determinante de la victimización por estos delitos que exigen, generalmente, que sea el propio sujeto el que al visitar una determinada web o al descargarse un programa, cargue involuntariamente el virus; y, derivado de la segunda, que el uso de instrumentos digitales de seguridad tales como cortafuegos, antivi-

---

[2] YAR, M., «The novelty of "cybercrime"...», *op. cit.,* p. 421.
[3] ALSHALAN, A., *Cyber-Crime Fear and Victimization..., op. cit.,* p. 123.
[4] *Ibid.,* pp. 47 y ss.
[5] *Ibid.,* p. 126.

Gráfico 5.1. Modelo estructural para examinar la victimización por *spyware* y *adware.* Elaboración propia.



rus o programas *antispyware* como guardianes capaces puede determinar su riesgo de victimización [6].

Este estudio de Yucedal, en realidad, apenas difiere, excepto en el objeto, del que, a mi parecer, es el más interesante estudio sobre la victimización en el ciberespacio, el de Choi, que realiza una interesante identificación entre los comportamientos cotidianos en Internet y la teoría de los estilos de vida y la utilización de sistemas de protección con el tópico, para él central, de la ausencia de guardián capaz en la teoría de las actividades cotidianas [7]. También por medio de un estudio empírico de ecuaciones estructurales para la evaluación de la relevancia de variables como el estilo de vida en Internet y la utilización de sistemas informáticos de protección, Choi llega a la conclusión después confirmada por Yucedal relativa a que el *hacking* es más factible en personas con ordenadores personales que no tienen instalados programas de seguridad informática, que utilizan mucho Internet y que realizan conductas de riesgo en línea [8].

Pese que hay otros autores, como Marcum, Bossler y Holt, que han obtenido resultados contradictorios con respecto a la tenencia de sistemas de seguridad informática, donde no tenerlos no reduce la victimización [9], incluso llegando al extremo contrario, donde tener un antivirus correlaciona positi-

---

[6] YUCEDAL, B., «Victimization in cyberspace»..., *op. cit.,* pp. 117 y ss. En el caso de la incorporación de sistemas de autoprotección el estudio utiliza como variables la tendencia de cortafuegos y de antivirus.

[7] CHOI, K., «Computer Crime Victimization and Integrated Theory...», *op. cit.,* pp. 309 y ss.

[8] *Ibid.,* p. 321. Frente a la forma de medición de Yucedal, la variable del estilo de vida *online* es medida por medio de tres variables distintas, actividades vocacionales y de ocio, actividades de ocio peligrosas, y actividades vocacionales de riesgo.

[9] BOSSLER, A. M., y HOLT T. J., «Online Activities, Guardianship, and Malware Infection», en *IJCC,* vol. 3, núm. 1, enero-junio de 2009, pp. 400 y ss.

vamente con la victimización de *malware* [10], todo apunta a que efectivamente, tener *software* de protección reduce el cibercrimen siempre y cuando se use correctamente. Los resultados contradictorios probablemente se deban a la metodología empleada, pues seguramente ambas variables miden los mismo, sólo los que tienen sistemas antivirus pueden advertir la presencia de uno en sus sistemas y, sobre todo, teniendo en cuenta además tal y como advierte el Instituto Nacional de Tecnologías de la Comunicación (INTECO, 2011) que en la mayoría de los casos un ordenador infectado no muestra síntomas fácilmente reconocibles por el usuario, y que sólo es alertado de esta victimización cuando los propios programas de seguridad se lo advierten. Pero al final, el tener *software* de protección depende de la potencial víctima. Será ella quien tenga que proveerse de los distintos programas además de mantenerlos actualizados.

Ha habido otros intentos de identificar otros elementos que minimizan el riesgo de victimización, como por ejemplo el lugar en que se hace uso de Internet. Marcum obtuvo que usar Internet en un lugar no vigilado o acompañado de otras personas, aumenta la probabilidad de recibir solicitaciones de sexo no deseadas. Sin embargo, lo interesante es comprobar el tipo de actividades que realizan estando acompañados y a solas que determinarán la probabilidad de riesgo.

Estos estudios, y otros que analizaremos después y que se aplican ya en ámbitos concretos de victimización, vienen a confirmar algo que ya habíamos afirmado: que la víctima define el ámbito de riesgo al que puede acceder el agresor motivado. Aunque Choi ponga el acento del riesgo de victimización en el ciberespacio en el guardián capaz, es la víctima con su conducta la que también acaba por definir ese elemento y, por tanto, el riesgo de victimización al que se somete: es la víctima la que decide actualizar o no las claves informáticas, contratar o no un sistema antivirus, actualizar el *software* de su ordenador, etc. Además también la víctima decide si descarga archivos aun ignorando su seguridad, así como las horas que pasa en Internet, elemento que todos los estudios consideran determinante: a mayor número de horas en Internet mayor riesgo de victimización.

Así, los estudios demuestran que interactuar con extraños a través de las redes sociales y en las salas de chat o abrir mensajes de desconocidos aumenta el riesgo de victimización [11], pero también descargar *software*, juegos o media pirata [12], realizar determinadas actividades de ocio como

---

[10] NGO, F., y PATERNOSTER, R., «Cybercrime Victimization: An examination of Individual and Situational level factors», en *IJCC*, vol. 5, núm. 1, 2011, pp. 773 y ss.

[11] Admitir extraños en las cuentas de red social está positivamente asociado a: contacto no deseado, al *harassment,* solicitación de sexo, *cyberstalking* e *identity fraud* en «Being Pursued Online...», *op. cit.,* p. 104. Resultados similares han obtenido NGO, F., y PATERNOSTER, R., «Cybercrime Victimization: An examination of...», *op. cit.,* pp. 773 y ss.

[12] YUCEDAL, B., «Victimization in...», *op. cit.,* pp. 1 y ss.; REYNS, B., «Being Pursued Online...», *op. cit.,* pp. 1149 y ss.; CHOI, K., «Computer Crime Victimization and...», *op. cit.,* pp. 308 y ss.

comprar [13], pasar más horas conectados [14], visitar páginas web para adultos [15], realizar comportamientos desviados como acceder de forma ilícita a sistemas informáticos, modificar archivos de otros, realizar *cyberstalking*, piratear media [16] y proporcionar información personal supone un riesgo [17] como por ejemplo, el nombre completo, el estado civil, la orientación sexual, colgar fotos personales y vídeos en las redes sociales [18] o divulgar el número de tarjeta de crédito a través de mensajes [19].

Todo, en definitiva, confirma la hipótesis de que el ciberespacio, al contraer las distancias y el tiempo, convierte a la víctima en determinante esencial de su victimización por medio de las conductas peligrosas que ella realice, los lugares a los que acceda, el tiempo que pase, los bienes que «suba» al ciberespacio, así como los guardianes que elija para su protección, etcétera.

Junto a estos condicionantes hay factores demográfico que también han resultado relevantes en la dinámica de victimización. Los estudios en Estados Unidos confirman que las personas de raza blanca tienen más riesgo de ser victimizadas. Marcum, de forma más concreta, señaló que ésta es la única variable demográfica que presenta como factor determinante en la probabilidad de victimización siendo los blancos quienes más reciben material sexual no deseado [20].

También ocurre con otras variables demográficas que parece ser claves en la explicación de la cibervictimización. Alshalan ya determinó que los hombres tienen más riesgo frente a la mujeres, lo cual a su vez se corresponde con la frecuencia de uso de Internet y la duración del tiempo pasado en el ciberespacio que son mayores en los varones como se muestra en la tabla basada en el estudio de Alshalan [21].

Trabajos posteriores han tenido resultados diferentes frente a la variable género, donde los investigadores han tratado de solventar estas discrepan-

---

[13] ALSHALAN, A., «Cyber-Crime Fear and Victimization...», *op. cit.;* YUCEDAL, B., «Victimization in cyberspace...», *op. cit.,* pp. 1 y ss.

[14] YUCEDAL, B., «Victimization in cyberspace...», *op. cit.,* pp. 1 y ss.

[15] CHOI, K., «Computer Crime Victimization and Integrated Theory...», *op. cit.*, pp. 308 y ss.

[16] BOSSLER A. M., y HOLT, T. J., «*Online Activities, Guardianship, and...», op. cit.,* pp. 400 y ss.

[17] MARCUM, C. D., «Adolescent online victimization and...», *op. cit.*; ALSHALAN, A., «Cyber-Crime Fear and Victimization...», *op. cit.,* pp. 1 y ss.

[18] REYNS, B., «Being Pursued Online...», pp. 1149 y ss., detectó que proporcionar el nombre completo, estado civil, orientación sexual, la dirección de correo, intereses, aficiones, fotos y vídeos a través de las redes sociales y en Internet en general se relaciona con la probabilidad de sufrir contacto no deseado, *harassment, sex advance* y *cyberstalking*.

[19] ALSHALAN, A., «Cyber-Crime Fear and Victimization...», *op. cit.,* pp. 1 y ss.

[20] MARCUM, C. D., «Adolescent online victimization and Constructs of Routine Activities theory...», *op. cit.,* pp. 253 y ss. RICKETTS, M. L., y HIGGINS, G. E., «Assessing sex experiences of online victimization: an examination of adolescent», en *Criminal Justice Review,* 2010, pp. 1-26.

[21] ALSHALAN, A., «Cyber-Crime Fear and Victimization...», *op. cit.,* p. 83.

Tabla 5.1. Comparaciones de medidas de variables seleccionadas por género. Elaborada por Alshalan en 2006.

Variables	*Hombre*		*Mujer*		*Diferencia medias*
	Media	*SD*	*Media*	*SD*	
Frecuencia[a]	4,7	1,18	4,43	1,29	0,278***
Duración[b]	2,028	1,16	1,98	1,09	0,046

[a] 1. Pocas veces por año. 2. Una o dos veces al mes. 3. Una o dos veces por semana. 4. Varios días por semana. 5. Una vez al día.
[b] 0. Nunca. 1. 30 minutos o menos. 2. 1 hora. 3. 1-2 horas. 4. 2-3 horas. 5. 3 o más horas.
*** Significativo para $p < 0,001$
** Significativo para $p < 0,01$

cias atribuyéndolo a los tipos de victimización. Y es que todo apunta a que el género y la edad pueden estar ligados al tipo de cibercrimen. Así, Bossler y Holt detectaron que los hombres tienen más probabilidad de sufrir cambios de información en sus ordenadores sin su permiso mientras que las mujeres tienen mayor probabilidad de sufrir *harassment*[22]. La causa no es el comportamiento de las mujeres en Internet, sino que los ciberacosadores las perciben como un objetivo atractivo (*atracctive target)*[23]. En este sentido, Reyns obtuvo que las mujeres sufren más conductas de acoso (*unwanted contact, harassment, sexual advances and cyberstalking*), los hombres sufren más amenazas de sufrir violencia física (aunque no son estadísticamente significativas) y no encontró diferencias en *identity fraud*[24]. Ngo y Paternoster concluyeron en su estudio que el sexo no tiene efecto en la probabilidad de cibervictimización en ninguno de los tipos de cibercrimen medidos (infección de *malware,* el *harassment* por conocidos y desconocidos, la exposición a material pornográfico no deseado, la solicitación de sexo, *phishing* y la difamación *online*)[25].

Estas discrepancias entre estudios pueden deberse a que las variables sociodemográficas influyen el tipo de actividades cotidianas realizadas en el espacio: las que realizan los hombres (especialmente en cuanto a descarga de archivos o actividad de comercio electrónico) frente a las que realizan las mujeres para entender el menor riesgo de victimización del hombre[26]. Como

---

[22] Bossler, A. M., y Holt, T. J., «The effect of self-control on victimization in the cyberworld», en *Journal of Criminal Justice,* 2010, pp. 227-236.

[23] Bosssler, A. M., y Holt, T. J., *Examining the applicability of life style-routine activities theory for cybercrime victimization,* 2009, pp. 16 y 20.

[24] Reyns, B., «Being Pursued Online...», *op. cit.,* p. 9. Debemos destacar, que en el caso de las amenazas físicas, fueron los hombres quienes las recibieron en mayor porcentaje, 5,4 por 100 frente a un 3,7 por 100 de las mujeres, pero esta diferencia no resultó estadísticamente significativa (Chi = 1,56; $p = 0,41$).

[25] Ngo, F., y Paternoster, R., «Cybercrime Victimization...», *op. cit.,* p. 785.

[26] También puede ser relevante el factor miedo al delito que es mayor en mujeres que en hombres, conforme al propio estudio de Alshalan, A., «Cyber-Crime Fear and Victimization...»,

explica Yucedal, los hombres con mayor nivel de educación participan en más actividades básicas (uso de correo electrónico, compras, crear o leer webs y blogs) y de ocio (como jugar *online*, compartir archivos, descargar películas, música, programas y visitar páginas de adultos) [27].

También está generalmente admitido, y sobre ello volveremos más adelante, que el tiempo de uso en Internet es significativamente mayor en los usuarios jóvenes que en los más mayores. Concretamente en el estudio de Pratt, Holfreter y Reisig, se señala que por cada unidad en la que se incrementa la edad disminuye en tres unidades porcentuales el tiempo pasado en el ciberespacio durante la semana [28]. Puede decirse, por tanto, que hay un mayor riesgo de victimización en el ciberespacio para los más jóvenes, pero derivado del estilo de vida de los mismos, concretamente de las horas que suelen pasar en Internet.

Y es que el análisis comparado de los estudios que hemos citado nos lleva a la conclusión, como también a los autores que los han desarrollado, que los factores demográficos son menos relevantes que las actividades cotidianas en Internet llevadas a cabo por las víctimas. Así lo demuestran los estudios empíricos conforme a los cuales cuando se incluyen las variables derivadas de la teoría de las actividades cotidianas, los efectos de la edad, la educación y otros sobre la victimización por cibercrímenes son eliminadas [29]. Y la conclusión es importante: si finalmente el tiempo pasado en el ciberespacio es un factor de riesgo de victimización (pese a no saber de forma empírica si más tiempo pasado supone una mayor exposición en la medida que correlaciona positivamente con el mayor número de actividades realizadas en el ciberespacio) y, como parece inevitable, en los próximos años irá aumentando la media de tiempo que las personas dedican a Internet, será necesario también incrementar la formación en seguridad para la implantación de actividades cotidianas seguras en el ciberespacio que busquen tanto evitar los lugares inseguros como lograr incorporar guardianes capaces para la protección de bienes tan importantes como la intimidad o el patrimonio.

---

op. cit., pp. 145 y ss., aunque son menos susceptibles de ser victimizadas. Sería interesante analizar en qué medida el miedo al delito condiciona las concretas actividades realizadas por las mujeres, frente a los hombres, en el ciberespacio.

[27] YUCEDAL, B., «Victimization in...», *op. cit.,* p. 140.

[28] PRATT, T. C.; HOLFRETER, K., y REISIG, M. D., «Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory», en *Journal of Research in Crime and Delinquency,* vol. 47, núm. 3, 2010, pp. 267-296.

[29] ALSHALAN, A., «Cyber-Crime Fear and Victimization...», *op. cit.*, p. 146. En el mismo sentido, PRATT, T. C.; HOLFRETER, K., y REISIG, M. D.: «Routine Online Activity...», *op. cit.,* p. 267.

3. ANÁLISIS DE ALGUNOS ÁMBITOS ESPECÍFICOS DE VICTIMIZACIÓN

3.1. Comercio y banca electrónica y victimización frente al cibercrimen

Los estudios de victimización que hemos analizado y que confirmaban las hipótesis derivadas de la aplicación abstracta de la teoría de las actividades cotidianas al ciberespacio, se centraban especialmente en los cibercrímenes consistentes en el envío de virus, el *hacking* o la utilización de *spyware*. Todos ellos son cibercrímenes que generalmente entrarán en la categoría que hemos definido como cibercriminalidad económica: afecten o no al patrimonio de la víctima, la intención con la que se realizan es la obtención de un beneficio patrimonial, y tales conductas suelen ser usualmente «primeros pasos» adoptados para el posterior fraude una vez se dispone de la información necesaria. En estas formas de criminalidad hemos visto que la victimización depende muy especialmente de la adopción de actitudes pasivas respecto a la incorporación de autoguardianes capaces digitales, pero también de actitudes proactivas respecto al mundo virtual tales como pasar mucho tiempo en el ciberespacio, entrar en determinado tipo de páginas o descargar archivos sin conocer con seguridad su contenido.

Pero no son éstas las únicas conductas que pueden conllevar un riesgo de victimización por fraude en el ciberespacio, sino que hay muchas otras relacionadas con el comercio y la banca electrónica que hacen que este sector de la actividad en el ciberespacio, por sí mismo, constituya un ámbito de victimización propio y específico que merece ser analizado.

Pues bien, el primer factor que parece estar directamente relacionado con la victimización por ciberfraude es el consistente en realizar compras en Internet. Conforme a un interesante estudio de Pratt, Holfreter y Reisig, realizar compras *online* incrementa la posibilidad de ser objetivo de un ciberfraude en un 377 por 100[30]. Corroborado por otros estudios como el de Marcum, que determinó que el que realiza compras por Internet tiene una probabilidad dos veces mayor de sufrir victimización. Si tenemos en cuenta que el número de usuarios de Internet que realizan transacciones económicas utilizando la Red sigue incrementándose[31], podemos comprender la importancia de este factor y la necesidad de incrementar la protección para los compradores en el ciberespacio.

---

[30] Pratt, T. C.; Holfreter, K., y Reisig, M. D., «Routine Online Activity and Internet Fraud Targeting...», *op. cit.,* p. 281.

[31] «El número de usuarios de Internet que realizan compras en línea también sigue aumentando. Una encuesta reciente manifestó que el 66 por 100 de los consumidores conectados a Internet había comprado *online* algún tipo de producto (por ejemplo, los libros, la música y la ropa), frente al 46 por 100 en 2000», Reisig, M. D.; Travis, C. P., y Holfreter, K., «Perceived Risk of Internet Theft Victimization: Examining the Effects of Social Vulnerability and Financial Impulsivity», en *CJB,* vol. 36, 2009, p. 370.

A partir de la constatación de que la realización de compras por Internet aumenta tan significativamente el riesgo de ser víctima del ciberdelito, resulta interesante analizar el perfil de los cibercompradores. Conforme a un estudio de Rachtford, Talukadar y Lee, los compradores por Internet tienden a ser personas de nivel cultural medio o alto que, además, ocupan niveles de ingresos más bien altos [32]. De hecho, parece que existe una relación entre tener altos ingresos y tener un nivel formativo más alto, con el hecho de comprar más por medios *online* [33].Y aún más clara parece la relación entre el género y la actividad de compra *online*. Según todos los estudios, los hombres suelen hacer mas compras *online* que las mujeres [34]. Aunque se trata de cibercrímenes distintos, esto podría relacionarse con la anteriormente comentada no correlación entre las horas en Internet (no significativa) y la (sí significativa) mayor victimización en hombres que en mujeres. La explicación es que al igual que los hombres compran más *online*, también harán, seguramente, e independientemente de que pasen el mismo tiempo que las mujeres en el ciberespacio, otras conductas no seguras como la descarga de archivos, etc., que explicará que tengan un mayor índice de victimización que las mujeres.

Relacionar la compra *online* con la victimización por ciberfraude tiene sentido si tenemos en cuenta que muchos de los ciberfraudes existentes tienen que ver con esta actividad (los fraudes de subasta y otros, como se vio) [35], pero también si pensamos que al pagar *online* generalmente se acaban «tecleando» los datos bancarios personales y así se incluyen en el sistema como objeto potencial de ataque. Obviamente, no es la propia actividad de compra, sino lo que viene unido a ella, lo que incrementa el riesgo de ser víctima del delito.

3.2. Redes sociales y demás medios de intercomunicación social en el ciberespacio

3.2.1. *Conducta de la víctima y cibercriminalidad social*

El ciberespacio en la era 2.0 es algo más de lo que era: junto a la posibilidad de contacto entre particulares y empresas (y cada uno entre sí) para la realización de actividades económicas, de difusión de información y de conocimiento y, también, pero con limitaciones, para las relaciones personales, surgen ahora variados instrumentos entre los que destacan las redes sociales

---

[32] Ratchford, B. T.; Talukadar, D., y Lee, M., *A Model of Consumer Choice of the Internet as an Information Source,* 2001, pp. 8 y ss.

[33] Korgaonkar, P., y Wolin, L. D., «Web usage, advertising, and shopping: relationship patterns»; en *IR,* vol. 12, núm. 2, 2002, pp. 191 y ss.

[34] *Ibid.;* Soopramanie, D. G., y Robertson, A., «Adoption and usage of online shopping: an empirical analysis of the characteristics of "buyers" and "non-Internet shoppers"», en *JRCR,* vol. 14, núm. 1, 2007, pp. 75 y ss.

[35] Véase *supra* cap. II.

pero también los sistemas de mensajería instantánea a través de los nuevos *smartphones*, que convierten el ciberespacio en un ámbito nuevo para las relaciones sociales, personales, de ocio o laborales, en el que puede existir contacto visual (aunque no físico), en el que las relaciones pueden ser en el mismo momento con usuarios de todo el mundo, y en el que se puede hacer, y de hecho se hace, vida social desde casa, el lugar de trabajo o paseando, pero en el ciberespacio. El principal protagonismo en este sentido lo han adquirido las redes sociales, plataformas de intercomunicación social en las que el usuario puede crear un perfil con elementos de representación de su realidad física pero en el ciberespacio, a través del cual vivir experiencias sociales de amistad y demás en Internet.

A los efectos que nos interesan ahora de definición de los determinantes de la victimización en el ciberespacio, puede decirse que muchas de las actividades cotidianas de las personas en la actualidad se desarrollan en el ciberespacio, y ya no se limitan a navegar en webs para obtener información o para realizar compras, ni a enviar correos electrónicos personales o en relación con el trabajo, sino que llegan mucho más allá y van desde colgar fotos personales para que las vean sus amigos, hacer comentarios sobre el estado de ánimo o acerca de noticias y temas de actualidad, poner información personal sobre el lugar de nacimiento o el estado civil en la web personal, agregar a personas al círculo de contactos individual, comentar las fotos de otros, tener conversaciones verticales en páginas propias o ajenas, mantener conversaciones privadas en chats de las redes o en otros canales IRC, etc. La pregunta que debemos hacernos es si la realización de alguna de estas conductas puede tener relación con la victimización por cibercrímenes sociales tales como el ciberacoso, el ciberacoso sexual, el *cyberbullying*, el *cyberstalking*, las ciberamenazas, las injurias y calumnias por Internet, entre otros. Efectivamente, este tipo de conductas suponen un riesgo tal y como demuestra Reyns, quien detectó que proporcionar el nombre completo, estado civil, orientación sexual, la dirección de correo, intereses, aficiones, fotos y vídeos a través de las redes sociales y en Internet en general se relaciona con la probabilidad de sufrir *cyberstalking*. Desde la premisa de que el delito exige la concurrencia de un agresor motivado, una víctima en ausencia de un guardián capaz y un lugar de ejecución, puede suponerse que a mayor realización de comunicaciones en Internet, a mayor número de usuarios con los que existe relación, a mayor número de actividades sociales distintas en el ciberespacio, mayor será el riesgo de sufrir acoso, injurias o una actividad similar. Además, y como se verá posteriormente, hay algunas conductas en particular que entrañan especial riesgo, como puede ser el compartir con extraños los datos personales en Internet [36]. En todo caso, es necesario, y

[36] Reyns, B., «Being Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/ Routine Activities Perspective...», *op. cit.,* p. 104 (admitir a extraños en las redes sociales está positivamente asociado al contacto repetido no deseado, al *harassment*, la solicitación de sexo,

será posible dentro de poco, confirmar por medio de estudios empíricos de victimización si esto es así y en qué medida, pues apenas hay en la actualidad investigaciones en este sentido.

La mayoría de los estudios de victimización en la línea de relacionar el riesgo con las actividades cotidianas de comunicación social en Internet se centran, sin embargo, en los jóvenes. La razón podría ser doble: por una parte qué duda cabe de que éste es un sector de la población a cuya mejor tutela la sociedad es especialmente sensible, muy particularmente la que se centre en la libre formación de la sexualidad de los menores. Por otra parte, y quizás sea ésta la razón definitiva, son los jóvenes los que de forma más generalizada usan las herramientas de intercomunicación social existentes en el ciberespacio, y no sólo el correo sino, más allá, los chats, sistemas de mensajería instantánea y redes sociales, por lo que son ellos los que van a estar más sometidos a los riesgos de victimización relacionados con la que hemos denominado cibercriminalidad social o personal. Hipotetizamos que los jóvenes son más victimizados por el tipo de actividades que realizan, sin embargo Ngo y Paternoster [37] afirman que a mayor edad, más probabilidad de sufrir una infección de *malware* y de sufrir difamación en línea. Puede ser también que como apuntan Bossler y Holt [38] para las mujeres en el *harassment*, los jóvenes de por sí pueden ser un blanco atractivo (sobre todo en ciberacoso sexual). De todas formas, no hay estudios con muestras con un intervalo de edad amplio que nos permita hacer diferenciaciones por edad. Casi la totalidad de los estudios han sido obtenidos en población estudiantil (universitaria y de los últimos cursos de educación secundaria) tal y como explica Reyns [39].

En todo caso, no son los jóvenes los únicos que sufren victimización por cibercrímenes sociales. También los adultos pueden ser víctimas del ciberacoso en Internet, siendo el *cyberstalking*, especialmente cuando es entendido en sentido amplio, el comportamiento más relacionado con la actividad social en la web 2.0. Como se vio en la parte fenomenológica [40], existe una importante confusión sobre el alcance y prevalencia del *stalking* realizado en el ciberespacio, derivado de la diferente metodología utilizada para realizar los estudios y de la propia existencia de dos concepciones sobre el *cyberstalking*, una estricta en la que se define el mismo como el *stalking* puro realizado por medio de las TIC, y otra más amplia en la que se identifica a la víctima de *cyberstalking* como cualquiera que en dos o más ocasiones haya sido

---

cyberstalking e *identityfraud*. Marcum, Ngo y Paternoster obtienen datos parecidos respecto a la comunicación con desconocidos).

[37] Ngo, F., y Paternoster, R., «Cybercrime Victimization...», *op. cit.,* p. 783.

[38] Bossler, A. M., y Holt, T. J., *Examining the applicability of life style-routine activities theory for cybercrime victimization,* 2009, pp. 16 y 20.

[39] Reyns, B., «Being Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective...», *op. cit.*

[40] Cap. II.2.2.5.2.

acosada, atormentada, atemorizada, le hayan intentado robar su identidad o información personal para perjudicarle, le hayan realizado insinuaciones sexuales, le hayan amenazado o se hayan puesto en contacto con ella tras solicitar que no lo hiciera.

Evidentemente, los resultados de victimización por *cyberstalking* en estudios de estas características serán altos. Así sucede con el análisis realizado por Reyns *et al.*, en el que detectaron que un 41 por 100 de los encuestados de una muestra válida de 974 estudiantes universitarios había sufrido alguna forma de *cyberstalking*. En los resultados se puede observar cómo los porcentajes van disminuyendo cuando se analiza cada uno de los comportamientos por separado, en el que obtuvieron que un 23 por 100 de los encuestados había intentado contactar con ellos en dos o más ocasiones cuando previamente se les había pedido que no lo hicieran (contacto no deseado) un 20 por 100 *harassment* repetido, un 14 por 100 recibió solicitudes de sexo no deseadas y un 4 por 100 amenazas con violencia.

Tampoco hay estudios suficientes que nos ayuden a entender la dinámica de victimización para poder establecer comparaciones fiables sobre las diferencias entre unos y otros casos. Así por ejemplo para Bocij, la víctima del *stalking* tradicional es más probable que conozca a su agresor que en los casos de *cyberstalking*. Pero en cambio, los estudios apuntan a que el perfil de las víctimas es similar a las del *stalking* tradicional, siendo la mayoría de los casos mujeres de menos de treinta años no casadas o divorciadas [41].

Finalmente, la población que tiene más probabilidad de sufrir *cyberstalking* son las mujeres, siendo dos veces más probable que siendo hombre. Reyns obtuvo en su estudio sobre una muestra de estudiantes universitarios, que el 46 por 100 de las mujeres había sufrido algún tipo de *cyberstalking* frente a al 32 por 100 de los hombres [42]. También tienen más riesgo los jóvenes porque están conectados a una variedad de medios electrónicos para comunicarse. En todo caso el predictor que Ryens *et al.*, han obtenido como más relevante ha sido precisamente el de realizar comportamientos desviados en Internet. La víctima más probable es el agresor. Al menos así se constata del estudio en el que determinaron que aquel que realiza más comportamientos desviados en Internet como contactar con alguien en repetidas ocasiones cuando le han pedido que pare, acosar o molestar a alguien por Internet, solicitar sexo a alguien que no quiere, amenazar por Internet, descargar música o películas piratas y enviar o recibir imágenes de contenido sexual, incrementa la probabilidad de sufrir actos de *cyberstalking* o, quizás con más precisión, de *cyberharassment*. Concretamente, multiplica por seis la probabilidad de que alguien contacte en repetidas ocasiones cuando pre-

[41] HENSON, B., «Cyberstalking», *op. cit.,* p. 255.

[42] REYNS, B., «Being Pursued Online...», *op. cit.,* p. 1162. Henson también detectó que las mujeres son más victimizadas de forma significativa. HENSON, B., «Cyberstalking», *op. cit.,* p. 138.

viamente se le ha pedido que no lo haga, por diez la probabilidad de sufrir acoso *online*, por quince las solicitudes de sexo no deseado y el *cyberstalking* en general aumenta catorce veces [43].

Otros factores de riesgo asociados son el uso constante de las redes sociales y de una forma específica: el mayor número de fotos subidas a las redes sociales, el número de actualizaciones de estado y el número de cuentas de redes sociales. También la mensajería instantánea y el contacto con extraños [44].

De nuevo, las actividades cotidianas en el ciberespacio son predictores significativos de la victimización también en la cibercriminalidad social como se verá en particular a continuación para el caso de los menores.

A esto me dedicaré en el segundo punto, a revisar los principales estudios sobre la victimización en menores. Algunas de las conclusiones de los mismos son extrapolables a las conductas de los adultos en el ciberespacio, especialmente aquellas que relacionan el riesgo de victimización en Internet con las actividades cotidianas, dado que, como se ha adelantado anteriormente, las variables sociodemográficas son significativamente menos relevantes que las derivadas de la «vida diaria en Internet». Así, conductas como dar información personal a desconocidos en Internet o utilizar chats y canales tipo IRC, incrementan el riesgo de victimización de cibercrímenes como el acoso, las amenazas y similares en el caso de los menores y todo parece indicar que esto será igual para los mayores.

3.2.2. *Los menores como víctimas de la cibercriminalidad social en el ciberespacio*

La conversión del menor en una víctima potencialmente muy relevante en Internet tiene que ver con lo que Pease señaló hace ya una década muy gráficamente: «Internet terminó con la era de la casa como refugio, al igual que la artillería acabó con la del castillo como fortaleza» [45]. Si la casa y la escuela, la protección familiar e institucional, parecían barreras complejas de superar, algo menos lo son desde el momento en que se ha abierto a los menores, y también a los potenciales agresores de los mismos, una ventana tan grande para la intercomunicación social como es el ciberespacio. De entre los usuarios privados potenciales victimarios de la cibercriminalidad destacan en la actualidad, por su importancia social y por el crecimiento exponencial de su incorporación al ciberespacio, los menores de edad, naci-

---

[43] Reyns, B. W.; Henson, B., y Fisher, B., «Being Pursued Online...», *op. cit.*, pp. 1149-1169. Esto merecería, en todo caso, una revisión mucho más profunda, dado que no influirá de la misma forma todo tipo de «desviación» en todo tipo de victimización.

[44] *Ibid.,* p. 1162.

[45] Pease, K., «Crime futures and foresight...», *op. cit.,* p. 24.

dos ya en la era de Internet, acostumbrados totalmente al uso de las TIC, y tendentes a pasar mucho más tiempo en el ciberespacio que otros usuarios, en los que centraremos posteriormente un análisis más pormenorizado.

Los menores pueden ver atacado su patrimonio al tratar de utilizar su ingenuidad para la realización sobre ellos de estafas tradicionales realizadas por medios informáticos, o al dañarse los datos informáticos que posean mediante los ataques de *malware*; pero no es ése el bien jurídico más en riesgo en su caso. Más bien son bienes jurídicos personalísimos como la intimidad, la libertad sexual o la libre formación de la sexualidad para los que estén en período de formación en este ámbito, los que pueden verse especialmente afectados por la cibercriminalidad. En cuanto a la intimidad, hoy la Red es la forma de interrelación social más poderosa que existe, y en una época en que la búsqueda de la identidad lleva a la multiplicación de la comunicación social como la adolescencia, instrumentos como el correo electrónico o las redes sociales pueden ser tanto un magnífico instrumento para conocer otros jóvenes, como un peligroso modo de difundir información privada que puede ser utilizada con malos fines. Algo similar ocurre con la libertad sexual y la libre formación de la sexualidad en el caso de los menores de trece años: para estos últimos Internet no sólo es un medio de información que puede llegar a ser peligroso sin algún tipo de control educativo, sino que especialmente es un medio de proliferación de la difusión de pornografía infantil que revierte en la multiplicación de este fenómeno y en la consiguiente explotación de miles de menores en todo el mundo para el lucro de organizaciones criminales poderosas. En el caso de los adolescentes, la Red también puede convertirles en objetivo de acosadores sexuales que aprovechen el anonimato del ciberespacio para hacerse pasar por «iguales» y entablar un primer contacto para tratar de lograr posteriormente el contacto sexual.

Antes de analizar los delitos por los que puede haber victimización de menores en el ciberespacio y de concretar las actividades de riesgo en cada uno de ellos conforme a los estudios existentes, es recomendable comenzar con algunos datos generales relativos al uso de Internet por parte de los menores de edad con especial atención al uso del mismo como herramienta de comunicación social.

Pues bien, los estudios señalan que en Estados Unidos, donde obviamente el acceso a las nuevas tecnologías está muy implantado el porcentaje de menores que usa Internet es altísimo y creciente [46]. Concretamente, y conforme al estudio de Lenhart *et al.,* el 94 por 100 de los adolescentes usaba

[46] Ya en 1998 afirmaban el exponencial uso de las TIC por los jóvenes en Estados Unidos IZENBERG, N., y LIEBERMAN, D., «The web, communication trends, and children's health: How the children use the web», en *ClP,* 1998, pp. 335 y ss., pero tales valoraciones aún estaban lejos de la realidad confirmada entre otros por RAINIE, L., *Life Online: teens and technology and the world to come. Speech to the annual conference of the Public Library Association,* Boston, 2006, pp. 25 y ss.

Internet [47], existiendo otros datos también significativos como que el 63 por 100 lo hace diariamente e incluso un 35 por 100 accede varias veces al día [48]. Aunque más de dos tercios de los menores en Estados Unidos (de edades de 12 a 17 años) tienen acceso a conexión de alta velocidad a Internet en casa, el 93 por 100 de los jóvenes accede al ciberespacio desde más de un lugar [49]. Concretamente, y según lo señalado por el citado estudio de Lenhart *et al.,* el 89 por 100 accede desde casa, el 77 por 100 accede desde la escuela, el 71 por 100 accede desde casa de un amigo y el 60 por 100 desde la biblioteca.

Internet, por tanto, está absolutamente arraigado en Estados Unidos como forma de comunicación de los jóvenes, acercándose o superando el 90 por 100 de los que lo utilizan en todas las categorías demográficas y socioeconómicas, si bien el porcentaje de acceso es mayor en algunos grupos (blancos y adolescentes de familias con mayores ingresos) que en otros (hispanos y familias de bajos ingresos).

Resulta significativo que, conforme a los estudios existentes, este masivo uso de Internet por los jóvenes se realice sin apenas control de los padres [50]. Son muchos los estudiantes que usan sus ordenadores personales, *smartphones* y otros servicios móviles y los de sus amigos sin ningún tipo de supervisión parental, y sin ningún tipo de orientación previa ni de la familia ni de las instituciones escolares o demás públicas sobre el uso seguro de Internet [51]. Y esto se corresponde con la constatación de que la mayor parte de los padres, profesores y adultos en posiciones de responsabilidad en relación con los niños están desinformados sobre los riesgos del ciberespacio y no son capaces de educar para la prevención de los ataques a los menores en el ciberespacio [52]. La cuestión es importante, pues según estudios recientes, la monitorización por parte de los padres del comportamiento de los menores en Internet reduce significativamente el riesgo de estar expuesto a materiales o a conductas peligrosas [53]. También se constata en el mismo estudio, sin embargo, que la eficacia de tal actividad de monitorización disminuye conforme aumenta la edad de los menores [54]. A esto hay que sumar la conclusión de otros estudios, como el de Fleming *et al.,* relativo a los efectos de las medidas

---

[47] Lenhart, A., Arafeh, S.; Macgill, S. A., y Rankin, A., «Writing, Technology and Teens», Pew Internet and American Life Project», 2008. En Internet, en *http://www.pewinternet.org/Reports/2008/Writing-Technology-and-Teens.aspx?r=1* (última visita el 9 de septiembre de 2010), p. 4.

[48] Patchin, J. W., e Hinduja, S., «Trends in online social networking: adolescent use of MySpace over time», en *New Media Society*, enero, 2010, pp. 197 y ss.

[49] *Ibid.*

[50] Mcquade III, S. C., «Cybercrime», *op. cit.,* p. 481.

[51] *Ibid.,* p. 489.

[52] *Ibid.,* p. 490.

[53] Lwin, M.; Stanaland, A., y Miyazaki, A., «Protecting children's privacy online: how parental mediation strategies affect website safeguard effectiveness», en *Journal of Retailing,* 2008, pp. 207 y ss.

[54] *Ibid.,* p. 212.

de protección parental para evitar la victimización *online* de los menores. Conforme a tal investigación y a otras más genéricas pero que también abarcaban tales elementos [55], la instalación de filtros y otras formas de *software* para el control parental no tiene efectos significativos en la exposición de los menores a contenidos nocivos o en la victimización por cibercrímenes [56].

Pasando ya al análisis de las concretas actividades llevadas a cabo por los jóvenes en el ciberespacio, resulta adecuado comenzar por la herramienta que más usa este segmento de la población aunque no tiene por qué ser la que dé lugar a mayor victimización: las redes sociales. Conforme al estudio de Lenhart y Madden de 2007, más del 55 por 100 de los adolescentes usan alguna red social en Internet [57], utilizándola como forma de comunicación social para sus relaciones de amistad, amorosas y familiares [58], pero también para contactar con desconocidos o con conocidos compañeros del colegio [59]. Y el uso no es del todo ocasional: el 23 por 100 de los jóvenes visita su perfil varias veces al día, el 34 por 100 por lo menos una vez al día, y el 17 por 100 por lo menos una vez a la semana [60]; de todo lo cual no hay conocimiento mayoritario de los padres según los propios menores: el 42 por 100 de los encuestados que accedían a las redes sociales afirmaban que sus padres conocían la existencia de su perfil, pero sólo el 26 por 100 confirmaban que su familia había visitado el mismo.

El acceso y utilización de redes sociales conlleva, de algún modo, la realización de actividades que pueden incidir en una potencial victimización. Así, según el estudio de Lenhart y Madden, del 55 por 100 que tienen perfiles *online*, el 49 por 100 «postea» información personal relativa a la escuela en la que estudia, el 29 por 100 el nombre completo, y el 29 por 100 la dirección de correo electrónico. Más completo es el estudio de Pierce, en el que a partir del estudio de 700 perfiles de jóvenes en Myspace se llega a los siguientes resultados que muestran un importante uso de los datos personales en las redes sociales [61]:

---

[55] MARCUM, C. D., «Adolescent Online Victimization...», *op. cit.,* p. 270.

[56] FLEMING, M.; GREENTREE, S.; COCOTTI-MULLER, D.; ELIAS, K., y MORRISON, S., «Safety in cyberspace: Adolescents'safety and exposure online», en *YS*, 38, 2006, pp. 136 y ss.

[57] LENHART, A., y MADDEN, M., «Teens, privacy and online social networks...», *op. cit.*

[58] MAZUR, E., «Teen blogs as mines of adolescent data», en *TP,* 32, 2005, pp. 1 y ss.

[59] WILLIAMS, A. L., y MERTEN, M. J., *A review of online social networking profiles by adolescents: Implications for future research and intervention,* Libra Publishers Inc. 2008, p. 260.

[60] PIERCE, T. A., «Talking to Strangers on MySpace: Teens' Use of Internet Social Networking Sites», en *Journal of Media Psychology*, vol. 11, núm. 3, 2006. En Internet, en *http://www.calstatela.edu/faculty/sfischo/myspace.htm* (última visita el 1 de agosto de 2011). Concretamente, se seleccionaron 700 sitios de MySpace al azar utilizando el *browser*, opción dentro de la opción de búsqueda del sitio de redes sociales, resultando finalmente elegidos 426 perfiles de mujeres y 274 de varones.

[61] Los resultados en aquellos ítems también utilizados, son comparables a los del estudio realizado por HINDUJA, S., y PATCHIN, J. W., «Personal Information of Adolescents...», *op. cit.*, p. 134, aunque con diferencias. Por ejemplo, en el estudio de Hinduja y Patchin las personas que incluían el primer apellido eran el 40 por 100 frente al 53 por 100, en el estudio de Piercey en lo relativo a la

Tabla 5.2. Información personal incluida en MySpace en el estudio de Pierce.

Información personal incluida en páginas abiertas de MySpace	*% incluido*
Información personal	95
Edad	93
Domicilio	93
Imágenes propias	81
Comentarios personales	70
Sólo nombre	53
Alias	28
Nombre y apellidos	12
Imágenes propias y de otros	6
Número de teléfono	4
Correo electrónico / Dirección MI	3
Dirección personal	1
Acceso a webcam	1

Más significativo aún resulta el análisis en lo relativo a las imágenes con contenido sexual que comparten los menores en las redes sociales [62].

Tabla 5.3. Análisis de las imágenes con contenido sexual que comparten los menores en las redes sociales.

Contenido sexual	*% incluido*
Subido de tono / poses sexuales (vestido pero sugerente)	59
Desnudo frontal parcial (hombre)	28
Desnudo frontal parcial (mujer)	17
Mostrar las nalgas desnudas	14
Enlaces a pornografía	9

ciudad el 83 frente al 93 por 100, y es muy similar el porcentaje de quienes ponen el nombre completo (9 por 100 en el caso de Hinduja y Patchin frente al 12 por 100). En todo caso, las diferencias entre los indicadores se mantienen.

[62] PIERCE, T. A., «X-Posed on MySpace: A Content Analysis of "MySpace" Social Networking Sites», en *Journal of Media Psychology*, vol. 12, núm. 1, winter, 2007. En Internet, en *http://www.calstatela.edu/faculty/sfischo/X-posed_on_%20MySpace.htm* (última visita el 1 de agosto de 2011).

Tabla 5.3. *(cont.).*

Contenido sexual	*% incluido*
Ver a través de la ropa	9
Contacto homosexual	8
Animaciones / dibujos animados con actos sexuales	8
Desnudo completo (mujer)	6
Visualización de «otros» contenidos sexuales	6
Autoenlace en una web con pornografía	4
Animaciones / dibujos animados desnudos	4
Exposición de genitales	4
Desnudo completo (hombre)	4
Copulación	2
Masturbación	1

Así, como señalan Patchin e Hinduja, resulta significativo que mientras que un pequeño porcentaje de los menores ponen su nombre completo, el número de teléfono o la dirección de correo electrónico, un significativo número de menores incluye fotos con poses sexualmente reveladoras e incluso desnudos, que son más habituales en los hombres que en las mujeres [63]. Evidentemente, lo relevante ahora sería relacionar estos datos con la victimización por cibercrímenes como el *online grooming* o el *cyberbullying*. En relación con el primero, y como se verá al analizar estas conductas, puede tener mucha importancia el compartir datos personales, mientras que en relación con el acoso escolar puede ser muy relevante el que el agresor acceda a las fotos personales para, posteriormente, ridiculizarle o hacer un uso abusivo de ellas. En todo caso, existen estudios empíricos que demuestran la relación entre la entrega de información personal *online* y la victimización por los delitos más relacionados con los jóvenes como víctimas (ciberacoso sexual y *cyberbullying*) [64].

Junto con las redes sociales también es habitual el uso de los canales de chat por parte de los menores y, conforme se verá posteriormente, tal ámbito de comunicación conlleva un mayor riesgo de victimización que otros como las redes sociales debido al tipo de contacto virtual: inmediato y *tête-à-tête*, que caracteriza al mismo. Pues bien, el estudio de Lenhart *et al.,* concluye que el uso de las salas de chat por parte de los menores ha ido decreciendo

[63] Patchin, J. W., e Hinduja, S., «Trends in online social networking...», *op. cit.*, p. 201.
[64] Marcum, C. D., «Adolescent online victimization...», *op. cit.,* p. 269.

significativamente, pasando de un 55 por 100 de menores que utilizaban dicha forma de comunicación en 2000, a un 18 por 100 en 2007, quizás por las campañas de sensibilización entre los padres sobre los riesgos de la comunicación con extraños en salas de chat, o también por su sustitución por otras formas de interrelación personal como las redes sociales [65].

Y algo similar sucede con el uso del *e-mail* por parte de los menores de edad. Pese a tratarse de una poderosa herramienta para la comunicación entre personas, su uso está esencialmente asociado a la comunicación profesional y, por tanto, al entorno laboral, siendo escaso (el 14 por 100) su uso por parte de los menores de edad según los estudios existentes [66].

Por el contrario, los blogs son herramientas de comunicación que han comenzado a ser muy populares entre los adolescentes. Según el estudio de Lenhart en Estados Unidos, el porcentaje de adolescentes que han creado un blog o diario personal en el ciberespacio pasó de un 19 por 100 en 2004 a un 28 por 100 en 2006 [67]. Conforme a tal investigación, hay significativas diferencias entre su uso según el sexo: las adolescentes crean blogs en un porcentaje mucho más alto (35 por 100) de lo que lo hacen los adolescentes (20 por 100), creciendo tal diferencia de porcentaje con la edad (los de las adolescentes de 15 a 17 los crean un 38 por 100 frente al 18 por 100 de los adolescentes de la misma edad) [68].

Pasando ya a los condicionantes de la victimización de menores, resulta evidente que la misma dependerá del tipo de comportamiento delictivo y que, por tanto, habrá que analizar las características psicosociales de las víctimas para la predicción de la agresión de que se trate. Aun así hay quien ha señalado elementos generales a todos ellos. Es el caso de McQuade, quien señala que la mayoría de los jóvenes que son victimizados conocen en el entorno físico a su agresor. Esto supondría que pese al potencial crecimiento de víctimas y agresores que pueden ponerse en contacto en el ciberespacio, seguiría siendo en el entorno cercano donde se producen los contactos sociales que darán lugar posteriormente a la victimización. El ciberespacio simplemente se convierte, en estos casos, en un instrumento más para el ataque de una persona que conoce a su víctima en el espacio físico pero que prefiere realizar el mismo en el virtual, quizá por la seguridad o tranquilidad que da éste. Es discutible, sin embargo, y necesitaría de un refrendo empírico, que esto sea así para todos los delitos por los que puede haber victimización

---

[65] PUJAZON-ZAZIK, M., y PARK, M. J., «To Tweet, or Not to Tweet: Gender Differences and Potential Positive and Negative Health Outcomes of Adolescents' Social Internet Use», *Am. J. Mens Health*, 2010, p. 79

[66] LENHART, A., y MADDEN, M., «Teens, privacy and online social networks...», *op. cit.*

[67] *Ibid.*

[68] *Ibid.,* pp. 1 y ss. Añaden que la comparación se hace más evidente si se confrontan las adolescentes de 12 a 14 con los adolescentes de 15 a 17, un 32 por 100 en el primer caso y un 18 por 100 en el segundo.

de menores en el ciberespacio. Es lógico pensar que el conocimiento en el espacio físico estará más presente entre agresor y víctima en el *cyberbullying* que en el *grooming*. Vamos a analizar a continuación algunos caracteres concretos de la victimización en estos delitos centrándonos, en todo caso, en las variables demográficas y las relacionadas con las actividades cotidianas en el ciberespacio y dejando de lado, por tanto, las psicosociales que serán esenciales para el estudio de la victimización de cada tipología criminológica pero que interesan menos a la hora de una caracterización genérica de la victimización en el ciberespacio.

Obviamente, uno de los delitos en los que va a ser común la victimización de menores será el *cyberbullying* o acoso escolar ejercido en el ámbito del ciberespacio, concretado en el acoso, intimidación o difamación a través de Internet o el teléfono móvil a un menor por medio de mensajes de *e-mail*, burlas en los perfiles de las redes sociales, fotos de *sexting* enviadas a terceras personas para humillar a la víctima, etcétera.

El *cyberbullying*, pues, se conforma por conductas similares a las que el acosador ejecuta sobre la víctima en el espacio físico: desprecio, insultos, amenazas, rumores, actos de ridiculización, ignorar a la persona, etc.; cambiando tan sólo que no existen agresiones físicas dado que todas esas conductas se realizan a través del ciberespacio, especialmente por medio de mensajería instantánea o a través de las redes sociales como puede verse en la tabla de la página siguiente [69].

Aunque los estudios demuestran que sigue siendo mayoritario el *bullying* realizado por medio de agresiones físicas (20,8 por 100), verbales (53,6 por 100), sociales (51,4 por 100), frente a las realizadas en el ciberespacio (13,6 por 100) [70], todos los estudios constatan que conforme se va implantando el uso de las TIC entre los menores el ciberacoso escolar aumenta.

Conforme al estudio de Magid, un 9 por 100 de los usuarios de Internet menores de 18 años fueron acosados en línea, siendo un 6 por 100 los suje-

---

[69] Sourander, A.; Brunstein Klomek, A.; Ikonen, M.; Lindroos, J.; Luntamo, T.; Koskeleainen, M.; Ristkari, T., y Helenius, H., «Psychosocial Risk Factors Associated With Cyberbullying Among Adolescents. A Population-Based Study», en *AGP,* núm. 67, 2010, p. 724.

[70] Wang, J., Iannotti, R. J., y Nansell, T., «School Bullying Among US Adolescents: Physical, Verbal, Relational and Cyber», en *JAH,* núm. 65, 2009, octubre, pp. 368 y ss. Cifras diferentes, pero resultados similares especialmente en lo relativo a la prevalencia del *bullying* tradicional frente al *cyberbullying*, da el estudio de Smith, P. K.; Mahdavi, J.; Carvalho, M.; Fisher, S.; Russell, S., y Tippett, N., «Cyberbullying: its nature and...», *op. cit.*, pp. 376 y ss., conforme al cual frente a los datos del acoso físico de un 14,1 por 100 habitualmente (dos o tres veces al mes o bien una o varias veces a la semana), y del 31,5 por 100 no habitualmente (una o dos al mes) y el 54,3 por 100 nunca, para el *cyberbullying* las cifras eran del 6,6 por 100 a menudo y del 15,6 por 100 no habitualmente, y el 77,8 por 100 nunca. Similares conclusiones de la prevalencia del *bullying* frente al *cyberbullying* se derivan del estudio de Sourander, A.; Brunstein Klomek, A.; Ikonen, M.; Lindroos, J.; Luntamo, T.; Koskeleainen, M.; Ristkari, T., y Helenius, H., «Psychosocial Risk Factors Associated...», *op. cit.,* pp. 720 y ss.

Tabla 5.4. Características de los métodos, localización y total de cibervíctimas.

Características	*Respondieron sí*				
	Núm. total	*Muestra total, % (n=2.215)*	*Chicos, % (n=1.093)*	*Chicas, % (n=1.094)*	χ^2 *P Valor*
¿Cuántas veces has sido cibervictimizado de esta forma?					
Has sido ignorado por otros	2.136	7,6	4,9	9,9	<0,001
Falta de respeto	2.137	10,4	7,9	12,5	<0,001
Te han puesto apodos	2.136	17,7	16,0	18,7	0,10
Han vertido rumores	2.134	13,8	10,4	16,8	<0,001
Te han amenazado	2.135	6,9	8,3	5,1	0,003
Te han bombardeado con *e-mails*	2.136	8,5	7,7	8,8	0,32
Se han burlado de ti	2.135	13,3	12,8	13,7	0,54
Te han ridiculizado	2.135	9,7	8,9	10,0	0,42
Te han dejado en ridículo	2.135	4,2	4,3	3,9	0,65
¿Dónde tuvo lugar el *ciberbullying*?					
Sala de chat virtual	2.089	3,7	3,6	3,6	0,95
Servicio de mensajería instantánea	2.095	18,0	12,6	23,0	<0,001
E-mail	2.088	2,6	2,5	2,2	0,63
Mensajes de texto en el teléfono	2.093	8,2	5,7	10,3	<0,001
Grupos de discusión, ejemplo: IRC-Galleria, Suomi24, MySpace	2.098	13,8	8,8	18,3	<0,001
Sala de chat, ejemplo: IRC, Suomi24	2.083	5,6	5,0	5,7	0,47
Otros	1.530	3,7	4,7	2,4	0,02
¿Quién fue tu agresor?					
Compañero del mismo sexo	2.065	20,1	16,4	23,7	<0,001
Compañero del sexo opuesto	2.063	10,5	5,0	16,0	<0,001
Adulto del mismo sexo	2.044	2,3	2,6	2,1	0,46
Adulto del sexo opuesto	2.047	3,1	2,1	4,0	0,01
Persona desconocida (no está seguro de la edad)	2.052	10,0	8,9	10,7	0,16
Grupo (ejemplo: grupo de amigos, clase)	2.044	5,1	5,0	4,9	0,90

tos que respondían haberlo hecho; además los objetivos generalmente son chicas adolescentes (58 por 100) frente a los varones (42 por 100), siendo también mayores los episodios de acoso en adolescentes de 14 a 17 años (72 por 100) que en los adolescentes menores [71].

En cifras similares se sitúa el estudio de Kowalski y Limber, quienes cifraron en un 11 por 100 las víctimas del *cyberbullying*, siendo un 4 por 100 *bullies* o acosadores y situándose un 7 por 100 en ambas categorías [72]. De todos modos estas cifras no pueden considerarse concluyentes, cuanto menos si se comparan con las de otros estudios rigurosos y coherentes con otros análisis sobre el *bullying* tradicional [73]. Así, por ejemplo, en el estudio realizado por Qing Li que constata un mayor índice de victimización de los menores por *cyberbullying*. Concretamente en la investigación con una muestra de más de 450 personas se concluyó que uno de cada tres adolescentes había sido víctima de ciberacoso, uno de cada cinco era ciberacosador y más de la mitad había experimentado o escuchado que alguien cercano había sufrido un incidente de acoso cibernético [74]. Y en un término medio, en el estudio quizás más preciso metodológicamente, se sitúa el análisis de Carroll Campfield, quien ofrece unos porcentajes de casi un 20 por 100 de cibervíctimas y más de un 10 por 100 de ciberagresores que podrían ser los más cercanos a la realidad. Haciendo un repaso de los estudios restantes los porcentajes de menores implicados en casos de *cyberbullying* se sitúan entre un 40 y un 55 por 100 de los escolares, situándose el porcentaje de alumnos que dicen haber sufrido algún tipo de conducta entre el 20 y el 50 por 100, reduciéndose este porcentaje a entre un 2 y un 7 por 100 cuando la violencia sufrida es severa [75]. La conclusión, por tanto, es que es imposible generalizar sobre la prevalencia e incidencia del *cyberbullying* porque cada estudio usa una metodología distinta, los porcentajes de victimización varían desde el 55 por 100 en Estados Unidos y en Asia hasta el 22 por 100 del resto de países americanos, el 30 por 100 en Europa, y un 25 por 100 Canadá y Oceanía) [76].

---

[71] MAGID, L., «What Can Parents Do about Web Safety? Talking to Teens and Tweens, Says Larry Magid, Can Help a Lot», CBS Interactive Inc., 2006. En Internet, en *http://www.cbsnews.com/stories/2006/11/13/scitech/pcanswer/main2174962.shtml*.

[72] KOWALSKI, R. M., y LIMBER, S. P., «Electronic bullying among middle school students», en *JAH,* 2001, pp. S22 y ss.

[73] Por ejemplo, el de PELLEGRINI, A., y BARTINI, M., «A longitudinal study of bullying, victimization, and peer affiliation during the transition from primary school to middle school», en *American Educational Research Journal,* 37 (3), 2000.

[74] LI, Q., «Bullying in the new playground: Research into cyberbullying and cyber victimization», en *Australasian Journal of Educational Technology,* 2007, pp. 436 y ss. Estas cifras son similares a las del estudio de Patchin e Hinduja que establece en un 29 por 100 el porcentaje de personas victimizadas y en un 11 por 100 el porcentaje de «matones» en el ciberespacio. PATCHIN, J. W., e HINDUJA, S., «Trends in online social networking...», *op. cit.*, p. 201.

[75] GARAIGORDOBIL, M., «Prevalencia y consecuencias del *cyberbullying*: una revisión», en *IJPPT*, vol. 11, núm. 2, 2011, pp. 233-254.

[76] *Ibid*.

Tabla 5.5. Frecuencias de los miembros del grupo de *cyberbullying* ($N = 219$)[77].

Grupo	*Frecuencia (N)*	*Porcentaje*
Cibergrupo control	67 (Cibercontrol)	30,6%
Ciberbullies	26 (CB)	11,9%
Cibervíctimas	42 (CV)	19,2%
Cyberbullying / víctimas	82 (CB/V)	37,4%

Tampoco hay coincidencia en los porcentajes relativos al género. Algunos estudios informan sobre la tendencia de los chicos a ser agresores y las chicas a ser víctimas, mientras que otros estudios no encuentran diferencias. Datos que, pese a la necesidad de mayor investigación, apuntan a contradecir las cifras del *bullying* tradicional, donde tanto agresores como víctimas son, en su mayoría chicos, salvo en determinadas conductas como «hablar mal», que las hacen y las reciben más las chicas[78].

Tabla 5.6. Asociación entre género y relación con *cyberbullying* y/o victimización.

	Hombres	*Mujeres*
Víctima de *cyberbullying,* víctima de *bullying* (56) (94)	37%	63%*
No víctima de *cyberbullying* o víctima de *bullying* (38) (30)	56%	44%
		$\chi^2(1) = 6{,}56$*

En cuanto a la edad, hay estudios en los que se ha demostrado que a más edad, más probabilidad, como el de Kowalski y Limber, y el de Patchin e Hinduja, mientras que Slonje y Smith encontraron tasas más altas para los estudiantes entre 12-15 años, y Smith *et al.* no encontraron ninguna relación entre la edad y ser víctima.

Pero más interesantes que las variables sociodemográficas, son otras que definen distintos e importantes factores de riesgo de victimización por el ciberacoso. Uno de los más relevantes según el estudio de Li es el haber sido previamente ciberacosador: el «matón» tenía una probabilidad 2,81 veces mayor

[77] Carroll Campfield, D., «Cyberbullying and victimization: psychosozial characteristics of bullies, victims, and bully/victims», en Internet, en *http://etd.lib.umt.edu/theses/available/etd-12112008-120806/unrestricted/umi-umt-1107.pdf*, p. 61.

[78] Defensor del Pueblo-UNICEF, *Violencia escolar..., op. cit.*

que el que no lo había sido nunca de ser víctima del *cyberbullying* [79], lo cual coincide en lo esencial con el de Patchin e Hinduja que muestra como significativo elemento configurador del ciberagresor el haber sido previamente víctima [80]. Por el contrario, los estudiantes que habían sido víctimas tenían un índice de riesgo ligeramente inferior de ser ciberacosador que los estudiantes que no lo habían sido [81]. Ya más relacionada con los postulados de la teoría de las actividades cotidianas, Li también relaciona el riesgo de victimización con la frecuencia de acceso a Internet, si bien lo analiza desde la perspectiva del agresor. Los usuarios que lo hacían más frecuentemente (más de tres veces al mes) tenían casi el doble de probabilidad de ser acosadores que los que accedían menos de cuatro ocasiones al mes [82]. Ybarra encontró como predictor de victimización para las chicas la cantidad de uso de Internet y programas de mensajería instantánea y para los chicos el uso de Internet. Respecto al uso de Internet, Patchin e Hinduja [83] llegaron a una conclusión similar, los jóvenes que participaron en más actividades en línea son más propensos a experimentar el acoso en línea. Juvonen y Gross encontraron que el uso de la mensajería instantánea y las webcams aumenta la probabilidad de ser acosados de forma repetida. Y Vandebosch y Lleemput [84] concluyeron que los niños con padres menos involucrados en Internet tienen mayor probabilidad de convertirse en víctimas.

Por otra parte, y muy relacionado con las especiales características del nuevo ámbito de oportunidad criminal que es el ciberespacio y que se analizaron anteriormente, parece que existe una relación entre el anonimato que puede brindar Internet y la victimización por ciberacoso en el ámbito escolar [85]. Esta conclusión podría derivarse del dato, extraído del citado estudio de Li, de que casi la mitad de las víctimas cibernéticas no conocía a sus acosadores [86]. Frente a la necesidad de un contacto personal y directo que conlleva el *bullying*, con los consiguientes riesgos que ello lleva aparejado para el agresor (especialmente el riesgo a ser cazado, pero también a recibir represalias, o a percibir un reproche social), así como la propia percepción del daño que se está causando [87], el ciberacoso permite ocultar la identidad del agresor y, así, evitar las consecuencias o, cuanto menos, eludir el efecto de las mismas en la motivación del agresor.

---

[79] Li, Q., «Bullying in the new...», *op. cit.,* pp. 435 y ss.

[80] En su estudio, de la muestra de jóvenes menores de 18 años de edad del 11 por 100 que reconocía haber realizado *cyberbullying* un 75 por 100 afirmaba haber sido víctima del mismo, frente al 29 por 100 general que reflejaba tal victimización.

[81] Li, Q., «Bullying in the new...», *op. cit.,* pp. 435 y ss.

[82] *Ibid.*

[83] Patchin, J. W., e Hinduja, S., «Bullies Move Beyond...», *op. cit.*

[84] Vandebosch, H., y Van Cleemput, K., «Cyberbullying among youngsters...», *op. cit.*

[85] Así lo señalan también, Mitchell, K. J.; Finkelhor, D., y Wolak, J., «Youth Internet users at...», *op. cit.,* pp. 532-537.

[86] Li, Q., «Bullying in the new...», *op. cit.,* pp. 435 y ss.

[87] Carroll, D., «Cyberbullying and victimization...», p. 32.

Por último, también destaca del estudio de Li la escasa información que reciben los adultos del *cyberbullying*. Más de la mitad de las cibervíctimas no informó a los adultos acerca de los incidentes, y menos del 35 por 100 de todos los encuestados afirmaban haber informado acerca de algún incidente propio o ajeno [88]. Señala Li que esto reproduce el patrón identificado en la investigación del *bullying* cara a cara: tanto espectadores como víctimas callan [89].

Junto con el *cyberbullying* el comportamiento criminal en el que puede existir una significativa victimización de jóvenes es el *online grooming* o ciberacoso sexual en Internet. El *grooming*, término con el que los analistas de los depredadores sexuales se refieren a las conductas de acercamiento de los pederastas a sus víctimas previas al propio contacto o ataque sexual, ha pasado de los parques a la Red, donde por motivos obvios son muchos más los menores, especialmente las chicas [90], que pueden ser objeto de un ataque de ese tipo. En la cuestión del perfil de las víctimas potenciales del *grooming*, y dejando de lado el estudio de los rasgos de la personalidad que inciden en el riesgo de sufrir un ataque de este tipo [91], resulta de especial interés, a los efectos de valorar posteriormente el modelo penal de intervención, la cuestión de la edad de la víctima. El Código Penal, como se verá, ha situado el tope legal en 13 años, frente a lo primeramente establecido por la enmienda que presentó la necesidad de la tipificación del precepto que se remitía como límite a la «minoría de edad». En el *grooming* tradicional, el llevado a cabo por el pedófilo, el objetivo del agresor era, como se ha visto, el menor de 12 años, sin embargo los estudios existentes señalan que en el *grooming* usando las TIC la edad de la víctima aumenta. Según el estudio de Wolak, Finkelhor, Mitchell e Ybarra el 99 por 100 de las víctimas de intentos de ataques sexuales a través de Internet comprendía edades entre los 13 a los 17 años, quedando el 1 por 100 para víctimas de 12 años, no encontrándose ataques a menores de dicha edad. Es significativo, además, que el 48 por 100 de los ataques de *grooming* se llevaban a cabo sobre menores de 13

---

[88] Li, Q., «Bullying in the new...», *op. cit.,* pp. 435 y ss.

[89] *Ibid.*

[90] En efecto, los estudios victimológicos demuestran que son mucho más propensas a recibir ataques y proposiciones de este tipo las mujeres frente a los hombres, incluso aquellos que empiezan a mostrar tendencias homosexuales. Wolak, J.; Finkelhor, D.; Mitchell, K. J., e Ybarra, M. L., «Online "Predators"*...», op. cit.,* p. 117. Este último es, en todo caso, un colectivo especialmente susceptible de sufrir victimización. Los chicos constituyen el 25 por 100 de las víctimas, pero los estudios demuestran que gran parte de ellos son gais o bien se están cuestionando su orientación sexual. Mitchell, K. J.; Finkelhor, D., y Wolak, J., «Youth Internet users at...», *op. cit.*, p. 534.

[91] Véase al respecto el profundo estudio de Wolak, J.; Finkelhor, D.; Mitchell, K. J.; Ybarra, M. L., «Online "Predators"*...*», *op. cit.,* pp. 63-114*,* quienes concluyen que en contra de lo que se cree no es la inocencia del menor lo que incrementa el riesgo de sufrir un ataque, sino que los factores que hacen a los jóvenes vulnerables a la seducción de esos «*online molesters*», es una compleja suma de factores relacionados con la inmadurez, la inexperiencia y la impulsividad con las que algunos menores viven la sexualidad.

y 14 años [92]. Esto concuerda con la forma de comportarse de los jóvenes en Internet y con la evolución de la «inocencia» en los menores: hasta los 14 años los menores tienden a retraerse y a tomar gran cuidado a la hora de tratar esas temáticas y de contactar con extraños en Internet. Esto cambia a partir de los 15 años, cuando los menores comienzan a tomar riesgos, a contactar con personas desconocidas y a renunciar a parte de su privacidad [93]. Como veremos esto contradice la supuesta eficacia que la reforma del Código Penal pueda tener en relación con los delitos de ciberacoso sexual a menores, si bien sobre estas cuestiones jurídicas se volverá más adelante en profundidad.

Interesa ahora, por el contrario, el análisis de la victimización y, especialmente, lo relativo a la propia conducta de la víctima en relación con el riesgo de ser víctima de un ciberataque de *grooming*. Pues bien, el análisis de la conducta de ciberacoso sexual a menores constata que prácticamente todas las modalidades de ataque se configuran en torno a una similar dinámica en la que el paso inicial suele ser el previo envío, por parte de la víctima, de información personal a personas desconocidas [94]. En efecto, los estudios victimológicos existentes parecen demostrar que mientras que el mero hecho de colgar información personal en páginas web o redes sociales [95], no es un factor que incide en el aumento de riesgo de recibir un ataque de *grooming*, sí lo es el enviar directamente información personal a desconocidos. El dato es importante si tenemos en cuenta que el 55 por 100 de los usuarios jóvenes de 12 a 17 años hacen pública parte de su información en webs o redes sociales [96], y también es lógico si partimos de que el sujeto que realiza *grooming* lleva a cabo un acercamiento personal que tendrá más posibilidades de ser exitoso si es la propia víctima la que ya se ha prestado a enviar información privada al agresor. De nuevo las actividades cotidianas de la víctima, en este caso una de ellas íntimamente ligada con su privacidad, constituyen un elemento decisivo en la selección del agresor de la víctima del ciberataque.

4. ENTRE LA EXAGERACIÓN Y LA BANALIZACIÓN: CIFRA NEGRA Y REALIDAD DE LA AMENAZA DEL CIBERCRIMEN

Resulta oportuno finalizar esta parte del libro en la que se analiza desde la criminología la delincuencia en el ciberespacio tratando la cuestión de la dimensión real de la amenaza que representa en la actualidad, y para el futuro, la cibercriminalidad. Al fin y al cabo, se ha hablado aquí de un in-

---

[92] *Ibid.,* p. 113.
[93] *Ibid.*
[94] *Ibid.,* p. 112.
[95] *Ibid.,* p. 114.
[96] Lenhart, A., y Madden, M., «Teens, privacy and online social networks...», *op. cit.,* pp. 1 y ss.

cremento potencial de agresores y víctimas en el ciberespacio debido a las características de ese nuevo ámbito de oportunidad criminal, se han analizado más de treinta tipos de comportamiento cibercriminal entre los que se ha tratado el ciberterrorismo o la ciberguerra, y ante todo esto es inevitable que surja la cuestión de si no supone ello una exageración de un fenómeno cuya repercusión, en términos cuantificables de denuncias judiciales, no es tan grande como parece. Los informes de la Fiscalía General del Estado apenas hacen mención a la cibercriminalidad. Paralelamente, desde muchos ámbitos se sigue afirmando que su amenaza es creciente: ¿no hay una evidente contradicción en todo ello?

Lo cierto es que en los últimos tiempos desde varios sectores se está observando la necesidad de situar en su justa medida las dimensiones de la amenaza del cibercrimen, y se está observando cómo, curiosamente, a nivel de valoración social y política del fenómeno se están dando dos efectos concatenados y aparentemente contradictorios en el mismo, como son una exageración de algunos aspectos del cibercrimen junto con, por otra parte, una banalización de la gravedad del problema. Voy a analizar brevemente esta cuestión de la máxima importancia.

En efecto, el hecho de que comunicativamente sea muy poderosa la suma de la imagen de un ciberespacio universal y transnacional englobador de millones de conductas en un único punto, con la del crimen en sus múltiples manifestaciones y todo ello bajo el prisma de una sociedad del riesgo insegura como ésta en la que vivimos, ha hecho que exista un temor a la cibercriminalidad que, en muchos aspectos, podría tildarse de exagerado. Hay muchos que señalan que la amenaza de una ciberguerra es totalmente remota, pese a que existe un temor social sobre ella [97]. En el caso del ciberterrorismo, entendido en el sentido más estricto de la utilización del ciberespacio para la realización de ataques terroristas, también ha habido una significativa exageración del alcance del fenómeno que conlleva un temor social más allá de la realidad de la amenaza [98]. Y ese mismo temor se extiende al cibercrimen, al que se sobredimensiona no tanto en lo cuantitativo sino en lo cualitativo, como una amenaza desconocida y más allá de lo real. Así, puede sorprender que en algunas encuestas poblacionales exista un 13 por 100 de personas

---

[97] SOMMER, P., y BROWN, I., «Reducing Systemic Cybersecurity Risk», *Contribution to the OECD project Future «Global Shocks», op. cit.*, p. 6. Señala, sin embargo, GUINCHARD, A., «Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy», en *JSC,* vol. 4, núm. 2, 2011, p. 76, aunque no existe un general acuerdo sobre esto, pues también hay quienes señalan que la guerra cibernética es una posibilidad real, *World Economic Forum, «Global Risks 2011: Sixth edition*», 2011, p. 36. En Internet, en *http://riskreport.weforum.org/*.

[98] Véase especialmente, DUNN CAVELTY, M., «Cyber-Terror - Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate», en *Journal of Information Technology & Politics,* vol. 4, núm. 1, 2007, pp. 19 y ss., y también CONWAY, M., «Cyberterrorism: Media Myth or Clear and Present Danger?» en IRWIN, J. (ed): *War and virtual war: the challenges to communities*, 2004, pp. 25 y ss.

que estén más preocupadas por ser víctima de un cibercrimen que por serlo de un delito en el espacio físico [99], especialmente si lo que se mide no es tanto la probabilidad como el temor dada la mayor gravedad general que conlleva la victimización en el espacio físico [100].

En realidad, y como ha señalado acertadamente Guinchard, el discurso sobre las amenazas cibernéticas tiende a estar dominado por el exceso de publicidad dada a algunas amenazas en perjuicio de los demás, y por las afirmaciones exageradas sobre la frecuencia y magnitud de los ataques [101]. La exageración la llevan a cabo en ocasiones las propias empresas de *software* que colaboran con los organismos públicos para evaluar la amenaza del cibercrimen y que, como interesadas en la financiación de sistemas de protección, pueden exagerar las cifras del crimen [102]. Pero especialmente significativa es la cobertura que realizan los medios de comunicación que se centra, por ejemplo, en la presentación de informes sobre ataques a gran escala, como si cuanto mayor fuera el ataque, más grande fuera la amenaza. Sin embargo, los ciberincidentes pueden ser menos dramáticos comunicativamente pero muchísimo más problemáticos. Por poner un ejemplo, la realización de ataques de denegación de servicio contra las webs de la SGAE y los principales partidos políticos españoles recibe una cobertura informativa impresionante, llegando incluso a ser portada de los principales periódicos nacionales, pese a que la consecuencia de los mismos sea simplemente que unas webs con poca afluencia de usuarios no pudieron ser visitadas durante algunas horas. Mucho más grave es, sin embargo, la pérdida de información para empresas o usuarios debido a las infecciones de *malware* o el aumento de las conductas de ciberacoso escolar a menores tal y como certifica el análisis jurisprudencial, si bien ese tipo de comportamientos nunca recibirá tal cobertura informativa.

Lo cierto es que esta forma de relato distorsiona la percepción pública de las amenazas y, por tanto, enmascara la realidad pudiendo producir el efecto contrario. En efecto, la exageración, junto a la desinformación, puede llevarnos a la minusvaloración de la amenaza del cibercrimen a partir de la

---

[99] Así, cita WILKINSON, S., «The Modern Policing Environment», en BAMMER, G. (ed.): *Dealing with Uncertainties in Policing Serious Crime,* Sidney, SANU E Press, 2010, p. 23, un estudio de 2008 en Reino Unido donde se daba ese 13 por 100 de mayor temor hacia la cibercriminalidad que hacia la criminalidad en el espacio físico.

[100] De modo similar, un estudio financiado por IBM concluyó que aproximadamente el 70 por 100 de los usuarios de Internet creen que es más posible ser víctima de un ciberataque que de un ataque en el espacio físico. PRATT, T. C.; HOLFRETER, K., y REISIG, M. D., «Routine Online Activity and Internet Fraud Targeting...», *op. cit.*, pp. 47, 267.

[101] GUINCHARD, A., «Between Hype and Understatement...», *op. cit.,* p. 86.

[102] Así lo pone de manifiesto GUINCHARD, A., «Between Hype and Understatement...», *op. cit.,* pp. 777 y ss. Mucho más problemático en cuanto a la metodología es el informe de 2011 sobre el costo a empresas y ciudadanos de los delitos cibernéticos en el Reino Unido, calculados en 27.000 millones de libras. Sin embargo, el informe no utiliza, ni para el caso discutir, las estadísticas oficiales sobre la delincuencia cibernética.

creencia de que se está sobrevalorando la misma dada la aparentemente válida constatación de que tal tipo de criminalidad no ha llegado a los tribunales de forma masiva en los últimos años. En otros términos: si llevamos más de una década avisando del riesgo que va a suponer la cibercriminalidad, hablando de ciberguerra y demás, y, sin embargo, nuestros tribunales siguen ocupándose de delitos contra la seguridad vial, de violencia de género y de tráfico de drogas esencialmente, quizá haya que convenir que tal amenaza no lo era tanto. Esta argumentación resumiría el efecto contrapuesto, la «banalización» del cibercrimen, que también es manifiestamente peligroso y además erróneo.

Es peligroso dado que se minusvaloran los riesgos existentes y, con ello, se dejan de adoptar medidas de protección así como de obtención de información para el conocimiento de las dimensiones reales de la amenaza del cibercrimen [103]. Lo cierto es que pese a la completa implantación de las TIC en los ámbitos empresarial y comercial, y pese a su expansión a otros contextos sociales en los que los bienes jurídicos en juego pueden ser incluso más importantes como es todo lo relacionado con la intercomunicación personal, aún son muchos los sistemas informáticos que no tienen sistemas de protección básicos y, lo que es más importante, sigue sin existir una educación en las TIC que, aparte de lo técnico, centre la atención en los riesgos reales existentes y en las posibilidades para detectarlos y evitarlos. Tampoco la prioridad en el mercado de las TIC es la seguridad: se siguen vendiendo sistemas informáticos que van a acceder inmediatamente a redes telemáticas sin antivirus o con *software* que tiene que ser actualizado por el usuario que tiene que ir pagando por su seguridad mientras que la velocidad o la memoria de alta capacidad vienen incorporadas de serie. Como señala Guinchard, es sorprendente que nosotros, ciudadanos privados, pero también instituciones privadas y públicas, toleremos múltiples vulnerabilidades técnicas y sus consecuencias como el precio a pagar por la innovación y la competencia en un mercado libre, cuando nadie toleraría un coche con un sistema de frenado que tiene que ser activado y actualizado por el propio usuario. La cuestión es que se perciben como riesgos algunos que todavía están muy lejanos (ciberguerra y otros ciberataques que afecten a la población y que sólo podrán producirse cuando haya una mayor dependencia de la tecnología también relacionada con los servicios y atenciones básicas) y no se perciben como riesgos otros que sí son reales pero que, de alguna forma, se mantienen ocultos debido, esencialmente, al desconocimiento de las propias TIC y a, en ocasiones, la voluntad de ocultar tales amenazas para el éxito de su implantación social.

Ahora bien, la banalización de la cibercriminalidad sólo es realmente tal si dicha forma de delincuencia existe o, más bien, si supone una problemáti-

[103] GUINCHARD, A., «Between Hype and Understatement...», *op. cit.,* p. 77.

ca creciente y digna de estudio. Al fin y al cabo, todas las expectativas de crecimiento de la cibercriminalidad, todas las previsiones sobre el cibercrimen, parecen chocar violentamente con el escasísimo impacto del ciberdelito en los tribunales de justicia. En Inglaterra, Wall recuerda que en quince años de la *Computer Misuse Act* de 1990 tan sólo ha habido más de doscientos enjuiciamientos [104]. En España, las estadísticas oficiales también constatan un aumento del cibercrimen: es cierto que todavía es tenue, pero qué duda cabe de que la tipificación de nuevas figuras delictivas y, en especial, la popularización de la web 2.0 conlleva la realización de conductas delictivas en el ciberespacio que están comenzando a ser denunciadas aunque aún no tienen gran reflejo en los procesos judiciales.

La cuestión, en todo caso y como ha señalado Wall, es si esa escasez de procesos judiciales por cibercrímenes se debe a la ausencia de pruebas para la imputación de los mismos o más bien a la propia ausencia de cibercrímenes [105], esto es, si en realidad hay una sobredimensión de la amenaza del cibercrimen o una pobre respuesta judicial al mismo debido a factores varios todos más o menos directamente relacionados con la novedad del fenómeno y el anquilosamiento espacial-territorial del sistema de administración de justicia. En el primer caso no habría banalización sino valoración del cibercrimen en su justa medida, como mera anécdota en el océano de la delincuencia tradicional; en el segundo caso sí la habría, y sería necesario tanto una mejora de la observación criminológica de este fenómeno para la correcta mesura del mismo como una intervención decidida en aras a su prevención.

Pues bien, la mayoría de quienes han tratado el tema de la cibercriminalidad con profundidad son de la opinión de que existe una importante cifra negra en materia de cibercriminalidad, esto es, que los delitos que se cometen son muchos más que los que aparecen en las estadísticas oficiales al ser enjuiciados y condenados como tales, hasta el punto de que hay quien ha señalado que la cibercriminalidad es la forma de delincuencia más infradenunciada de toda la existente [106]. Lo entiende así la doctrina [107], que argumenta que si en todo tipo de delincuencia hay una cifra negra, ésta debe ser mayor en el caso de la cibercriminalidad [108]. Pero además, hay datos, y no meras hipótesis, que certificarían que con la cibercriminalidad ocurriría algo

---

[104] WALL, D., «Cybercrime, media and....», *op. cit.,* p. 45.

[105] *Ibid.,* p. 46.

[106] KSHETRI, N., «The Simple Economics of...», *op. cit.*

[107] GONZÁLEZ RUS, J. J., «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», en *RFDUCM,* núm. 12, 1986, p. 109; ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos,* Granada, Comares, 2002. HERRERA MORENO, M., «El fraude informático en Derecho penal español», en *Actualidad Penal,* núm. 39. 2001, p. 8.

[108] DE LA CUESTA ARZAMENDI, J. L., y PÉREZ MACHÍO, A. I., «Ciberdelincuentes y cibervíctimas», en DE LA CUESTA ARZAMENDI, J. L. (dir.), *Derecho penal informático,* Cizur Menor, Civitas, 2010, p. 116.

similar a lo que sucede con los icebergs, que lo que se percibe o visualiza es tan sólo un porcentaje ínfimo en comparación con lo que realmente existe [109]. Variados estudios insisten en que el cibercrimen está en crecimiento desde hace más de diez años, siendo múltiples los ataques recibidos diariamente en España, algunos de los cuales no son propiamente delictivos (el caso del envío de *spam*) pero otros sí, como los daños, el acceso informático ilícito, las injurias y las calumnias, los ataques de DoS, etc. Así lo ponen de manifiesto numerosos informes independientes de algunas importantes empresas de seguridad como Javelin [110], que en su estudio sobre fraude de identidad detectó un incremento de un 12 por 100 de víctimas de esta modalidad de ciberdelito, o el informe encargado a *Pricewaterhouse Coopers* [111], en el que pone de manifiesto que, mientras que en un estudio de 2008 sobre brechas de seguridad en las empresas, el 21 por 100 de los encuestados declararon haber sido infectados por virus u otro *software* malicioso, en 2010 esta cifra ascendió al 61 por 100. Este mismo informe destaca otro dato llamativo: únicamente el 16 por 100 de las empresas encuestadas esperan un número menor de ataques en el año próximo. Otros informes publicados por instituciones gubernamentales o auspiciadas por los gobiernos, como el Internet *Crime Complaint Center* (IC3) [112], constatan que las denuncias por cibercrímenes pasaron de 16.838 en 2000 a 303.809 en 2010 [113]. También parecen certificar esta tendencia de incremento del cibercrimen otro tipo de estudios contra los que no podrá argumentarse, como se hace con los realizados por empresas de *software*, la falta de imparcialidad. Me refiero a las investigaciones sobre victimización en el ciberespacio que abarcan muchos tipos de ciberdelitos, si bien se ocupan más especialmente de las infecciones de *malware,* el *phishing,* el *cyberbullying,* el *online grooming* o el *cyberstalking.* Todas las investigaciones que he citado en este trabajo reflejan un aumento de la criminalidad, si bien debe reprocharse a las mismas que ninguna de ellas cuestiona las razones por la falta de denuncia de estos delitos.

Por último, tampoco debemos despreciar los propios argumentos teóricos que hemos defendido en este libro: la aplicación abstracta de los presupuestos de la teoría de las actividades cotidianas al ciberespacio, que anticiparía, a mi parecer, un aumento del crimen en el ciberespacio conforme los

---

[109] Fafinski, S., y Minassian, N., *UK Cybercrime report 2009*, Invenio Research September 2009, p. 23.

[110] En Internet en *https://www.javelinstrategy.com/news/831/92/Javelin-Study-Finds-Identity-Fraud-Reached-New-High-in-2009-but-Consumers-are-Fighting-Back/d,pressRoomDetail* (última visita el 29 de agosto de 2011).

[111] En Internet en *http://www.infosec.co.uk/files/isbs_2010_technical_report_single_ pages.pdf* (última visita el 29 de agosto de 2011).

[112] El IC3 es una iniciativa fruto de la colaboración entre el FBI, el centro nacional para la criminalidad de cuello blanco («National White Collar Crime Center», NW3C) y la oficina de asistencia a la justicia («Bureau of Justice Assistance», BJA).

[113] Guinchard, A., «Between Hype...», *op. cit.,* p. 80.

comportamientos en sociedad vayan realizándose también en este nuevo ámbito de intercomunicación personal que acerca a personas sin restricción de distancias. La criminalidad en el ciberespacio, por tanto, estaría aumentando y seguirá haciéndolo mientras vayan ampliándose los ámbitos de comunicación entre personas en Internet. No creo que deba exagerarse la amenaza, pues si bien es cierto que los ataques han ido aumentando a lo largo de los años, también lo es que los procedimientos en seguridad también han ido mejorando, y conforme vayan surgiendo ámbitos de criminalidad irán desarrollándose estrategias preventivas que limitarán los efectos de los mismos. Tampoco creo que estemos en condiciones de cuantificar la cifra negra sin ningún tipo de apoyo empírico [114]. Por el contrario sería recomendable la realización de investigaciones empíricas profundas que sirvieran para reflejar las dimensiones reales del fenómeno: por ejemplo, estudios cuantitativos y cualitativos sobre las denuncias archivadas en un determinado ámbito judicial por cibercrímenes, o también de victimización en la población española que certificaran el tipo de ataques recibidos y la posible consideración delictiva de los mismos. La investigación criminológica, sin embargo, no siempre cuenta con los medios necesarios para la realización de tales estudios que, cuando se realizan, tampoco son tomados totalmente en serio por los organismos públicos. Entre tanto podemos, como ha señalado Wall [115], afirmar como única realidad posible los datos oficiales, definir como realidad lo que sólo intuimos, o bien observar y comprender bien el fenómeno y tratar de dimensionar lo más precisamente, dentro de lo posible, el mismo. Para tomar el camino correcto debemos preguntarnos, como ha hecho parte de la doctrina, por las citadas razones de la cifra negra del cibercrimen.

En efecto, reconociendo que la visualización judicial de la cibercriminalidad sería, si no ínfima [116], sí claramente inferior en comparación con el tamaño real del problema, la cuestión central entonces sería ¿por qué? ¿Cuáles son las razones por las que una delincuencia que existe no se manifiesta en las instituciones judiciales?

Pues bien, como señalan acertadamente Fafinski y Minassian [117], si ya de por sí no es fácil contar cualquier tipo de delito, hay buenas razones para que el cibercrimen sea particularmente difícil de cuantificar. Voy a tratar de exponer las principales razones explicativas de la cifra negra del cibercrimen diferenciando entre los que, a mi parecer, son los dos grandes tipos de motivos de que la cibercriminalidad no llegue en toda su dimensión a los tribunales: por una parte los que se relacionan con la falta de denuncia de

---

[114] Álvarez Vizcaya, M., «Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la Red», en *CDJ,* núm. 10, 2001, Madrid, p. 264.

[115] Wall, D., *Cybercrime: the transformation of crime..., op. cit.*

[116] Fafinski, S., y Minassian, N., *UK Cybercrime report 2009*, *Invenio Research September* 2009, p. 23.

[117] *Ibid.*

estos delitos y, por otra, las que lo hacen con el propio proceso judicial aun cuando haya existido denuncia.

Comenzando por estos últimos, no debe ser ningún descubrimiento la afirmación de que los procesos judiciales contra gran parte de los cibercrímenes pueden tener muchas más complicaciones generales que los que se inician contra crímenes en el espacio físico. La razón principal es que cuando existe una denuncia, generalmente en estos casos no dirigida contra alguien en concreto sino reflejando una concreta victimización (un dinero defraudado por un usuario indeterminado, un daño en el sistema por un virus, una calumnia en una página web, etc.), los primeros pasos de la investigación policial se dirigen hacia la determinación de los autores y hay varios motivos por los que ésta puede ser especialmente complicada para estos delitos. En primer lugar, por las propias características, favorecedoras del anonimato, del ciberespacio: aunque el ciberdelito es cometido por alguien en concreto, en Internet sólo se muestra una representación virtual del autor (la dirección IP) que puede ser concretada, pero a la que después hay que atribuir la concreta persona física que está detrás de la acción, y eso ya es más complicado, pues exige, primero, la colaboración de las empresas proveedoras de servicios y, después, la investigación del titular del sistema informático desde el que se ha realizado el ataque y la concreción, de entre todos los usuarios del mismo, del que en particular lo ha ejecutado [118]. En segundo lugar, y relacionado con lo primero, la determinación judicial de las personas autoras del cibercrimen suele complicarse debido a la transnacionalidad del delito. Ya no se trata, como en la criminalidad física, de que el delincuente haya podido trasladarse a otro país tras cometer el delito y haya que solicitar su entrega a las autoridades judiciales españolas, sino de que el delito haya sido directamente cometido desde el extranjero, con lo que los procesos para la identificación del cibercriminal requieren de la colaboración de otros Estados, no siempre sencilla de lograr. Al fin y al cabo, no es lo mismo solicitar la extradición de una persona concreta por la comisión de un determinado delito, que solicitar a un Estado extranjero que investigue quién puede ser el sujeto que se halle detrás de una concreta IP que presuntamente puede haber perpetrado una infracción penal. La práctica judicial demuestra que la fiscalía suele cesar en el intento de identificación cuando la IP se encuentra en Rusia o países similares relacionados con mafias de cibercriminales.

El segundo grupo de motivos, a mi parecer los que constituyen la razón esencial de que exista más cibercriminalidad de la que efectivamente es enjuiciada y condenada, tiene que ver con la falta de denuncia de la víctima del cibercrimen. Las razones son diversas y, probablemente, deban ser valoradas de distinta medida para según qué delito. Al fin y al cabo, la ciber-

[118] *Ibid*.

criminalidad no viene a ser más que toda la criminalidad en el ciberespacio y la cifra negra no será idéntica para todas y cada una de las tipologías de delitos.

En primer lugar, en muchas ocasiones la conducta criminal pasa directamente inadvertida, de modo que no es denunciada aunque haya sido consumada e incluso se hayan logrado los efectos criminales con la misma [119]. Esto puede ocurrir con otros delitos cometidos en el espacio físico, pero de forma muy excepcional, dado que en él la visualidad de los efectos y consecuencias de las acciones es mayor. Así puede ocurrir por ejemplo con las infecciones de virus maliciosos que produzcan daños en los sistemas informáticos, también con injurias y calumnias colgadas en sitios web y que sean percibidas por otros sujetos pero no por la víctima de las mismas, pero especialmente sucederá en el caso del *hacking* o acceso informático ilícito, conducta consistente en la mera intromisión en el sistema informático ajeno, reputada delictiva a partir de la reforma del CP de 2010, y que en muchos casos, prácticamente en la mayoría, no será percibida por el titular del sistema. Incluso puede suceder que la víctima no perciba el ataque en el caso de las defraudaciones en el ciberespacio. Así, señala Álvarez Vizcaya que el intento de descubrir la comisión de fraudes informáticos puede implicar enormes costes debido a las comprobaciones minuciosas, etc., que pueden suponer mayores pérdidas que el propio perjuicio causado [120].

En otros casos, lo que sucede es que la víctima sí se percibe del ataque pero lo hace tarde, cuando el mismo ha prescrito o cuando ya valora absurdo el presentar demanda judicial [121] dado que habrá pocas posibilidades de que la policía llegue a identificar, detener y procesar a los delincuentes [122]. Esto será habitual en los ciberfraudes, especialmente en relación con los bancarios, dado que puede suceder que la víctima se aperciba de que le falta un dinero en su cuenta o de que le han imputado un gasto que no es propio después de que suceda. Desde luego esto es lo que ocurrirá en el *hacking* en aquellos casos en los que la víctima lo perciba, pues es prácticamente imposible que esta conducta delictiva sea visualizada por la víctima en el mismo momento en que acontece. También ocurrirá en las infecciones de virus con resultado de daños, que a veces son percibidas por el sujeto pero no en otros casos, teniendo en cuenta además que el efecto del virus puede tener lugar en un determinado momento pero la infección puede haberse producido en otro muy anterior.

---

[119] *Ibid.*

[120] Álvarez Vizcaya, M., «Consideraciones político criminales sobre la delincuencia informática...», *op. cit.,* p. 257.

[121] De la Cuesta Arzamendi, J. L., y Pérez Machío, A. I., «Ciberdelincuentes...», *op. cit.,* p. 116 y Romeo Casabona, C. M., «Poder informático y seguridad jurídica...», *op. cit.*, p. 38.

[122] Adler, F.; Mueller, G. O. W., y Laufer, W. S., *Criminology and the Criminal..., op. cit.,* p. 351.

Otro factor a tener en cuenta y que ha valorado la doctrina como motivo de la cifra negra de la cibercriminalidad es que la propia víctima, que sí se percibe del ciberataque, ni siquiera valora el mismo como una conducta delictiva, por lo que no procede a denunciarlo. Como señalan Fafinski y Minassian, esto ocurre especialmente en el caso de las infecciones de virus [123], de las que muchos desconocen que generalmente podría ser constitutiva de delito conforme al Código Penal español; pero también ocurre con gran parte del envío de *spam* que contiene mensajes de *scam* (como las cartas nigerianas) o *phishing* que puede ser reputado tentativa de estafa en algunos casos si no es utilización ilícita fraudulenta de la imagen de una empresa o estafa punible en el caso de que se cree una web para el *pharming* y aunque no haya pérdida patrimonial; desde luego sucede con el *hacking* o acceso informático ilícito que todavía no tiene la valoración social de comportamiento delictivo; e incluso puede ocurrir con los pequeños fraudes, con aquellos que producen una pérdida patrimonial tan ínfima para la víctima que puede pensar que ni siquiera resultan delictivos. Como señala Guinchard, sin embargo, los criminales cibernéticos aprovechan esa subestimación crónica de los delitos cibernéticos, puesto que una pérdida de 30 libras o euros para una persona puede significar una ganancia mínima de 3.000 al infractor, ya que las estafas se dirigen a cientos de miles de personas en línea [124].

En otras ocasiones, la razón de la denuncia es precisamente la falta de confianza en las autoridades judiciales para la averiguación de los hechos [125], generalmente por la convicción de la dificultad que conllevará la identificación de los responsables [126]. Esto ocurriría especialmente en los cibercrímenes económicos, particularmente en aquellos en los que las pérdidas no sean dramáticas, y en los que la víctima preferirá la pérdida al propio gasto judicial debido a las dudas que le plantea el éxito de la denuncia. Al fin y al cabo, todos los problemas de identificación y la cuestión de la transnacionalidad del ataque no son ajenos a la víctima, que los tendrá en cuenta a la hora de iniciar un proceso judicial incierto. Por el contrario, cuando la víctima constate que el ciberataque es realizado por alguien conocido (aunque no esté identificado) o de nacionalidad propia es más posible entonces que se denuncie con la esperanza de que se pueda identificar al agresor. Y lo mismo sucederá cuando la denuncia trate de borrar los efectos visibles del delito (en el caso de las injurias, calumnias o atentados a la dignidad de una persona por medio de una publicación en una página web o similar).

Por último, y en particular en relación con las empresas que sufren ciberataques, se suele considerar como determinante en la cifra negra el que para grandes empresas e instituciones públicas resulta tan ventajoso el uso de

---

[123] Fafinski, S.; Minassian, N., *UK Cybercrime report 2009*, *op. cit.*, p. 23.
[124] Guinchard, A., «Between Hype and Understatement...», *op. cit.,* p. 80.
[125] Kshetri, N., «The Simple Economics of Cybercrimes», *op. cit.,* pp. 1 y ss.
[126] Reyna Alfaro, L. M., «La víctima en el delito informático», p. 8.

los sistemas informáticos, por lo que «no es extraño que éstas prefieran, en ocasiones, asumir las pérdidas derivadas de los posibles abusos de terceros a admitir públicamente su vulnerabilidad, mediante la denuncia de dichas conductas», dado que la desconfianza de los clientes respecto al uso de dichos sistemas les supondría muchos más perjuicios que los que se derivan de la propia actividad criminal [127]. Así en un estudio realizado por Kshetri, el 70 por 100 de los cibercrímenes que no son denunciados tienen como razón para no denunciar la publicidad negativa que conllevaría el reconocimiento del ataque sufrido [128]. Esto ocurre especialmente en el caso de los bancos, que no quieren aparecer públicamente como víctimas de fraudes *online* y pueden preferir pagar las indemnizaciones de los clientes antes que reconocer inseguridades en un sistema, el de la banca electrónica, que por los escasos costes de personal les puede resultar muy beneficioso a medio o largo plazo [129].

---

[127] Galán Muñoz, A., «Expansión e intensificación...», *op. cit.*, pp. 18 y 19. También en este sentido Acurio del Pino, S., «La delincuencia informática transnacional y la UDIMP», en *Revista del Derecho Informático*, núm. 95, 2006, p. 17; y Álvarez Vizcaya quien señala que «los perjuicios que ello podría suponer para su reputación podrían ser mayores que el resarcimiento que obtuviesen en una probable pero no cierta, condena. Poco o nulo interés tiene una entidad financiera en manifestar públicamente la vulnerabilidad de su sistema informático», Álvarez Vizcaya, M., «Consideraciones político criminales sobre la delincuencia informática...», *op. cit.,* p. 267.

[128] Kshetri, N., «The Simple Economics of Cybercrimes», *op. cit.,* pp. 1 y ss.

[129] Guinchard, A., «Between Hype and Understatement...», *op. cit.,* p. 80.

GLOSARIO

***Adware*:** Se trata de programas autoejecutables que, generalmente sin conocimiento ni consentimiento del usuario, muestran publicidad en el ordenador al instalarse o al interaccionar con determinadas webs, y que pueden servir para espiar sus hábitos en Internet .

Anonymous: Grupo *hacktivista* abierto e indefinido, conformado por *hackers* entre los que hay desde expertos a meros iniciados, a los que unen convicciones ideológicas antisistema, en general, y en particular contrarias a las restricciones legales en Internet, que venían realizando actividades *hacker* en general y ataques DDoS en particular contra distintos Estados y organizaciones empresariales, pero que saltó a la palestra a finales de 2010 en relación con el fenómeno Wikileaks.

***Antisocial networks*:** Comportamiento consistente en la manipulación de redes sociales o de grupos de ellas con finalidad de utilizarlas posteriormente para el fraude o para cualquier otro tipo de ciberdelito.

***Antispam*:** Herramienta informática que se encarga de detectar y eliminar el *spam* y los correos no deseados.

***Antispyware*:** Aplicación que se encarga de buscar, detectar y eliminar espías en el sistema.

Antivirus: Programa que analiza un sistema informático, en busca de *software* malicioso.

Archivo lmhost: Es un archivo de texto local que asigna direcciones IP a nombres de NetBIOS de servidores remotos con los que se comunica a través del protocolo TCP/IP.

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

***Auction Fraud*:** Fraude cometido en las subastas, consistente en la tergiversación de un producto o su no entrega conforme a lo pactado en los sistemas de subasta *online* tipo eBay.

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

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

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

***Botnet*:** Conjunto de redes de ordenadores comprometidos (*bots*) y controlados por el mensajero.

***Carnivore*:** Es un sistema computacional diseñado para permitir al FBI en colaboración con un proveedor de Internet (ISP) que se haga valer una orden judicial que exige la recolección de cierta información en relación con el correo electrónico u otros tipos de comunicaciones electrónicas de un usuario específico que es objeto de investigación.

Cartas nigerianas: Correo electrónico enviado por el estafador con la intención de engañar al usuario tratando de interesar a la víctima con un potencial beneficio patrimonial o ganarse su confianza para que sea él quien finalmente realice el acto de disposición patrimonial que le perjudica.

Certificados SSL: Archivo electrónico que usa el protocolo *Secure Sockets Layer* que identifica de forma exclusiva a individuos y sitios web en Internet y permite establecer comunicaciones confidenciales y seguras.

Chat: Conversación escrita, virtual y en tiempo real, que tiene lugar en el ciberespacio.

***Chat room*:** Habitación independiente en el ciberespacio, en la que se puede hablar con otros usuarios conectados al mismo canal.

***Childgrooming*:** Consiste en contactar con menores por medio de las redes sociales o de otras formas de comunicación como salas de chat, canales de *messenger* o similares, para acercarse a ellos e intentar posteriormente un contacto sexual.

Ciberacoso: O acoso en el ciberespacio, estaría conformado por el uso de las TIC para atentar de forma continuada, con amenazas, insultos, actos de persecución, etc., contra la dignidad de una persona.

Ciberagresor: Sujeto que utiliza las TIC para realizar un crimen, generalmente mediante el ataque a otra u otras personas.

Ciberataques de contenido: Todos aquellos ciberataques en los que el centro de la infracción lo constituye el contenido que se comunica o se transmite a través de las redes telemáticas, particularmente de Internet.

Ciberataques puros: Todos aquellos ataques en el ciberespacio que no tienen correspondencia en el espacio físico al consistir en un concreto uso de las TIC previamente no existente fuera de Internet.

Ciberataques réplica: Aquellos ciberataques en los que el ciberespacio es el nuevo medio desde el que realizar delitos que tienen su correspondencia en el espacio físico.

Ciberblanqueo de capitales: Cuando se utiliza el ciberespacio y sus diferentes servicios para el lavado de dinero y activos procedentes de actividades ilegales, generalmente de mafias organizadas.

Cibercafés: Lugares públicos dónde conectarse a Internet a cambio de una cantidad económica variable según el tiempo.

Cibercrimen: Cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan.

Cibercrimen económico: Todo cibercrimen o ciberataque realizado con el propósito final de obtener un lucro económico con el consiguiente perjuicio de uno o varios usuarios. Son cibercrímenes económicos tanto aquellos ciberataques en los que la conducta termina en un fraude, como otros que no son más que un acto preparatorio de los ciberataques defraudatorios finales.

Cibercrimen político: Dícese de la utilización, por sujetos individuales, instituciones, grupos, incluso Estados, de Internet como forma de difusión de un determinado mensaje político o como forma de ataque a un Estado o a concretas instituciones no gubernamentales.

Cibercrimen social: Grupo de delitos en Internet que tienen que ver con las relaciones sociales entre las personas y que no son más que la trasposición al ciberespacio de los crímenes tradicionales derivados de conflictos entre personas.

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

Ciberextorsión: Consiste en la solicitud de importantes cantidades económicas a cambio de cesar en la realización de algún tipo de ciberataque o incluso de empezar a ejecutarlo.

Ciberfraudes: Fraude en el que las redes telemáticas se convierten en el instrumento mediante el cual lograr un beneficio patrimonial derivado de un perjuicio patrimonial a una víctima.

Ciberguerra: Actos de guerra entre Estados o contra Estados que tienen lugar en el ciberespacio.

***Ciberhacktivismo*:** Conjunto de ataques llevados a cabo por *hackers* informáticos pero no con una finalidad maliciosa de defraudar a las víctimas, de robarles información para traficar con ella o de causar daños para perjudicarles económicamente, sino con la intención de lanzar un men-

saje ideológico, de lucha política y defensa de ideas generalmente relacionadas con la libertad en Internet, aunque teniendo cabida cualesquiera otras convicciones ideológicas.

Cibermula: Dícese del colaborador o recolector de los beneficios en Internet que luego envía el dinero, por medios seguros de transmisión, a los autores del delito.

Ciberpiratería intelectual: Forma de explotación ilícita de obras protegidas por derechos de propiedad intelectual utilizando Internet.

Ciberterrorismo: Conjunto de actividades realizadas en el ciberespacio por una organización terrorista para difundir sus mensajes, obtener financiación, facilitar la acción de sus bases o directamente para realizar ciberataques terroristas contra objetivos concretos.

Cibervíctima: Persona que sufre los efectos de un ciberdelito.

***Cloaked websites*:** Aquellos sitios web que aparentan ser de ONG u otras organizaciones preocupadas por problemas sociales de cualquier tipo o que simulan ser lugares de transmisión de información, y que ocultan una ideología racista que va apareciendo poco a poco en forma de mensajes web.

***Cookies*:** Archivos que almacenan información del usuario en su propio sistema y que sirven para que los sitios web identifiquen al visitante.

Cortafuegos: Sistema diseñado para impedir el acceso no autorizado a una red privada.

***Crack*:** Programa que provoca una rotura de un sistema, sea de *hardware* o de *software*.

***Cracker*:** *Hackers* que utilizan el acceso informático para robar información relevante, defraudar o causar algún otro tipo de daño.

***Creativecommons*:** Proyecto de licencias libres nacido en Estados Unidos en 2002 que proporciona a los autores un rango flexible de protección y libertad.

***Cybergrooming*:** Ciberacoso sexual a menores.

***Cyberbullying*:** Ciberacoso escolar o a menores, esto es, variante del ciberacoso en la que un menor, atormenta, amenaza, hostiga, humilla, o molesta de alguna otra manera a otro, haciendo uso de Internet, teléfono móvil, videoconsola o alguna otra tecnología telemática de comunicación.

***Cyberhate speech*:** Difusión de mensajes de odio racial en el ciberespacio.

***Cyberstalking*:** Ciberacoso continuado a una persona, consistente en el seguimiento, hostigamiento y persecución de la víctima por medio del uso de Internet. También se define como *cyberstalking*, en un sentido más amplio, la utilización de Internet para realizar uno o más actos de ame-

nazas, insultos, uso indebido de la imagen, solicitud sexual o cualquier otra forma de hostigamiento a una persona.

***Cyberwarfare*:** Forma de definir los ataques planeados por naciones o sus agentes contra sistemas informáticos, terminales y demás con la intención de causar daños en el enemigo.

***Dark Web*:** Sistema de vigilancia creado para rastrear y analizar el contenido publicado en la Red que pueda estar vinculado con terroristas.

***Data breaches*:** Cualquier forma de destrucción, modificación o acceso a datos de empresas o de particulares

***Data mining* (minería de datos):** Técnica por la que se busca toda la información relativa a una persona, incluso aquella aparentemente menos trascendente, tratando de enlazarla y relacionarla posteriormente para poder configurar un retrato lo más certero posible de la persona contra la que se va a realizar el fraude o similar.

Denial of Service (DoS): Denegación de Servicio. Ciberataque consistente en saturar el servidor del sistema logrando que el mismo se centre en la petición que realiza el atacante sin que pueda atender a ninguna más.

Distributed Denial of Service (DDoS): Ataque de Denegación de Servicio Distribuido. Se trata de una denegación de servicios realizada, simultáneamente, desde varios sistemas informáticos bien por diversos usuarios a la vez o bien, generalmente, por medio del control de botnets.

DNS (DomainName Server): Servidor de Nombres de Dominio.

DNS spoofing: En el que lo que se modifica es el nombre de dominio-IP de un servidor DNS, aprovechando alguna vulnerabilidad.

eBay: Es el mayor centro de compra y venta en Internet: un lugar en el que se reúnen compradores y vendedores para intercambiar cualquier mercancía. El vendedor opta por aceptar sólo pujas por el artículo (un anuncio de subasta) u ofrecer la opción de precio fijo que permite a los compradores adquirir el artículo de inmediato.

Echelon: Sistema de vigilancia creado en los años setenta que controla las comunicaciones (correo electrónico, fax, comunicaciones vía satélite...) que tenía como fin la lucha contra el terrorismo internacional y el tráfico de drogas y que sirvió para el desarrollo de Internet.

Enfopol: Versión Europea de Echelon.

Facebook: Red social creada en 2004 por Mark Zuckerberg que cuenta en 2012 con más de un billón de usuarios.

Firewall: Cortafuegos.

Foro: Modalidad de sitio web o de parte del mismo en el que se permite y fomenta la discusión de un tema a distancia y de forma diferida en el tiempo.

***Game hackers*:** *Hackers* que en los años ochenta desarrollaron aplicaciones de *software* para juegos.

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

***Hacker*:** Experto informático (y apasionado por Internet y las nuevas tecnologías) que busca superar barreras por el mero hecho de su existencia sin entrar en el campo de lo delictivo, en ocasiones incluso usando sus conocimientos para la mejora de la seguridad de las redes y los sistemas (también denominados samuráis). También se utiliza el término para referirse al sujeto que accede de forma ilícita al sistema informático ajeno.

***Hackers* clandestinos:** Concepto casi idéntico al de *cracker* que englobaría los *hackers* que se dedican tanto a la intromisión informática, a la realización de ataques DoS, a la creación de webs para el fraude, al diseño de virus, a la infección de *bots,* al envío de *spam,* y todo ello con finalidad económica (generalmente) o bien política, y que actúan de forma individualizada o formando parte de un grupo que tanto puede ser una banda organizada tradicional que opera ahora en el ciberespacio, como una ciberbanda de *hackers* que unen sus esfuerzos para un fin criminal común.

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

***Hacking* blanco (*White hat hacking*):** Tipo de *hacking* consistente simplemente en acceder al sistema o a sus datos e información, pero sin ningún propósito de sabotaje o utilización posterior de la información.

***Hacking* negro (*Black hat hacking*):** *Hacking* realizado con ánimo destructivo o ilícito.

***Hacktivismo*:** Difusión de mensajes de protesta en Internet generalmente dirigidos contra organismos o Estados en relación con la voluntad de mantener libre de normas el ciberespacio

***Hardware*:** Conjunto de los componentes que integran la parte material de una computadora.

***Hardware hackers*:** En los setenta desarrollaron algunos de los equipos y tecnologías más importantes.

***Hosting*:** Servicio que consiste en proveer un espacio para alojar una página web.

Https: Protocolo creado por Netscape Communications Corporation para designar documentos que llegan desde un servidor web seguro. Esta seguridad es dada por el protocolo SSL (*Secure Socket Layer*).

***Identitytheft*:** Robo o fraude de identidad en el que se suplanta la personalidad de un usuario con ánimo defraudatorio.

***Information Warriors*:** Obtienen información y la transmiten al grupo organizado del que forman parte o bien la transmiten a otros a cambio de dinero; y también los meros ladrones, que utilizan burdos engaños o técnicas más sofisticadas para hacerse con la información bancaria que después les permite acceder al dinero por medio de la banca *online*.

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

***Insiders*:** Cibercriminal que pertenece o trabaja para la institución o empresa víctima de la infracción.

***IP spoofing*:** Mediante la utilización de programas específicamente destinados a ello, se sustituye la dirección IP original por otra.

Java: Lenguaje de programación que permite ejecutar programas escritos en un lenguaje muy parecido al C++. La ejecución del programa es completamente realizada en el equipo del cliente en lugar de en el servidor.

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

***Keystrokeloggers*:** Virus que capturan información de los sistemas informáticos.

***Mail spoofing*:** Suplantación de la dirección de correo electrónico de otras personas o entidades.

***Malware*:** *Software* malicioso destinado a dañar, controlar o modificar un sistema informático.

***Man-in-the-middle/phishing*:** Técnica de *phishing* en la que el atacante es capaz de controlar y registrar las transacciones e información sensible del usuario, interponiendo un *proxy* entre el cliente y el servidor web.

***Market-based cybercrimes*:** Cibercrímenes caracterizados por generar nuevos valores económicos más que por redistribuir los existentes, y que consisten en la realización de servicios que son actividades criminales, tales como la venta de *software* malicioso, la venta de drogas *online* o la venta de información referida a tarjetas de crédito.

***Meatspace*:** Término utilizado para referirse al espacio físico frente al ciberespacio.

Megaupload: Servicio dedicado al alojamiento de archivos y que era utilizado para la descarga directa de obras protegidas por parte de los usuarios. Fue cerrado por el FBI en 2012.

Messenger: Programa de mensajería instantánea.

MMS: Multimedia Messaging Service. Servicio de Mensajería multimedia.

MySpace3: Red social, que en 2012 contaba con más de 30 millones de visitantes.

Nativos digitales: Término acuñado para referirse a la generación nacida con la implantación total de Internet.

***Netiquette*:** Reglas del buen uso de Internet que servirán para que quien acceda a ese nuevo ámbito de comunicación social comprenda sus usos básicos, su funcionamiento aceptado por la sociedad que lo conforma.

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

***Online grooming*:** Acercamiento sexual a menores con el propósito de realizar posteriormente un contacto o abuso sexual.

***Online hate speech*:** Otro término para referirse a la difusión de mensajes de odio racial en el ciberespacio.

***Open source*:** Código libre. *Software* de distribución libre, de código abierto que puede ser modificado y estudiado.

***Packetsniffer*:** Sistema que captura todo el tráfico que viaja de una determinada forma o con unas determinadas características por la Red.

Parche: Modificación hecha a los archivos originales de un sistema operativo o de una aplicación de *software,* ya sean por el autor o por un tercero, para corregir, actualizar o mejorar el original.

PayPal: Servicio que permite enviar dinero por Internet a cualquier persona que disponga de un correo electrónico.

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

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

***Phishing* tradicional:** Tipo de *phishing* en el que se utiliza la imagen corporativa de una entidad bancaria o de una institución, para solicitar a la víctima por medio de correo electrónico que envíe a una dirección de correo que simula ser de tal entidad los datos bancarios requeridos.

***Phreakers*:** *Hackers* que manipulan las líneas telefónicas, para conseguir, entre otras cosas, el uso gratuito de las telecomunicaciones.

***Predatory cybercrimes*:** Aquellos actos ilegales en el ciberespacio en los que el cibercriminal intencionadamente daña la propiedad o la persona de alguien, entre los que incluye el robo de dinero de la cuenta bancaria o la infracción de la propiedad intelectual.

Protocolo FTP: Protocolo de transferencia de ficheros.

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

Protocolo IRC: Internet Relay Chat. Protocolo de comunicación en tiempo real.

Protocolo P2P: Peer-to-peer, protocolo que permite el intercambio directo de información, de igual a igual.

Protocolo TCP/IP: Protocolo de control de transmisión/Protocolo de Internet. Es el protocolo básico de comunicación en Internet.

Proxy: Es un servidor que sirve de intermediario entre un cliente y otro servidor.

Redes sociales: Web que permite la relación de personas en el ciberespacio.

***Rootkits*:** Virus que esconde el software malicioso o permite el control del sistema.

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

***Screenlogers*:** Programas diseñados para monitorizar las entradas en pantalla.

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

***Sessionhijackers*:** Secuestro de sesiones lo que permite el acceso a los archivos del equipo o a los servicios del sistema.

***Sexting*:** Tipo de *online grooming*. Consiste en la realización, por parte de menores, de fotografías propias de desnudos completos o de partes desnudas y su envío, generalmente por medio del teléfono móvil, a otros, junto con textos obscenos y con la finalidad de conocer personas o de enviar mensajes de amor o de odio.

***Skimming*:** Obtención de información relativa a tarjetas de crédito bien mediante engaño o gracias a la utilización de técnicas de clonado o de fotografía o de grabación de la actividad de una tarjeta de crédito con la

intención de usar tales datos para el posterior fraude; bien por medio de micro cámaras, de dispositivos incorporados a la ranura de los cajeros automáticos que clonan la banda magnética, o de engaños más burdos realizados en conjunción con camareros o vendedores cómplices que pasan la tarjeta al sujeto que las clona cuando el cliente no lo ve.

Skype: Programa que permite la comunicación de texto, audio y vídeo a través de Internet.

***Smartphones*:** Teléfono móvil diseñado para permitir al usuario la instalación de aplicaciones y el acceso a Internet.

SMS (Short Message): Service. Mensajes cortos de texto.

***Sniffer*:** Programas de captura de tramas de información que no están destinadas a él o persona que rastrea y captura información por la Red por medio de los denominados «*packet sniffers*».

***Snooping*:** Acceso no autorizado a datos de otros.

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

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

***Spammer*:** *Hacker* encargado de realizar envíos masivos de correo no deseado.

***Spear phishing*:** Modalidad de *phishing* que en lugar de dirigirse a objetivos indiscriminados busca clientes de entidades bancarias u otro tipo de organizaciones concretas.

***Spoofer*:** Persona que suplanta la identidad de otro usuario de la Red.

***Spoofing*:** Suplantación de identidad.

***Spyware*:** Virus que capturan información de los sistemas informáticos o software que se instala en un sistema informático y que recopila determinada información de éste que después envía a otro sistema.

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

***Streaming*:** Reproducción de audio y vídeo a través de la Red, puede ser en directo o en diferido.

TIC: Tecnologías de la Información y la Comunicación.

Top manta: Distribución física de copias ilegales.

Troyanos: Programas maliciosos que mediante ventanas emergentes recogen claves o utilizan cualquier otra técnica que permite perfeccionar el engaño haciendo creer a la víctima que está fuera de peligro.

***True hackers*:** Aficionados pioneros de la informática en los primeros días de la aparición de esta tecnología en los años sesenta.

Twitter: Red social que permite a sus usuarios a enviar y recibir mensajes de hasta 140 caracteres, conocidos como *tweets*. Fue creada en 2006 por Jack Dorsey que actualmente cuenta con más de 500 millones de usuarios.

URL (Uniform Resource Locator): Dirección única que identifica una página en Internet.

***Virucker*:** Término utilizado en castellano y dentro de la «jerga» de los propios *hackers* para referirse a aquellos que programan *malware* malicioso y realizan con él ataques a sistemas informáticos.

***Vishing*:** Práctica consistente en la utilización de mensajes de telefonía basada en voz sobre IP para conseguir de la víctima información personal, financiera o cualquier otro tipo de datos confidenciales.

VoIP (VoiceOver Internet Protocol): Significa «voz sobre un Protocolo de Internet».

Web 2.0: Término asociado a aplicaciones web centradas en el usuario, del tal modo que le permiten compartir información, interaccionar y colaborar con otros internautas creando una comunidad virtual, a diferencia de la web estática en la que los usuarios se limitan a ser receptores de los contenidos creados para ellos.

***Web spoofing*:** A través de un enlace u otras formas de engaño, se hace pasar una página web, imitada y albergada en otro servidor, por la real, por medio de un código que solicita la información requerida por el sistema víctima a cada servidor original y remite a la web falsa.

***Whaling*:** Modalidad de *fishing* en la que se ataca a los empleados de alto nivel de grandes empresas o gobiernos.

Whattsapp: Sistema de mensajería instantánea para los teléfonos móviles de última generación.

Wikileaks: Web creada en 2006 para la revelación de información secreta o confidencial de interés público.

***Wifi*:** Tecnología de comunicación inalámbrica.

XSS (*Cross-site scripting*): Técnica de *phishing* consistente en introducir código o URL falsas en una web real de este modo la mayor parte del contenido web es original, sin embargo una parte, la referida a la información sensible, está construida para obtener los datos objetivo sin que el usuario pueda detectar anomalías.

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

BIBLIOGRAFÍA

ACHAERANDIO, R., y MALDONADO, F., «Observatorio de piratería y hábitos de consumo de contenidos digitales», 2011.

ADLER, F.; MUELLER, G. O. W., y LAUFER, W. S., *Criminology and the Criminal Justice System*, New York, McGraw Hill, 2001 (4.ª ed.).

AGUIRRE ROMERO, J. M.ª, «Ciberespacio y comunicación: nuevas formas de vertebración social en el siglo XXI», en *EREL*, núm. 27, Universidad Complutense de Madrid, julio/octubre, 2004. En Internet en *http://www.ucm.es/info/especulo/numero27/cibercom.html* (última visita el 1 de octubre de 2010).

AGUSTINA SANLLEHÍ, J. R., «La arquitectura digital de Internet como factor criminógeno», en *IeJCS,* art. 4, núm. 3, 2009.

— «¿Menores infractores o víctimas de pornografía infantil? Respuestas legales e hipótesis criminológicas ante el Sexting», en *RECPC*, núm. 12-11, 2010.

— (dir.) *et al., La pornografía: Sus efectos sociales y criminógenos. Una aproximación multidisciplinar,* Montevideo-Buenos Aires-Madrid, BdeF-Edisofer, 2011.

AKDENIZ, Y., «Controlling illegal and harmful content on the Internet», en WALL, D. (ed.), *Crime and the Internet,* London, Routledge, 2001.

AKERS, R. L., y SELLERS, C. S., *Criminological theories. Introduction, evaluation, and application,* Los Angeles, Roxbury Publishing Company, 2004 (4.ª ed.).

ALCÁNTARA, J., *La neutralidad en la Red, y por qué es una mala idea acabar con ella*, Madrid, Biblioteca de Las Indias, 2011.

ALFONSO LASO, D., «El *hackering* blanco. Una conducta ¿punible o impune?», en *Internet y el Derecho penal,* Madrid, Consejo del Poder Judicial, 2002.

ALLEYNE, B., «Sociology of Hackers Revisited», en *TSR,* vol. 58, 2010.

ALSHALAN, A., *Cyber-Crime Fear and Victimization: An Analysis of a National Survey,* Mississippi, Mississippi State University, 2006.

ÁLVAREZ VIZCAYA, M., «Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la Red», en *CDJ,* Madrid, núm. 10, 2001.

ANDRÉS BLASCO, J., «¿Qué es Internet?», en GARCÍA MEXÍA, P. (dir.), *Principios de Derecho de Internet,* Valencia, Tirant lo Blanch, 2002.

ARIELY, G., «Knowledge Management, Terrorism, and Cyber Terrorism», en JANCZEWSKI, L. J., y COLARIK, A., *Cyber Warfare and Cyber Terrorism,* USA, Idea Group Inc (IGI), 2008.

ATHANASOPOULOS, E.; MAKRIDAKIS, A.; ANTONATOS, S.; ANTONIADES, D.; IOANNIDIS, S.; ANAGNOSTAKIS, K. G., y MARKATOS, E. P., «Antisocial Networks: Turning a Social Network into a Botnet», en *LNCS,* vol. 5222/2008, 2008.

AVILÉS MARTÍNEZ, J. M.ª, «Éxito escolar y ciberbullying», en *BP,* núm. 98, marzo 2010.

BABCHISHIN, K. M.; HANSON, R. K., y HERMANN, C. A., «The characteristics of online sex offenders: a meta-analysis», en *SA,* vol. 23, núm. 1, marzo 2011. En Internet

en *http://sax.sagepub.com/content/early/2010/07/23/1079063210370708* (última visita el 23 de diciembre de 2010).

BACK, L., «Aryans Reading Adorno: Cyber-culture and Twenty-first Century Racism», en *ERS,* vol. 25, núm. 4, 2002.

BAKER, W. *et al.,* «2010 Data Breach Investigations Report. A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service», 2010. En Internet en *http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf* (última visita el 29 de noviembre de 2010).

BALLARD, J. D.; HORNIK, J. G., y MCKENZIE, D., «Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues», en *ABS,* vol. 45, núm. 6, 2002.

BARBER, R., «Hackers Profiled-Who Are They and What Are Their Motivations?», en *CFS*, vol. 2001, núm. 2, febrero 2001.

BARLOW, J. P., «A Not Terribly Brief History of the Electronic Frontier Foundation», 1990. 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).

BARNES, G. C., «Defining and optimizing displacement», en *Criminal prevention,* 1995.

BASU, S., y JONES, R., «Regulating cyberstalking», en *JILT,* vol. 22, 2007.

BAUM, K.; CATALANO, S.; RAND, M., y ROSE, K., «Stalking Victimization in the United States», en *BJS,* U.S. Department of Justice, Office of Justice Programs January, 2009. En Internet en *http://bjs.ojp.usdoj.gov/content/pub/pdf/svus.pdf* (última visita el 18 de junio de 2012).

BEEBE, N. L., y RAO, S. V., «Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security», en *Proceedings of the 2005 Soft-Wars Conference,* Las Vegas, NV, Dec. 2005.

BELSEY, B., «Cyberbullying: An Emerging Threat to the "Always On" Generation», 2005. En Internet en *http://www.cyberbullying.ca/pdf/Cyberbullying_Article_by_Bill_Belsey.pdf* (última visita el 7 de octubre de 2011).

BENSON, M., y SIMPSON, S., *White collar crime: an opportunity prespective,* London, Routledge, 2009.

BIDE, M., «Does copyright have a future?: Can the lawlessness of the Internet be tamed?», en *BIR,* vol. 26, núm. 4, 2009.

BOCIJ, P., «Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet», en *FMPRJI,* vol. 8, núm. 10, 2003.

BOCIJ, P., y MCFARLANE, L., «Seven fallacies about cyberstalking», en *PSJ,* núm. 149, 2003.

BOSSLER A. M., y HOLT, T. J., «Online Activities, Guardianship, and Malware Infection», en *IJCC,* vol. 3, núm. 1, enero-junio 2009.

BOTTOMS, A. E., y WILES, P., «Environmental Criminology», en MAGUIRE, M.; MORGAN, R., y REINER, R., *The Oxford handbook of criminology*, New York, Oxford University Press, 1997 (2.ª ed.).

BOYD, D. M., y ELLISON, N. B., «Social network sites: Definition, history, and scholarship», en *JCMC*, vol. *13,* núm. 1, 2007.

BRANTHINGHAM, P. J., y BRANTHINGHAM, P., «The implications of the criminal event model for crime prevention», en MEIER, R. F.; KENNEDY, L. W., y SACCO, V. F. (eds.), *The Process and structure of Crime. Criminal events and Crime analysis,* en *ACT*, vol. 9, New Jersey, Transaction Publishers, 2001.

BRENNER, S. W., «Cybercrime Investigation and Prosecution: the Role of Penal and Procedural Law», en *MUEJL,* vol. 8, núm. 2, 2001.

— «Organized Cybercrime? How Cyberspace May Affect the Structure of criminal Relationships», en *NCJOLT*, vol. 4, núm. 1, 2002.

— «Cybercrime Metrics: Old Wine, New Bottles?», en *VJOLT*, vol. 9, núm. 13, 2004.
BRENNER, S. W., y CLARKE, L. L., «Distributed Security: preventing cybercrime», en *TJMJCIL,* vol. 23, núm. 4, Summer 2005.
BRENNER, S. W., y KOOPS, B. J., «Approaches to Cybercrime Jurisdiction», en *JHTL*, vol. 4, núm. 1, 2004.
BRIGGS, A., y BURKE, P., *De Gutenberg a Internet. Una historia social de los medios de comunicación* (traducido por M. A. GALMARINI), Madrid, Taurus, 2002.
BROWN, I., «The Law and Economics of Cybersecurity», en *LQR,* vol. 123, 2007.
BROWN, I., y KORFF, D., «Terrorism and the Proportionality of Internet Surveillance», en *EJC*, vol. 6, núm. 2, 2009.
BSA/IDC, *Estudio de piratería 09. Séptimo estudio global anual,* 2010. En Internet en *http://portal.bsa.org/globalpiracy2009/studies/globalpiracystudy2009_es.pdf* (última visita el 28 de diciembre de 2010).
CALMAESTRA VILLÉN, J., *Cyberbullying: prevalencia y características de un nuevo tipo de bullying indirecto.* Tesis doctoral, Córdoba, Servicio de Publicaciones de la Universidad de Córdoba, 2011.
CALTAGIRONE, S., *A Practical Ethical Assessment of Hacktivism.* En Internet en *http://www.classstudio.com/scaltagi/* (última visita el 26 de diciembre de 2010).
CALVETE, E.; ORUE, I.; ESTÉVEZ, A.; VILLARDÓN, L., y PADILLA P., «Cyberbullying in adolescents: Modalities and aggressors' profile», en *Computers in Human Behavior,* vol. 26, núm. 5, 2010.
CAMPBELL, A. M., «False Faces and Broken Lives: An Exploratory Study of the Interaction Behaviors Used by Male Sex Offenders in Relating to Victims», en *JLSP,* vol. 28, núm. 4, diciembre, 2009.
CAMPFIELD, D. C., «Cyberbullying and victimization: psychosocial characteristics of bullies, victims, and bully/victims», Montana, University of Montana, 2008. En Internet en *http://etd.lib.umt.edu/theses/available/etd-12112008-120806/unrestricted/umi-umt-1107.pdf* (última visita el 19 de junio de 2012).
CANO PAÑOS, M. Á., «Internet y terrorismo islamista: aspectos criminológicos y legales», en *Eguzkilore,* núm. 22, San Sebastián, diciembre, 2008.
CAPELLER, W., «Not such a neat net: some comments on virtual criminality», en *SLS,* núm. 10, 2001.
CARR, J., «Child abuse, child pornography and the Internet», en *NCH*, London, 2004.
CASTELLS, M., *La era de la información. Vol. 1. La sociedad red,* Madrid, Alianza Editorial, 2000 (2.ª ed.).
— *La era de la información. Vol. 3. Fin de milenio*, Madrid, Alianza Editorial, 2006.
— «Internet y la sociedad red», en *Conferencia de Presentación del Programa de Doctorado sobre la Sociedad de la Información y el Conocimiento. Universitat Oberta de Catalunya, 7.10.2000.* En Internet en *http://www.mvdenred.edu.uy/download/destacados/castells.pdf* (última visita el 2 de diciembre de 2010).
CILLI, C., «Identity Theft: A New Frontier for Hackers and Cybercrime», en *Information Systems Control Journal,* vol. 6, 2005.
CHACÓN MEDINA, A., «Una nueva cara de Internet: el acoso», en *Revista Eticanet,* núm. 1, Granada, julio, 2003.
CHATTERJEE, J., *The Changing Structure of Organized Crime Groups* (2005), Royal Canadian Mounted Police. En Internet en *http://dsp-psd.pwgsc.gc.ca/Collection/PS64-9-2005E.pdf* (última visita el 6 de diciembre de 2010).
CHAWKI, M., y ABDEL WAHAB, M., «Identity Theft in Cyberspace: Issues and Solutions», en *LE*, vol. 11, núm. 1, printemps/spring, 2006.

CHIESA, R.; DUCCI, S., y CIAPPI, S., «Profiling Hackers», en *The Science of Criminal Profiling as Applied to the World of Hacking,* Taylor & Francis Group, 2009.
CHIU, C.; KU, Y.; LIE, T., y CHEN, Y., «Internet Auction Fraud Detection Using Social Network Analysis and Classification Tree Approaches», en *IJEC*, vol. 15, núm. 3, 2011.
CHOI, K., «Computer Crime Victimization and Integrated Theory: An Empirical Assessment», en *IJCC,* vol. 2, enero-junio, 2008.
CHOO, K. K. R., «Zombies and Botnets», en *TICCJ,* núm. 233, Canberra, 2007.
— «Organised crime groups in cyberspace: a typology», en *TOC,* 2008, núm. 11.
CHUA, C. E. H., y WAREHAM, J., «Fighting Internet Auction Fraud: An Assessment and Proposal Computer», en *IEEE Computer*, núm. 10, 2004.
CLABURN, T., «Microsoft Finds U.S. Leads in Botnets», en *Information Week,* Oct. 14, 2010. En Internet en *http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=227800051&c id=nl_IW_daily_2010-10-15_html* (última visita el 19 de junio de 2012).
CLARKE, R. V. (ed.), *Situational crime prevention. Successful Case Studies,* New York, Harrow and Heston Publishers, Guilderland, 1997 (2.ª ed.).
— «Introduction», en CLARKE, R. V. (ed.), *Situational crime prevention. Successful Case Studies,* New York, Harrow and Heston Publishers, Guilderland, 1997 (2.ª ed.).
— «Hot products: understanding, anticipating and reducing demand for stolen goods», Paper núm. 112, en *PRS*, London, British home Office Research Publications, 1999.
CLARKE, R., y FELSON, M. (eds.), «Routine activity and rational choice», en *ACT,* vol. 5, New Jersey, Transaction Publishers, New Brunswick, 1993.
CLARKE, R. V., y FELSON, M., «Introduction: Criminology, routine activity, and rational choice», en CLARKE, R. V., y FELSON, M. (eds.), *Advances and criminological theory,* 5. Routine activity and rational choice, New Brunswick, NJ: Transaction Books, 1993.
CLARKE, R. V., y WEISBURD, D., «Diffusion of crime control benefits: observations on the reverse of displacement», en *CPS,* vol. 2, 1994.
CLOUGH, J*., Principles of Cybercrime,* Cambridge, Cambridge University Press, 2010.
COHEN, L. E., y FELSON, M., «Social change and crime rate trends: a routine activity approach», en *ASR,* vol. 44, agosto 1979.
COLARIK, A. M., y JANCZEWSKI, L. J., «Introduction to Cyber Warfare and Cyber Terrorism», en JANCZEWSKI, L. J., y COLARIK, A. M. (eds.), *Cyber Warfare and Cyber Terrorism*, Hershey-London, IGI Global, 2008.
COLEMAN, G., y GOLUB, A., «Hacker practice: Moral genres and the cultural articulation of liberalism», en *AT,* núm. 8, septiembre, 2008.
CONWAY, M., «Cyberterrorism: Media Myth or Clear and Present Danger?» en IRWIN, J. (ed.), *War and virtual war: the challenges to communities*, 2004.
CORNISH, D. V., y CLARKE, R. V., «Opportunities, precipitator and criminal decisions: A reply to Wortley's critique of situational crime prevention», en SMITH, M., y CORNISH, D. B. (coords.), *Theory for Practice in Situational Crime Prevention,* en *CPS,* vol. 16, New York, Monsey, Criminal Justice Press, 2003.
— *The reasoning Criminal, Rational choice perspectives on offending,* New York, Springer, 1986.
COVA, M.; KRUEGEL, C., y VIGNA, G., *There is no free phish: An analysis of free and live phishing kits,* Proceedings of the Second USENIX Workshop on Offensive Technologies, 2008.
CURRAN, K.; CONCANNON, K., y MCKEEVER, S., «Cyber terrorism attacks», en JANCZEWSKI, L. J. y COLARIK, A. M. (eds.), *Cyber Warfare and Cyber Terrorism*, Hershey-London, IGI Global, 2008.

DANIELS, J., «Cloaked websites: propaganda, cyber-racism and epistemology in the digital era», en *NMS,* vol. 11, núm. 5, 2009.
— *Cyber racism: white supremacy online and the new attack on civil rights,* Lanham, Rowman & Littlefield Publishers, INC, 2009.
DAVIES, R., y PEASE, K., «Crime, technology and the future», en *SJ*, núm. 13, abril 2000.
DAVIDSON, D., *Essays on actions and events,* Oxford, Clarendon Press, 1980.
DEFENSOR DEL PUEBLO-UNICEF, *Violencia escolar: el maltrato entre iguales en la educación secundaria obligatoria. 1999-2006,* Madrid, Publicaciones de la Oficina del Defensor del Pueblo, 2007.
DE LA CORTE IBÁÑEZ, L., y GIMÉNEZ-SALINAS FRAMIS, A., *Crimen.org. Evolución y claves de la delincuencia organizada,* Barcelona, Ariel, 2010.
DE LA CUESTA ARZAMENDI, J. L. (dir.), *Derecho penal informático,* Cizur Menor, Civitas, 2010.
DE LA CUESTA ARZAMENDI, J. L., y PÉREZ MACHÍO, A. I., «Ciberdelincuentes y cibervíctimas», en DE LA CUESTA ARZAMENDI, J. L. (dir.), *Derecho penal informático,* Cizur Menor, Civitas, 2010.
DE LA CUESTA ARZAMENDI, J. L., y SAN JUAN GUILLEM, C., «La cibercriminalidad: interés y necesidad de estudio. Percepción de seguridad e inseguridad», en DE LA CUESTA ARZAMENDI, J. L. (dir.), *Derecho penal informático,* Cizur Menor, Civitas, 2010.
DE LA MATA BARRANCO, N. J., «Ilícitos vinculados al ámbito informático: la respuesta penal», en DE LA CUESTA ARZAMENDI, J. L. (dir.), *Derecho penal informático,* Cizur Menor, Civitas, 2010.
DONG, X.; CLARK, J. A., y JACOB, J. L., «Defending the weakest link: phishing websites detection by analysing user behaviors», en *Telecommun Syst,* núm. 45, 2010.
DUNN CAVELTY, M., «Cyber-Terror- Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate», en *Journal of Information Technology & Politics,* vol. 4, núm. 1, 2007.
DURKIN, K. F., «Misuse of the Internet by Pedophiles: Implications for Law Enforcement and Probation Practice», en *FP,* vol. 61, 1997.
EKBLOM, P., «Getting the best out of crime analysis», en *Crime Prevention Unit Paper* 10, London, Home Office, 1988.
ELLIOTT, I. A.; BEECH, A. R.; MANDEVILLE-NORDEN, R., y HAYES, E., «Psychological profiles of Internet sexual offenders: comparisons with contact sexual offenders», en *SA,* vol. 21, núm. 1, 2009. En Internet en *http://sax.sagepub.com/content/21/1/76* (última visita el 23 de diciembre de 2010).
EMIGH, A., *Online Identity Theft: Phishing Technology, Clokepoints and Countermeasures. ITTC Report on Online Identity Theft Technology and Countermeasures*, 2005.
FAFINSKI, S., y MINASSIAN, N., *UK Cybercrime report 2009*, Invenio Research September 2009.
FARRELL, G., y PEASE, K., «Criminology and Security», en GILL, M. (ed.), *The Handbook of Security,* Perpetuity Press, 2005.
FELSON, M., «Linking criminal choices, routine activities, informal control and criminal outcomes», en CORNISH, D. B., y CLARKE, R. V. (eds.), *The reasoning Criminal, Rational choice perspectives on offending*, New York, Springer-Verlag, 1986.
— «Technology, Business and Crime», en FELSON, M., y CLARKE, R. V. (ed.), *Business and Crime Prevention,* New York, 1997.
— *Crime and everyday life,* Thousand Oaks, CA: Pine Forge Press, 1998 (2.ª ed.).

FELSON, M., y CLARKE, R. V., «Routine precautions, criminology and crime prevention», en BARLOW, H. D. (ed.), *Crime and public policy: putting theory to work,* Boulder, CO, Westview Press, 1995.

FELSON, M., y BOBA, R., *Crime and everiday life,* Sage, Thousand Oaks, CA, 2009 (4.ª ed.).

FELTEN, E. W.; BALFANZ, D.; DEAN, D., y WALLACHD, S., «Web Spoofing: An Internet Con Game», en *Technical Report,* 540-96, New Jersey, Department of Computer Science, Princeton University, 1996.

FERNÁNDEZ PALMA, R., y MORALES GARCÍA, Ó., «El delito de daños informáticos y el caso Hispahack», en *LL,* núm. 1, 2000.

FERNÁNDEZ TERUELO, J. G., «Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de red», en *RDPC*, núm. 19, 2007.

FIELDING, A., «Cyber Space, Meat Space and a Sense of Place: Lessons from the interplay of the online and offline worlds». En Internet en *http://www.walk21.com/papers/Andrew%20Fielding_Cyber%20Space,%20Meat%20Space%20and%20a%20Sense%20of%20Place.pdf* (última visita el 19 de junio de 2012).

FITRI, N., «Democracy Discourses through the Internet Communication: Understanding the Hacktivism for the Global Changing», en *OJCMT,* vol. 1, núm. 2, abril 2011.

FLEMING, M.; GREENTREE, S.; COCOTTI-MULLER, D.; ELIAS, K., y MORRISON, S., «Safety in cyberspace: Adolescents' safety and exposure online», en *YS*, 38, 2006.

FRASER, C.; OLSEN, E.; LEE, K.; SOUTHWORTH, S., y TUCKER, S., «The new age of stalking: technological implications for stalking», en *JFCJ,* vol. 61, núm. 4, 2010.

FUCHS, C., «Transnational Space and the "Network Society"», en *Paper Presented at the Association of Internet Researchers (AoIR) Conference: Internet Research 7.0, Brisbane, September 27-30*, 2006.

FURNELL, S., «Cybercrime: vandalizing the information society», en *LNCS,* vol. 2722, 2003.

GALÁN MUÑOZ, A., «Expansión e intensificación del Derecho penal de las nuevas tecnologías: un análisis crítico de las últimas reformas legislativas en materia de criminalidad informática», en *RDPP,* núm. 15, 2006.

GARAIGORDOBIL, M., «Prevalencia y consecuencias del cyberbullying: una revisión», *IJPPT*, vol. 11, núm. 2, 2011.

GARLAND, D., «Ideas, Institutions and Situational Crime Prevention», en VON HIRSCH, A.; GARLAND, D., y WAKEFIELD, A., *Ethical and Social Perspectives on Situational Crime Prevention,* Hart Publishing, Oxford-Portland, 2000.

GARLAND, D., «The new criminologies of Everyday life: Routine Activity Theory in Historical and social context», en VON HIRSCH, A.; GARLAND, D., y WAKEFIELD, A., *Ethical and Social Perspectives on Situational Crime Prevention,* Oxford-Portland, Hart Publishing, 2000.

— *The Culture of Control. Crime and Social order in contemporary society,* New York, Oxford University Press, 2001.

GARRIDO, V., y SANCHÍS, J., *Delincuencia de «cuello blanco»,* Editorial Instituto de Estudios de Policía, Colección «Politeia», núm. 1, 1987.

GARRIDO V.; STANGELAND, P., y REDONDO, S., *Principios de Criminología,* Valencia, Tirant lo Blanch, 2006 (3.ª ed.).

GHOSH, S., y TURRINI, E. (eds.), *Cybercrimes: A Multidisciplinary Analysis*, Berlin-Heidelberg, Springer-Verlag, 2010.

GIBSON, W., *Neuromancer,* New York, Ace Books, 1984.

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).

GONZÁLEZ RUS, J. J., «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», en *RFDUCM,* núm. 12, 1986.

— «Tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», en *PJ, Número especial IX,* 1989.

GOODMAN, M. D., y BRENNER, S. W., «The emerging consensus on criminal conduct in cyberspace», en *IJLIT*, vol. 10, núm. 2, Oxford University Press, 2002.

GORDON, S., y CHESS, D. M., *Where There's Smoke, There's Mirrors: The Truth about Trojan Horses on the Internet,* München, Germany, Virus Bulletin Conference, 1998.

GOTVED, S., «Time and space in cyber social reality», en *NMS*, vol. 8, núm. 3, 2006.

GRABOSKY, P., «Computer crime: a criminological overview», en *Presentation at the Workshop on Crimes Related to the Computer Network, Tenth United Nations Congress on the Treatment of Offenders,* Vienna, 15 de abril de 2000.

— «Virtual Criminality: Old Wine in New Bottles?», en *SLS,* núm. 10, 2001.

— «The Internet, Technology, and Organised Crime», en *AJC*, vol. 2, núm. 2, 2007.

GRABOSKY, P., y SMITH, R., «Telecommunication fraud in the digital age: the convergence of technologies», en WALL, E. (ed.), *Crime and the internet*, London, Routledge, 2001.

GRAHAM, P. W., «Space and Cyberspace: on the enclosure of consciousness», en ARMITAGE, J., y ROBERTS, J. (eds.), *Living with cyberspace: technology & society in the 21st century,* London, Continuum International Publishing Group, 2002.

GRAHAM, S., «The end of geography or the explosion of place? Conceptualizing space, place and information technology», en *PHG,* vol. 22, núm. 2, 1998.

GREEN, J., «The myth of ciberterrorism», en *WM,* noviembre, 2002.

GREEN, N., «On the Move: technology, mobility, and the mediation of social time and space», en *IS*, vol. 18, núm. 4, 2002.

GUINCHARD, A., «Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy», en *JSC,* vol. 4, núm. 2, 2011.

GUTIÉRREZ PUEBLA, J., «Redes, espacio y tiempo», en *AGUC,* núm. 18, 1998.

HENSON, B., «Cyberstalking», en FISHER, B. S., y LAB, S. P. (eds.), *Encyclopedia of Victimology and Crime Prevention*, Thousand Oaks, CA, Sage, 2010.

HERNÁNDEZ PRADOS, M. A., y SOLANO FERNÁNDEZ, I. M., «Ciberbullying, un problema de acoso escolar», en *RIED*, vol. 10, 2007.

HERRERA MORENO, M., «El fraude informático en Derecho penal español», en *Actualidad Penal,* núm. 39, 2001.

HERRERO, C., «Capítulo 33: Los delitos socioeconómicos», en HERRERO, C., *Criminología (Parte General y Especial),* Madrid, Dykinson, 1997.

HEUSTON, G. Z., «Investigating the Information Superhighway: Global Views, local perspectives», en *JCJE*, vol. 2, núm. 6, 1995.

HIGGINS, G. E., y MAKIN, D. A., «Does Social Learning Theory Condition the Effects of Low Self-Control on College Students' Software Piracy?», en *IJCC,* primavera, vol. 2, 2004.

HIGGINS, G. E.; FELL, B. D., y WILSON, A. L., «Low Self-Control and Social Learning in Understanding Students' Intentions to Pirate Movies in the United States», en *SSCR,* núm. 25, 2007.

HIMANEN, P., *La ética del hacker y el espíritu de la era de la información,* Barcelona, Destino, 2004.

HINDELANG, M. J.; GOTTFREDSON, M. R., y GAROFALO, J., *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*, Cambridge, MA, Balliger Publishing Company, 1978.

HINDUJA, S., «Correlates of Internet *software* piracy», en *JCCJ,* vol. 17, núm. 4, noviembre, 2001.

HINDUJA, S., y PATCHIN J., «Personal Information of Adolescentsonthe Internet: A Quantitative Content Analysis of MySpace», en *JA,* 31(1), 2008.

HOLT, T. J., y BOSSLER, A. M., «Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization», en *DB*, vol. 30, núm. 1, enero 2009.

HOLT, T. J., y BOSSLER, A. M., «On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory», en *IJCC,* vol. 3, núm. 1, enero-junio 2009.

HONG, J., «The State of Phishing Attacks», en *Communications of the ACM,* vol. 55, núm. 1, 2012.

HUGHES, L. A., y DELONE, G. J., «Viruses, worms, and Trojan horses: serious crimes, nuisance, or both?», en *SSCR,* vol. 25, núm. 1, 2007.

HUMBACH, J. A., «"Sexting" and the First Amendment», en *HCLQ*, vol. 37, 2010.

HUTCHINGS, A., y HAYES, H., «Routine Activity Theory and Phishing Victimisation: Who Gets Caught in the "Net"?», en *CICJ*, vol. 20, núm. 3, marzo 2009.

INTECO, ORANGE, «Estudio sobre seguridad y privacidad en el uso de los servicios móviles por los menores españoles», 2010. Disponible en Internet en *http://www.inteco.es/Seguridad/Observatorio/Estudios/Estudio_moviles_menores*.

INTECO Y PANTALLAS AMIGAS, «Guía sobre adolescencia y *sexting:* qué es y cómo prevenirlo», febrero de 2011. Disponible en Internet en *http://www.inteco.es/Seguridad/Observatorio/guias/Guia_sexting.*

INTERPOL SPECIALIST GROUP ON CRIMES AGAINST CHILDREN, *http://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children* (última visita el 11 de junio de 2012).

ISLA CORTES, J. I. M., «Seguridad en redes informáticas». En Internet en *http://cybertesis.uach.cl/tesis/uach/2005/bmfcii.82s/doc/bmfcii.82s.pdf* (última visita el 30 de noviembre de 2010).

IZENBERG, N., y LIEBERMAN, D., «The web, communication trends, and children's health: How the children use the web», en *ClP,* 1998.

JAGATIC, T.; JOHNSON, N.; JAKOBSSON, M., y MENCZER, F., «Social Phishing», en *Communications of the ACM*, Bloomington, diciembre, 2005.

JAISHANKAR, K., «Identity related Crime in the Cyberspace: Examining Phishing and its impact», en *IJCC*, vol. 2, enero-junio, 2008.

— «Sexting: A new form of Victimless Crime?», en *IJCC*, vol. 3, enero-junio 2009.

JAKOBSSON, M., *Phishing and Countermesasures: Understanding the Increasing Problem of Electronic Identity Theft,* John Willey & Sons, 2005.

JANCZEWSKI, L. J., y COLARIK, A. M. (eds.), *Cyber Warfare and Cyber Terrorism*, Hershey-London, IGI Global, 2008.

JEN, W.; CHANG W., y CHOU S., *Cybercrime in Taiwan: an analysis of suspect records*. Paper to Workshop on Intelligence and Security, 2006.

JENIK, A., «Cyberwar in Estonia and the Middle East», en *NS*, vol. 2009, núm. 4, abril, 2009, pp. 4 y ss.

JEWKES, Y., «Cybercrime», en MCLAUGHLIN, E. U., y MUNCIE, J. (eds.), *The Sage Dictionary of Criminology,* London-California, Sage, 2006.

— *Crime Online, Willan Publishing,* Portland, 2007.

JONES, B. R., «Comment: Virtual neighborhood watch: open source *software* and community», en *JCLC,* 97, 2; Research Library, Winter 2007.

KEATS CITRON, D., y NORTON, H. L., «Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age», en *Boston University Law Review,* vol. 91, 2011.

KENNEDY, L. W., y GIBBS VAN BRUSCHOT, E., «Routines and the criminal event», en MEIER, R. F.; KENNEDY, L. W., y SACCO, V. F. (eds.), *The Process and structure of Crime. Criminal events and Crime analysis,* en *ACT*, vol. 9, New Jersey, Transaction Publishers, 2001.

KITCHIN, R. M., «Towards geographies of cyberspace», en *PHG,* vol. 22, núm. 3, 1998.

KNAPP, K. J., y BOULTON, W. R., «Ten Information Warfare Trends», en JANCZEWSKI, L. J., y COLARIK, A. M. (eds.), *Cyberwarfare and cyber terrorism,* Information Science Reference, 2008.

KOHLMANN, E. F., «"Homegrown" Terrorists: Theory and Cases in the War on Terror's Newest Front», en *ANNALS,* núm. 618, julio de 2008.

KONTOSTATHIS, A.; EDWARDS, L., y LEATHERMAN, A., «Text Mining and Cybercrime», en VVAA., *Text Mining: Applications and Theory,* John Willey and Sons, 2010.

KORGAONKAR, P., y WOLIN, L. D., «Web usage, advertising, and shopping: relationship patterns», en *IR,* vol. 12, núm. 2, 2002.

KOWALSKI, R. M., y LIMBER, S. P., «Electronic bullying among middle school students», en *JAH,* 2001.

KSHETRI, N., «The Simple Economics of Cybercrimes», en *IEEE Security and Privacy. The IEEE Computer Society,* vol. 4, núm. 1, 2006.

— *The Global Cybercrime Industry. Economic, Institutional and Strategic Perspectives,* Heidelberg, Springer Verlag, 2010.

LANNING, K. V., «Law enforcement perspective on the compliant child victim», en *APSACA,* vol. 14, núm. 2, 2002.

LEARY, M. G., «Self-Produced Child Pornography: The Appropriate Societal Response to Juvenile Self-Sexual Exploitation», en *VJSPL*, vol. 15, núm. 1, 2008.

— «Sexting or Self-Produced Child Pornography? The Dialogue Continues-Structured Prosecutorial Discretion within a Multidisciplinary Response», en *VJSPL*, 2010.

LEE, M. J., «Computer Viruses, Computer Hackers: Security Threats of the 1990's», en *National Criminal Justice Reference Service,* 1991.

LEE, H., y LIEBENAU, J., «Time and the Internet at the turn of the millenium», en *TSoc.,* vol. 9, núm. 1, 2000.

LENHART, A., «Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging» (2009), en *PIALP*, Washington D. C.. En Internet en *http://www.pewinternet.org/Reports/2009/Teens-and-Sexting.aspx* (última visita el 9 de septiembre de 2010).

LENHART, A., y MADDEN, M., *Teens, privacy and online social networks: How teens manage their online identities and personal information in the age of MySpace* (2007). En Internet en *http://pewresearch.org/pubs/454/teens-privacy--online-social-networks* (última visita el 10 de septiembre de 2010).

LENHART, A.; ARAFEH, S.; MACGILL, S. A., y RANKIN, A., «Writing, Technology and Teens», *Pew Internet and American Life Project,* 2008. En Internet en *http://www.pewinternet.org/Reports/2008/Writing-Technology-and-Teens.aspx?r=1* (última visita el 9 de septiembre de 2010).

LEVIN, B., «Cyberhate: a legal and historical analysis of extremists' use of computer networks in America», en *ABS,* núm. 45, 2002.

LEVY, S., *Hackers. Heroes of the computer revolution*, Sebastopol, California, O'Reilly Media, 2010.

LI, Q., «Bullying in the new playground: Research into cyberbullying and cybervictimization», en *Australasian Journal of Educational Technology,* 2007.

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

LONGE, O. B.; MBARIKA, V.; KOUROUMA, M.; WADA, F., e ISABALIJA, R., «Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities», en *IJCSIS,* vol. 6, núm. 3, 2009.

LWIN, M.; STANALAND, A., y MIYAZAKI, A., «Protecting children's privacy online: how parental mediation strategies affect website safeguard effectiveness», en *Journal of Retailing,* 2008.

MACIÁ FERNÁNDEZ, G., *Ataques de denegación de servicios a baja tasa contra servidores*, tesis doctoral presentada para el Doctorado en la Universidad de Granada, mayo, 2007.

MAGID, L., «What Can Parents Do about Web Safety? Talking to Teens and Tweens, Says Larry Magid, Can Help a Lot», en *CBS Interactive Inc.,* 2006, URL, *http://www.cbsnews.com/stories/2006/11/13/scitech/pcanswer/main2174962.shtml.*

MAHOONEY, K., «Hate speech, equality, and the state of canadian law», en *WFLR,* vol. 44, 2009.

MANAFY, M., y GAUTSCHI, H., *Dancing with digital natives: Staying in step with the generation that's transforming the way business is done,* New Jersey, Cyberage Books, Medford, 2011.

MANIYARA, M., Post del blog Security Response de Symantec (3 de febrero de 2010). En Internet en *http://www.symantec.com/connect/blogs/phishing-using-pornographic-content-bait* (última visita el 1 de diciembre de 2010).

MARCHENA GÓMEZ, M., «El sabotaje informático: entre los delitos de daños y desórdenes públicos», en *CDJ,* núm. 10, Madrid, 2001.

MARCO MARCO, J. J., «Menores, ciberacoso y derechos de la personalidad», en GARCÍA GONZÁLEZ, J. (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet,* Valencia, Tirant lo Blanch, 2010.

MARCUM, C. D., «Adolescent online victimization and Constructs of Routine Activities theory», en JAISHANKAR, K. (ed.), *Cyber Criminology. Exploring Internet crimes and criminal behavior*, Boca Ratón, CRC Press, 2011.

MARCUM, C. D.; RICKETTS, M. L., y HIGGINS, G. E., «Assessing sex experiences of online victimization: an examination of adolescent online behaviors using routine activity theory», en *CJR,* 2010.

MARTÍN LORENZO, M., y RAGUÉS I VALLÉS, R., «Libertad e indemnidad sexuales», en ORTIZ DE URBINA GIMENO, Í. (dir.), *Memento experto reforma penal 2010. Ley Orgánica 5/2010,* Madrid, Ediciones Francis Lefebvre, 2010.

MASON, K. L., «Cyberbullying: A Preliminary Assessment for School Personnel», en *Psychology in the Schools*, 45 (4), 2008.

MATA Y MARTÍN, R. M., *Delincuencia informática y Derecho penal,* Madrid, Edisofer, 2001.

MATTELART, T., «Audio-visual piracy: towards a study of the underground networks of cultural globalization», en *GMC,* vol. 5, núm. 3, 2009.

MAYHEW, P.; CLARKE, R.; STURMAN, A., y HOUGH, M., *Crime as opportunity,* London, Home Office Research Study 34, 1976.

MAZUR, E., «Teen blogs as mines of adolescent data», en *TP,* 32, 2005.

MCALINDEN, A. M., «Setting "Em Up": Personal, Familial and Institutional Grooming in the sexual Abuse of Children», en *SLS,* vol. 15, núm. 3, 2006.

MCCONNELL INTERNATIONAL, «Cyber Crime... and Punishment? Archaic Laws Threaten Global Information». En Internet en *http://www.witsa.org/papers/McConnell-cybercrime.pdf* (última visita el 9 de septiembre de 2010).

MCCUSKER, R., «Transnational organised cybercrime: distinguishing threat from reality», en *CLSC,* 46 (4-5), 2006.

MCFARLANE, L., y BOCIJ, P., «An Exploration of Predatory Behaviour in Cyberspace: Towards a Typology of Cyberstalkers», en *First Monday*, vol. 8, núm. 9, 2003.

MCLAUGHLIN, J. H., «Crime and Punishment: Teen Sexting in Context», Express, 2010. Disponible en Internet en *http://works.bepress.com/julia_mclaughlin/1.*

MCQUADE III, S. C., «Cybercrime», en TONRY, M. (ed.): *The Oxford Handbook of Crime and public policy,* New York, Oxford University Press, 2009.

MEDINA ARIZA, J. J., «El control social del delito a través de la prevención situacional», en *RDPC*, 2.ª época, núm. 2, 1998.

MEIER, R. F.; KENNEDY, L. W., y SACCO, V. F., «Crime and the criminal event perspective», en MEIER, R. F.; KENNEDY, L. W., y SACCO, V. F. (eds.), *The Process and structure of Crime. Criminal events and Crime analysis,* en *ACT*, vol. 9, New Jersey, Transaction Publishers, 2001.

MESTRE DELGADO, E., «Tiempos de cibercrimen», en *LL,* núm. 37, año IV, abril 2007.

MIRÓ LLINARES, F., *Internet y delitos contra la propiedad intelectual*, Madrid, Iberautor Promociones Culturales, 2005.

— «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen», en *RECPC,* núm. 13-07, 2011.

— «Cibercrímenes económicos y patrimoniales» en ORTIZ DE URBINA GIMENO, I. (dir.), *Memento práctico penal y económico de la empresa 2011-2012,* Madrid, Francis Lefebvre, 2011.

MITCHELL, K. J.; FINKELHOR, D., y WOLAK, J., «Youth internet users at risk for the most serious online sexual solicitations», en *AJPM*, vol. 32, núm. 6, 2007.

MÖHRENSCHLAGER, M. E., «El nuevo Derecho penal informático en Alemania» (traducido por J.-M.ª Silva Sánchez), en MIR PUIG, S. (comp.), *Delincuencia informática,* Barcelona, PPU, 1992.

MOORE, D.; VOELKER, G. M., y SAVAGE, S., «Inferring Internet Denial-of-Service Activity», en *ACM,* vol. 24, núm. 2, 2006.

MORA-MERCHÁN, J. A., y JÄGER, T. (eds.), *Cyberbullying. A Cross-national comparison,* Landau, Verlag Empirische Pädagogik, 2010.

MORALES GARCÍA, Ó., «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la convención del Consejo de Europa sobre Cyber-crime», en *CDJ,* núm. 9, 2002.

MORALES PRATS, F., «Los ilícitos en la Red (II): Pornografía infantil y ciberterrorismo», en ROMEO CASABONA, C. M. (coord.), *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Granada, Comares, 2006.

— «Pornografía Infantil e Internet: la respuesta en el Código Penal español», en MARTÍN-CASALLO LÓPEZ (dir.), *Problemática Jurídica en torno a fenómenos de Internet*, Madrid, Escuela Judicial Consejo General del Poder Judicial, 2000.

MORALES PRATS, F., y GARCÍA ALBERO, R., «Artículo 189», en QUINTERO OLIVARES, *Comentarios al nuevo Código Penal,* Navarra, 2004.

MORILLAS FERNÁNDEZ, D. L., *Análisis dogmático y criminológico de los delitos de pornografía infantil. Especial consideración de las modalidades comisivas relacionadas con Internet*, Colección Monografías de Derecho Penal, 4, Madrid, Dykinson, 2005.

MORÓN LERMA, E., *Internet y Derecho penal: Hacking y otras conductas ilícitas en la Red,* Cizur Menor, Aranzadi, 2002 (2.ª ed.).
— «Derecho penal y nuevas tecnologías. Panorama actual y perspectivas futuras», en CASANOVAS, P. (ed.), *Internet y pluralismo jurídico: formas emergentes de regulación,* Granada, Comares, 2003.
MORRIS, R. G., y HIGGINS, G. E., «Neutralizing Potential and Self-Reported Digital Piracy», en *CJR*, vol. 34, núm. 2, 2009.
MYERS, S., «Introduction to Phishing» en JAKOBSSON, M., y MYERS, S., *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft,* Hoboken, NJ, John Wiley and Sons, 2006.
NAYAR, P. K., «WikiLeaks, the New Information Cultures and Digital Parrhesia», en *Economic & Political Weekly,* núm. 52, diciembre, 2010.
NEGROPONTE, N., *El mundo digital* (traducido por M. ABDALA), Barcelona, Ediciones B, 1995.
NELKEN, D., «White-Collar crime», en MAGUIRE, M.; MORGAN, R., y REINER, R., *The Oxford handbook of criminology,* New York, Oxford University Press, 1997 (2.ª ed.).
NGO, F., y PATERNOSTER, R., «Cybercrime Victimization: An examination of Individual and Situational level factors», en *IJCC*, vol. 5, núm. 1, 2011.
NISBETT, C., «New directions on Cybercrime», White Paper, Qinetiq. En Internet en *http://apps.qinetiq.com/perspectives/pdf/EP_White_Paper3_Cyber%20Crime.pdf.*
NISSENBAUM, H., «Hackers and the contested ontology of cyberspace», en *NMS,* núm. 6, 2004.
OECD, *Malicious Software (Malware): A Security Threat to the Internet Economy*, OECD, junio, 2008.
OLLMANN, G., «The evolution of commercial malware development kits and colour-by-numbers custon malware», en *Computer Fraud and Security*, núm. 9, 2008.
— *The Phishing Guide: Understanding and Preventing Phishing Attacks. Informe Técnico,* NGSS, 2009.
OPHARDT, J. A., «Cyber warfare and the crime of aggression: the need for individual accountability on tomorrow's battlefield», en *DLTR,* núm. 3, 2010.
ORTEGA, R.; CALMAESTRA, J., y MORA-MERCHÁN, J., «Cyberbullying», *International Journal of Psychology and Psychological Therapy*, 8 (2), 2008. En Internet en *http://redalyc.uaemex.mx/redalyc/pdf/560/56080204.pdf*.
OST, S., *Child Pornography and Sexual Grooming. Legal and Societal Responses,* Cambridge, Cambridge University Press, 2009.
PARDO ALBIACH, J., «Ciberacoso: Cyberbullyng, grooming, redes sociales y otros peligros», en GARCÍA GONZÁLEZ, J. (coord.), *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet,* Valencia, Tirant lo Blanch, 2010.
PAREKH, B., «Hate speech: Is there a case for banning», en *PPR,* vol. 12, núm. 4, 2006.
PARKER, D. B., *Crime by Computer*, New York, Charles Scribner's Sons, 1976.
— *Fighting Computer Crime,* New York, Charles Scribner's Sons, 1983.
— *Fighting Computer Crime: A new Framework for Protecting Information,* New York, Wiley, 1998.
PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA, «*Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime*». *The Report of the Inquiry into Cyber Crime,* Canberra, junio 2010.
PATCHIN, J. W., e HINDUJA, S., «Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying», en *YVJJ,* vol. 4, 2006.
— «Trends in online social networking: adolescent use of MySpace over time», en *NMS*, enero, 2010.

PATHÉ, M., y MULLEN, P. E., «The impact of stalkers on their victims», en *BJP*, 1997.
PEASE, K., «Crime futures and foresight: Challenging criminal behaviour in the information age», en WALL, D. (ed.), *Crime and the Internet*, London, Routledge, 2001.
— «Science in the service of crime reduction», en TILLEY, N. (ed.), *Handbook of crime prevention and community safety,* UK, Willan Publishing, 2005.
— «Crime Prevention», en MAGUIRE, M.; MORGAN, R., y REINER, R., *The Oxford handbook of criminology*, New York, Oxford University Press, 1997 (2.ª ed.).
PELLEGRINI, A., y BARTINI, M., «A longitudinal study of bullying, victimization, and peer affiliation during the transition from primary school to middle school», en *American Educational Research Journal,* 37(3), 2000.
PÉREZ MARTÍNEZ, A., y ORTIGOSA BLANCH, A., «Una aproximación al *ciberbullying*», en GARCÍA GONZÁLEZ, J. (coord.), *Ciberacoso: La tutela penal de la intimidad, la integridad y la libertad sexual en Internet,* Valencia, Tirant lo Blanch, 2010.
PEW RESEARCH CENTER, «Pew Internet & American Life Project. Teens, Adults & Sexting: Data on sending & receipt of sexually suggestive nude or nearly nude images by American adolescents & adults». Disponible en Internet en *http://www.pewinternet.org/Presentations/2010/Oct/Teens-Adults-and-Sexting.aspx.*
PIERCE, T. A., «Talking to Strangers on MySpace: Teens' Use of Internet Social Networking Sites», en *Journal of Media Psychology*, vol. 11, núm. 3, 2006. En Internet en *http://www.calstatela.edu/faculty/sfischo/myspace.htm* (última visita el 1 de agosto de 2011).
— «X-Posed on MySpace: A Content Analysis of "MySpace" Social Networking Sites», en *Journal of Media Psychology,* vol. 12, núm. 1, winter 2007. En Internet, en, *http://www.calstatela.edu/faculty/sfischo/X-posed_on_%20MySpace.htm* (última visita el 1 de agosto de 2011).
PINGUELO, F. M., y MULLER, B. W., «Virtual Crimes, Real Damages: A Primer On Cybercrimes In The United States and Efforts to Combat Cybercriminals», en *VJLT*, vol. 16, núm. 1, Spring 2011.
PITTARO, M. L., «Cyber stalking: An Analysis of Online Harassment and Intimidation», en *IJCC*, vol. 1, núm. 2, 2007.
— «CyberStalking: Typology, Etiology, and Victims», en JAISHANKAR, K. (ed.), *Cyber Criminology. Exploring Internet crimes and criminal behavior*, Boca Ratón, CRC Press, 2011.
POLLOCK, E. T., «Understanding and Contextualising Racial Hatred on the Internet: A Study of Newsgroups and Websites», en *Internet Journal of Criminology*, 2010.
POULLET, Y., «Hacia nuevos principios de protección de datos en un nuevo entorno TIC», en *IDP*, núm. 5, 2007.
PRAS, A.; SPEROTTO, A.; MOURA, G. C.; DRAGO, I.; BARBOSA, R.; SADRE, R.; SCHMIDT, R., y HOFSTEDE, R., «Attacks by "Anonymous" WikiLeaks Proponents not Anonymous», *CTIT Technical Report 10.41,* December 10, 2010, pp. 1 y ss. En Internet en *http://eprints.eemcs.utwente.nl/19151/.*
PRATT, T. C.; HOLFRETER, K., y REISIG, M. D., «Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory», en *Journal of Research in Crime and Delinquency,* vol. 47, núm. 3, 2010.
PRENSKY, M., «Digital Natives, Digital Immigrants», *On the Horizon,* vol. 9, núm. 5, 2001.
PRICE, D., y SCHMADEKE, S., «Hackers Expose Web Weakness: There's No Defense Against Internet Assaults, Experts Confess, and Attackers are Elusive», en *DN*, 14 de febrero de 2000.

PRUNCKUN, H., «"Bogies in the wire": Is there a need for legislative control of cyber weapons?», en *GC,* vol. 9, núm. 3, agosto 2008.

PUJAZON-ZAZIK, M., y PARK, M. J., «To Tweet, or Not to Tweet: Gender Differences and Potential Positive and Negative Health Outcomes of Adolescents», en *Social Internet Use, Am. J. Mens Health,* vol. 4, núm. 1, 2010, pp. 77-85.

QUINTERO OLIVARES, G., «Internet y Derecho penal. Imputación de los delitos y determinación de la competencia», en *LL,* núm. 37, enero, año IV, abril 2007.

RAINIE, L., *Life Online: teens and technology and the world to come. Speech to the anual conference of the Public Library Association*, Boston, Massachusetts, 2006.

RALUCA, S., «Cybercrime and its challenges between reality and fiction. Where do we actually stand?», en *Rivista di Criminologia, Vittimologia e Sicurezza*, vol. 3, núm. 3, 2009.

RATCHFORD, B. T.; TALUKADAR, D., y LEE, M., «A Model of Consumer Choice of the Internet as an Information Source», en *International Journal of Electronic Commerce,* vol. 5, núm. 3, 2001, pp. 7-21.

RAYMOND, E. S., *How to Become a Hacker* (2001). En Internet en *http://www.catb.org/~esr/faqs/hacker-howto.html* (última visita el 9 de septiembre de 2010).

REDONDO ILLESCAS, S., «Individuos, sociedades y oportunidades en la explicación y prevención del delito: Modelo del triple Riesgo Delictivo (TRD)», en *Revista Española de Investigación Criminológica,* núm. 6, 2008.

REINARES NESTARES, F., *Terrorismo y antiterrorismo,* Barcelona, Paidós Ibérica, 1998.

REISIG, M. D.; TRAVIS C. P., y HOLFRETER, K., «Perceived Risk of Internet Theft Victimization: Examining the Effects of Social Vulnerability and Financial Impulsivity», en *CJB,* vol. 36, 2009.

REYNA ALFARO, L. M., «La víctima en el delito informático», en *Revista de Pensamiento Penal*, disponible en *http://200.61.183.148/node/28764.*

REYNS, B., «Being Pursued Online: Extent and Nature of Cyberstalking Victimization from a Lifestyle/Routine Activities Perspective», 2010. En Internet en *http://etd.ohiolink.edu/view.cgi?acc_num=ucin1273840781.*

REYNS, B. W.; HENSON, B., y FISHER, B. S., «Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization», en *CJB*, 2011.

RICHARDS, R. D., y CALVERT, C., «When Sex and Cell Phones Collide: Inside the Prosecution of a Teen Sexting Case», 2009. En Internet en *http://www.lawrencewalters.com/articles/AlpertArticle.pdf.*

RICKETTS, M. L., y HIGGINS, G. E., «Assessing sex experiences of online victimization: an examination of adolescent», en *Criminal Justice Review,* 2010, pp. 1-26.

RIVAS PALÁ, P., «Sociedad liberal y propaganda del odio racial», en *AFDUC*, núm. 6, 2002.

ROBIN, G., *Employees as Offenders, Journal of Research in Crime and Delinquency,* Sage Publications, 1969.

ROGERS, M. K., «The Psyche of Cybercriminals: A Psycho-Social Perspective», en GHOSH, S., y TURRINI, E. (eds.), *Cybercrimes: A Multidisciplinary Analysis*, Berlin-Heidelberg, Springer-Verlag, 2010.

ROJO GARCÍA, J. C., «La realidad de la pornografía infantil en Internet», en *Revista de Derecho Penal y Criminología,* 2.ª época, núm. 9, 2002.

ROLLINS, J., y WILSON, C., «Terrorist Capabilities for Cyberattack: Overview and Policy Issues», en *CRS Report for Congress,* enero 2007.

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.

— «Los delitos de daños en el ámbito informático», en *CPC,* núm. 43, 1991.

— «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.
ROSENZWEIG, R., «Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet», en *AHR*, vol. 103, núm. 5, diciembre, 1998.
ROVIRA DEL CANTO, E., *Delincuencia informática y fraudes informáticos,* Granada, Comares, 2002.
RUIZ VADILLO, E., «Tratamiento de la delincuencia informática como una de las expresiones de la criminalidad económica», en *PJ,* número especial IX, 1989.
SALTER, A. C., *Predators: Pedophiles, Rapists, and Other Sex Offenders: Who They Are, How They Operate, and How We Can Protect Our Children*, New York, Basic Books, 2003.
SAMUEL, A. W., *Hacktivism and the Future of Political Participation,* tesis doctoral presentada para el doctorado en la Harvard University Cambridge, Massachusetts, septiembre, 2004.
SANZ MULAS, N., «Pornografía en Internet», en *Revista Penal,* núm. 23, 2009.
SCHELL, B. H., y MARTIN, C., *Handbook on cybercrime,* Santa Bárbara, ABC-CLIO, 2004.
SCHJOLBERG, S., «The Legal Framework - Unauthorized Access to Computer Systems. Penal Legislation in 44 Countries». En Internet en *http://www.mosstingrett.no/info/legal.html* (última visita el 9 de septiembre de 2010).
SCHUR, E. M., *Crimes without victims: Deviant behavior and public policy: Abortion, homosexuality, drug addiction,* Englewood Cliffs, Prentice Hall, 1965.
SERRANO MAÍLLO, A., *Oportunidad y delito,* Madrid, Dykinson, 2009.
— *Introducción a la criminología*, 6.ª ed., Madrid, Dykinson, 2009.
SHADEL, D., *Outsmarting the Scam Artist: How to Protect Yourself From the most Clever Cons,* Wiley, 2012.
SHERIDAN, L., y GRANT, T., «Is cyberstalking different?», en *PCL,* 2007.
SIEBER, U., *Computerkriminalität und Strafrecht,* Köln/Berlin/Bonn/München, Carl Heymanns, 1980 (2.ª ed.).
— *Informationstechnologie und Strafrechtsreform,* Köln/Berlin/Bonn/München, Carl Heymanns, 1985.
— *The international handbook on computer crime*, Chichester, John Wiley and Sons, 1986.
— «Criminalidad informática: peligro y prevención» (traducido por E. FARRÉ TREPAT), en MIR PUIG, S. (comp.), *Delincuencia informática,* Barcelona, PPU, 1992.
SIEBER, U., y BRUNST, P., *Cyberterrorism. The use of the Internet for terrorist purposes*, Strasbourg, Council of Europe Publishing, 2007. En Internet en *http://book.coe.int/ftp/3013.pdf* (última visita el 29 de diciembre de 2010).
SINROD, E. J., y REILLY, W. P., «Cyber-crimes: a practical approach to the application of federal computer crime laws», en *CHTLJ,* vol. 16, 2000.
SLONJE, R., y SMITH, P. K., «Cyberbullying: another main type of bullying?», en *SJP,* 2008.
SMITH, A., *Protection of Children Online: Federal and State Laws Addressing Cyberstalking, Cyberharassment and Cyberbuylling,* Congressional Research Service, 2009.
SMITH, M., y CORNISH, D. B., «Theory for Practice in Situational Crime Prevention», en *CPS,* vol. 16.
SMITH, R. G., «Biometric solutions to identity-related cybercrime», en JEWKES, Y., *Crime Online*, Portland, Willan Publishing, 2007.
SMITH, R. G.; GRABOSKY, P., y URBAS, G., *Cybercriminals on trial,* Cambridge, Cambridge University Press, 2004.

SMITH, P. K.; MAHDAVI, J.; CARVALHO, M.; FISHER, S.; RUSSELL, S., y TIPPETT, N., «Cyberbullying: its nature and impact in secondary school pupils», en JCPP, 2008.

SOMMER, P., y BROWN, I., «Reducing Systemic Cybersecurity Risk. Contribution to the OECD project Future "Global Shocks"», 2011. En Internet en *http://www.oecd.org/dataoecd/57/44/46889922.pdf* (última visita el 19 de junio de 2012).

SOOPRAMANIE, D. G., y ROBERTSON, A., «Adoption and usage of online shopping: an empirical analysis of the characteristics of "buyers" and "non-internet shoppers"», en *JRCR,* vol. 14, núm. 1, 2007.

SOURANDER, A.; BRUNSTEIN KLOMEK, A.; IKONEN, M.; LINDROOS, J.; LUNTAMO, T.; KOSKELEAINEN, M.; RISTKARI, T., y HELENIUS, H., «Psychosocial Risk Factors Associated With Cyberbullying Among Adolescents. A Population-Based Study», en *AGP,* núm. 67, 2010.

SPITZNER, L., *Know Your Enemy: The Tools and Methodologies of the Script Kiddie*. En Internet en *http://www.firstvpn.com/papers/misc/KnowYourEnemy1.pdf* (última visita el 6 de diciembre de 2010).

SPRING, T., «Al Qaeda's Tech Traps. Investigations, arrests highlight how technology aids and weakens terror network», en *PCWorld*, septiembre, 2004. En Internet en *http://www.pcworld.com/news/article/0,aid,117658,00.asp* (última visita el 9 de septiembre de 2010).

STADLER, W. A., «Internet Fraud», en FISHER, B. S., y LAB, S. P., *Encyclopedia of Victimology and Crime Prevention,* vol. 1, California/London, Sage Publications, 2010.

STAJANO, F., y WILSON, P., «Understanding scam victims: Seven principles for systems security. Commun», en *ACM*, 2011.

SUBIJANA ZUNZUNEGUI, I. J., «El ciberterrorismo: una perspectiva legal y judicial», *Eguzkilore,* núm. 22, San Sebastián, diciembre, 2008.

SUBRAHMANYAM, K.; REICH, S. M.; WAECHTER, N., y ESPINOZA, G., «Online and offline social networks: Use of social networking sites by emerging adults», en *JADP,* 29, 2008.

SUKHAI, N. B., *Hacking and Cybercrime* (2004), Base de datos ACM. En Internet en *http://portal.acm.org/citation.cfm?id=1059553* (última visita el 9 de septiembre de 2010).

SUMERS, L., «Las técnicas de prevención situacional del delito aplicadas a la delincuencia juvenil», en *Revista de Derecho Penal y Criminología,* 2009.

SUSSMAN, V., «Policing cyberspace», en *U.S. News and World Report*, enero, 1995.

SVENSSON J. S., y BANNISTER F., «Pirates, sharks and moral crusaders: Social control in peer-to-peer networks», en *FMPRJI,* vol. 9, núms. 6-7, junio, 2004.

TAYLOR, P. A., «From hackers to hacktivists: speed bumps on the global superhighway?», en *NMS,* vol. 7, núm. 5*,* 2005.

TAYLOR, M., y QUAYLE, E., *Child Pornography. An Internet Crime*, New York, Routledge, 2003.

TERRADILLOS BASOCO, J., «El Derecho penal de la globalización: luces y sombras», en *Transformaciones del Derecho en la mundialización,* Madrid, Consejo General del Poder Judicial, 1999.

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.

THOMAS, J., «The moral ambiguity of social control in cyberspace: a retro-assessment of the "golden age" of hacking», en *NMS,* núm. 7, 2005.

TIEDEMANN, K., *Wirtschaftsstrafrecht und Wirtscahtskriminalität,* vol. 2, Hamburg, 1976.
— *Poder económico y delito,* Barcelona*,* Ariel, 1985.
TILLEY, N., *Crime Prevention*, Collumpton, Willan Publishing, 2009.
TIMOFEEVA, Y. A., «Hate speech online: restricted or protected? Comparison of regulations in the United States and Germany», en *JTLP*, vol. 12, núm. 2, 2003.
TOUNTAS, S. W., «Carnivore: Is the Regulation of Wireless Technology a Legally Viable Option to Curtail the Growth of Cybercrime?», en *WUJLP,* vol. 11, 2003.
TURGEMAN-GOLDSCHMIT, O., «Hacker's Accounts: Hacking as a social entertainment», en *SSCR,* núm. 23, 2005.
— «Meanings that Hackers Assign to their Being a Hacker», en *IJCC*, vol. 2, julio-diciembre, 2008.
TYLER, T., *Why People Obey the Law,* Princeton, Princeton University Press, 2006.
VAN BLARCUM, C. D., «Internet Hate Speech: The European Framework and the Emerging American Haven», en *WLLR,* vol. 62, núm. 2, 2005.
VANDEBOSCH, H., y VAN CLEEMPUT, K., «Cyberbullying among youngsters: profiles of bullies and victim», en *New Media and Society*, 2009.
VERISIGN, *Fraud Alert: Phishing. The Latest Tactics and Potential Business Impact,* White Paper, 2009, consultado en línea el 14 de junio de 2012 en *http://www.verisign.com/static/phishing-tactics.pdf.*
VILLACAMPA ESTIARTE, C., *Stalking y Derecho penal. Relevancia jurídico-penal de una nueva forma de acoso*, Madrid, Iustel, 2009.
— «La respuesta jurídico-penal frente al *stalking* en España: presente y futuro», en *Revista del Instituto Universitario de Investigación en Criminología y Ciencias Penales de la UV*, 2010. En Internet en *http://www.uv.es/recrim/recrim10/recrim10a03.pdf.*
VON HIRSH, A.; GARLAND, D., y WAKEFIELD, A., *Ethical and social perspectives in situational crime prevention*, Oxford, 2000.
VOZMEDIANO, L.; SAN JUAN, C., y VERGARA, A. I., «Problemas de medición del miedo al delito: algunas respuestas teóricas y técnicas», en *Revista Electrónica de Ciencia Penal y Criminología,* 2008.
WALL, D., «Cybercrimes and the Internet», en WALL, D. (ed.), *Crime and the Internet,* New York, Routledge, 2001.
— *Cybercrime: the transformation of crime in the information age*, Cambridge, Polity Press, 2007.
— «Cybercrime and the culture of fear: Social Science fiction(s) and the production of knowledge about cybercrime», en *ICS*, vol. 11, núm. 6, 2008.
WALL, D. S., «What are Cybercrimes?», en *CJR,* 2005.
— «The Internet as a Conduit for Criminals», en PATTAVINA, A., *Information Technology and the Criminal Justice System*, California, Thousand Oaks, Sage Publications Inc, 2005.
WALRAVE, M., y WANNES, H., «Cyberbullying: Predicting Victimisation and Perpetration», en *Children & Society*, vol. 25, núm. 1, 2009.
WALTERBACH, M., «International illicit convergence: the growing problem of transnational organized crime groups' involvement in intellectual property rights violations», en *FSULR*, vol. 34, núm. 2, 2007.
WANG, J.; IANNOTTI, R. J., y NANSELL, T., «School Bullying Among US Adolescents: Physical, Verbal, Relational and Cyber», en *JAH,* vol. 45, núm. 4, octubre, 2009.
WARK, M. K., «Hackers», en *TCS,* núm. 23, 2006.
WEIMANN, G., «The Psychology of Mass-Mediated Terrorism», en *ABS,* vol. 52, núm. 1, septiembre, 2008.

WEISBURD, D.; WYCKOFF, L. A.; READY, J.; ECK, J. E.; HINKLE, J. C., y GAJEWSKI, F., «Does crime just move around the corner? A controlled study of spatial displacement and diffusion of crime control benefits», en *Criminology*, vol. 44, núm. 3, 2006.

WELLMAN, B., «Computer Networks As Social Networks», en *Science*, vol. 293, 14 de septiembre de 2001.

THE WHITE HOUSE, «National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy», 2010. En Internet en *http://www.dhs.gov/xlibrary/assets/ns_tic.pdf*.

WILKINSON, S., «The Modern Policing Environment», en BAMMER, G. (ed.), *Dealing with Uncertainties in Policing Serious Crime,* Sidney, ANU E Press, 2010.

WILLIAMS, A. L., y MERTEN, M. J., *A review of online social networking profiles by adolescents: Implications for future research and intervention,* Libra Publishers Inc., 2008.

WILLIAMS, P., «Organized Crime and Cybercrime: Synergies, Trends, and Responses», en *ATC,* vol. 6, agosto 2001.

WOLAK, J.; FINKELHOR, D.; MITCHELL, K. J., e YBARRA, M. L., «Online "predators" and their victims: myths, realities and implications for prevention and treatment» (2008), en *APs,* vol. 63. En Internet en *http://psycnet.apa.org/journals/amp/63/2/* (última visita el 21 de diciembre de 2010).

WORLD ECONOMIC FORUM, «Global Risks 2011: Sixth edition» 2011. En Internet en *http://riskreport.weforum.org/*.

WORTLEY, R., y SMALLBONE, S., «Child pornography on the Internet», en *Problem-Oriented Guides for Police,* núm. 41, mayo, 2006. En Internet en *http://www.cops.usdoj.gov/Publications/e04062000.pdf.*

YAR, M., «The novelty of "cybercrime": an assessment in light of routine activity theory», en *EJC,* núm. 2, 2005.

— «The global "epidemic" of movie "piracy": crime-wave or social construction?», en *MCS,* vol. 27, núm. 5, 2005.

— *Cybercrime and society,* London, Sage, 2006.

YBARRA, M. L., y MITCHELL, K., «Exposure to Internet Pornography among Children and Adolescents: A National Survey», en *CpB,* vol. 8, núm. 5, 2005.

YEARGAIN, J. W.; SETTOON, R. P., y MCKAY, S. E., «Can-Spam act of 2003: How to spam legally», en *JSeC,* vol. 2, núm. 1, 2004.

YOUNG, K. S., «Profiling online sex offenders, cyber-predators, and pedophiles», en *JBP,* vol. 5, núm. 1, 2005.

YOUNG, R., y ZHANG, L., «Factors Affecting Illegal Hacking Behavior», en AMCIS 2005 Proceedings. *Paper 457*. En Internet en *http://aisel.aisnet.org/amcis2005/457* (última visita el 3 de diciembre de 2010).

YUCEDAL, B., «Victimization in cyberspace: An application of routine activity and lifestyle exposure Theories» (2010). En Internet en *http://etd.ohiolink.edu/send-pdf.cgi/YUCEDAL%20BEHZAT.pdf?kent1279290984* (última visita el 9 de septiembre de 2010).

ZHANG, X., «Charging children with child pornography. Using the legal system to handle the problem of Sexting», en *CLSR,* vol. 26, núm. 3, 2010.

ZHENG, R.; QIN, Y.; HUANG, Z., y CHEN, H., «Authorship Analysis in Cybercrime Investigation», en VVAA, *Lecture Notes in Computer Science,* Berlin-Heidelberg, Springer Verlag, 2003.

ZUCKERMAN, E.; ROBERTS, H., y YORK, J. C., «Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites», en *The Berkman Center for Internet & Society at Harvard University,* núm. 16, 2010.

COLECCIÓN «DERECHO PENAL Y CRIMINOLOGÍA»

http://www.derechopenalycriminologia.es

TÍTULOS PUBLICADOS

Principios distributivos del Derecho penal
A quién debe sancionarse y en qué medida
Paul H. Robinson

¿Conforme a qué criterios ha de establecerse la responsabilidad penal y determinarse la medida de la pena? La respuesta a esta pregunta está inseparablemente ligada a la cuestión de cuáles deban ser las finalidades del Derecho penal. Conforme al análisis tradicional, éstas se dividen en consecuencialistas u orientadas a fines futuros y retributivas o basadas en el merecimiento pasado, si bien muchos autores e incluso algunos textos legales se inclinan por una ponderación de las distintas finalidades.

En este importante libro, Paul H. Robinson muestra los problemas de los planteamientos que acuden simultáneamente a diversas finalidades sin establecer criterios claros sobre qué hacer en caso de que sus racionalidades entren en conflicto, así como las dificultades que aquejan a cada una de las finalidades, de tipo empírico en el caso de las consecuencialistas y de tipo conceptual y práctico en el caso de las basadas en el merecimiento. Una vez examinados estos problemas, y apoyándose en sus numerosas investigaciones sobre las intuiciones de la comunidad sobre la justicia penal, el profesor Robinson desarrolla su propio planteamiento, denominado «merecimiento empírico», con el que propone superar la situación de colisión entre teorías deontológicas y consecuencialistas. Además de numerosa información sobre los resultados de la investigación empírica acerca de los efectos de la pena, en el presente libro el lector encontrará una excelente revisión de la teoría de los fines de la pena en el ámbito anglosajón, escrita por uno de los más prestigiosos teóricos del Derecho penal actual.

Los delitos culturalmente motivados
Ideologías y modelos penales
Cristina de Maglie

La diversidad cultural presente en las sociedades actuales constituye una consecuencia inevitable de la globalización, pero puede generar al mismo tiempo numerosos conflictos de carácter político, social y jurídico. Los asesinatos por causa de honor, la infibulación del clítoris o la escarificación, son algunos de los comportamientos aceptados o incluso impuestos por la cultura de ciertas minorías culturales que pueden ser considerados delito por el ordenamiento jurídico de los países occidentales en los que estas se alojan. Asume así gran importancia el estudio de las distintas tendencias en la jurisprudencia y en la doctrina penales de dichos países frente al surgimiento de los llamados delitos culturalmente motivados.

La presente obra aborda esta temática desde una perspectiva sociológica y de Derecho comparado, partiendo de una rigurosa definición de *cultura* —entendida en su acepción étnica— para llegar a una noción precisa de *delito culturalmente motivado* y analizando los principales modelos desde los que el Derecho penal afronta los conflictos culturales. En particular, en la búsqueda de opciones plausibles en la aplicación en estos casos de circunstancias eximentes y atenuantes, la autora da una gran relevancia al papel del juez y a la función de la prueba del hecho culturalmente motivado. Finalmente, analiza las posibles soluciones basadas en el actual Derecho positivo italiano y concluye con una propuesta para el futuro legislador.

La evitabilidad del error de prohibición
Fernando Jorge Córdoba

En el debate de la dogmática de la teoría del error se ha escrito y discutido mucho sobre cuáles deberían ser las consecuencias de un error de prohibición evitable, pero muy poco sobre cómo se debería establecer la evitabilidad de ese error. El libro que se presenta quiere ser una aportación que contribuya a llenar ese vacío.

La obra tiene así como objetivo final proporcionar un conjunto de reglas para establecer en un caso concreto la evitabilidad o inevitabilidad de un error de prohibición. El objetivo intermedio, como en toda investigación dogmática, es ofrecer un marco teórico adecuado que sustente esas reglas, las explique y les dé coherencia sistemática entre sí y con el resto del sistema de la teoría del delito, en especial, con la teoría del ilícito y de la culpabilidad.

Con este fin, los conceptos habitualmente utilizados en la materia son reformulados a partir de una concepción funcionalista de la culpabilidad y reconducidos a dos preguntas centrales. La primera, dirigida a comprobar si el autor habría podido conocer el ilícito *si se hubiese motivado a conocer el significado jurídico de su conducta.* La segunda, y asumiendo que la respuesta al primer interrogante sea afirmativa, para establecer si el autor tenía *el deber de motivarse a conocer el significado jurídico de su conducta*, y si satisfizo ese deber. El análisis de las características físicas e intelectuales del autor concreto que condicionarían la respuesta a la primera cuestión, y la especificación de la naturaleza y la medida de ese deber completan el recorrido propuesto. Desde la misma perspectiva se toma postura respecto de dos cuestiones adicionales tratadas en la materia: las llamadas informaciones hipotéticas y la coincidencia temporal entre hecho y evitabilidad.

La interpretación conforme a la Constitución de las leyes penales
Lothar Kuhlen

Cada vez más las leyes penales se interpretan o corrigen de conformidad con la Constitución. Esto plantea una serie de problemas de método, jurídico-constitucionales y jurídico-penales. Esta investigación pretende realizar una aportación inductiva para resolverlos. Para ello, tras una exposición introductoria del problema, ofrece una visión de conjunto de las sentencias más importantes del Tribunal Constitucional Federal y del Tribunal Supremo Federal en materia de interpretación conforme a la Constitución de las leyes penales. A continuación se analizan con detalle la restricción conforme a la Constitución del tipo del blanqueo de capitales llevada a cabo por el Tribunal Constitucional Federal y la del tipo del cohecho pasivo, llevada a cabo por el Tribunal Supremo Federal.

En contraposición a la crítica fundamental de la doctrina formulada por algunos, en este trabajo se defiende en principio la conservación conforme a la Constitución de las leyes penales que ha sido practicada por el Tribunal Constitucional Federal y por el Tribunal Supremo Federal. Con todo, se formulan una serie de precisiones, modificaciones y correcciones de esta praxis y, en especial, una restricción de la interpretación conforme a la Constitución de las leyes en términos diferentes según si ésta la lleva a cabo el Tribunal Constitucional Federal, por una parte, o la realizan los tribunales penales, por otra. También se revela problemática la tendencia de la jurisprudencia más reciente a clasificar las leyes penales y su interpretación como inconstitucionales a causa de su falta de determinación.

Motivos reprochables
Una investigación acerca de la relevancia de las motivaciones individuales para el Derecho penal liberal
José Milton Peralta

En esta obra se trata un tema tan clásico como a veces relegado en el Derecho penal: la relevancia de las motivaciones individuales para la responsabilidad penal. El caso paradigmático, aunque el problema sea más general, es el del asesinato. Muchos ordenamientos agravan la muerte cuando el autor obra con ciertas motivaciones como el odio racial o religioso; o por xenofobia, codicia o para satisfacer el deseo sexual. Ya no se habla más de homicidio, sino de asesinato.

En el texto se inquiere sobre este problema desde un punto de vista normativo. Se pregunta si es que los motivos «deben» ser relevantes para la responsabilidad penal y no se asume sin más que lo «son». Por ende, la investigación no se dirige a interpretar un cierto ordenamiento positivo que dé relevancia a los motivos (aunque sus conclusiones luego tendrán un impacto al respecto), sino a determinar si tal relevancia existe en general. En particular, desde la perspectiva del Derecho penal de acto, no se puede descartar la posibilidad de descalificar por iliberal cualquier intento de hacer variar la pena conforme a un elemento tan interno como los motivos.

En esta tarea, el autor examina de un modo analítico diferentes intentos justificatorios, basándose en literatura alemana, española y argentina, con mención también de bibliografía angloamericana. El análisis se realiza tanto desde la teoría de la pena, como desde la teoría del delito, considerando diferentes perspectivas. Ante los resultados negativos de esos estudios, en la parte final propone y desarrolla un modelo de solución alternativo según el cual los motivos, entendiéndolos de cierta manera, tienen que ver con un «hecho» más grave.

La crisis del principio de legalidad en el nuevo Derecho penal: ¿decadencia o evolución?
Juan Pablo Montiel (ed.)

Durante las últimas tres décadas se viene sosteniendo que el Derecho penal y, en concreto, el principio de legalidad viven en un «estado de crisis». Tal situación se habría originado, principalmente, por el importante proceso de transformación que ha experimentado en este tiempo el Derecho penal como resultado de las nuevas formas de criminalidad, del particular contexto político-criminal y de la internacionalización. Esta crisis se asocia fundamentalmente a una clara disminución del poder de influencia de la ciencia penal, que se manifiesta en el relajamiento que en la praxis han experimentado, sobre todo, los postulados de *lex certa*, *lex scripta*, *lex stricta* y *lex praevia*. Sin embargo, en esta crisis el Derecho penal encuentra nuevos desafíos para continuar con su evolución y para hacer más racional su aplicación en ámbitos que tradicionalmente quedaban al margen de ella.

El presente volumen aborda ambos sentidos de la crisis a partir de las contribuciones de destacados juristas alemanes, argentinos, españoles y estadounidenses, resaltando la extraordinaria importancia que tiene este «estado de crisis» para contribuir al avance de la ciencia jurídico-penal y a una mejor comprensión del principio de legalidad.

Fundamentos de Política criminal
Un retorno a los principios
Pablo Sánchez-Ostiz

Fundamentos de Política criminal ofrece una visión original de temas clásicos. El autor procede a una sistematización de las diversas proposiciones empleadas comúnmente en la Política criminal: desde la regla *nullum crimen sine lege*, hasta la presunción de inocencia, pasando por la abolición de la pena de muerte y la tortura, así como el *ne bis in idem*. A juicio de su autor, es posible esa sistematización con base en tres principios (seguridad, legalidad y respeto de la dignidad), que diferencia de las diversas y abundantes reglas y sus consiguientes excepciones. De ahí el subtítulo que se ha dado a la obra: *Un retorno a los principios*, que es una mirada a los orígenes filosóficos, jurídicos y antropológicos del Derecho y de la Política.

El autor elabora un estudio inductivo de los enunciados vigentes en las decisiones del legislador, la judicatura y la Administración, para indagar a continuación los principios que les dan sentido. De este modo, se asume la tarea de aportar una fundamentación racional a la práctica político-criminal del Estado: se hace patente la racionalidad interna de las decisiones cotidianas de la Política frente al delito y a la vez se aportan claridad y elementos de crítica de las decisiones político-criminales al uso.

Variaciones sobre la presunción de inocencia
Análisis funcional desde el Derecho penal
Javier Sánchez-Vera Gómez-Trelles

El Derecho fundamental a la presunción de inocencia es la esencia de todo proceso penal: no es un principio más del proceso, es el proceso mismo, a modo de directa prohibición de desautorizarlo. El hilo conductor es la presunción de inocencia: problemas escogidos en torno a la misma, a través de un programa que explica sus efectos en diversos ámbitos del Derecho penal.

La obra revisa ampliamente el propio concepto de presunción de inocencia y otros aspectos básicos también relacionados, como el dolo, la prescripción, la prisión provisional, el delito flagrante, la psicología del testimonio o el careo, etc. Igualmente, la verdad procesal y sus implicaciones para el Derecho penal, las presunciones en el Código Penal, así como las máximas de la experiencia según los tipos de la Parte Especial: homicidio y lesiones, delitos sexuales, socioeconómicos, contra la seguridad vial, blanqueo de capitales y otros, todo presidido por las reglas de la lógica. Un epígrafe sobre la extensión *a toda* la tipicidad de los principios reservados a los indicios, se adentra de forma crítica en la configuración del tipo penal, y también se detalla pormenorizadamente la vigencia del esencial *in dubio pro reo*, a veces tan olvidado, su concepto y aplicabilidad en supuestos complejos, por ejemplo de concurso de delitos. Respondiendo a los objetivos de la presente colección, se analizan los *nuevos frentes* a los que la misma quiere contribuir: la incesante preocupación por la criminalidad y las posibles medidas correctoras, hoy en ebullición por los importantes cambios que se vienen produciendo en la política criminal y su praxis.

Variaciones, en suma, sobre un único principio que habrán de guardar el mismo patrón armónico del tema original: el baluarte de la inocencia como sistema afortunadamente proclamado por la Constitución para el Derecho penal.